THE LADY AND THE H@CKER

MARIA GENOVA

THE LADY AND THE H@CKER

THE NIGHTMARE OF IDENTITY THEFT

'The fastest growing crime is identity fraud' - De Telegraaf

More Than 1 Million Children Were Victims of Identity Theft in 2017 - Fortune

'It takes just a copy of your passport for your identity to be stolen' - NRC Handelsblad (Dutch national newspaper)

'Hackers set up thousands of false LinkedIn-accounts' - Knack

'Campaign to prevent identity fraud of children on social media' - Dutchcowboys.nl

'The victim of identity fraud ends up in a horror scenario in which bailiffs, debt collecting agencies and detectives chase after a shadow which always points in your direction'
- TV programme KRO Reporter

'NSA can tap nearly every mobile phone'
- Algemeen Dagblad (Dutch national newspaper)

More information about Maria Genova? www.mariagenova.nl

Original title: Komt een vrouw bij de H@cker / Just Publishers

English version: 1st print, December 2018
Author: Maria Genova
Design: Raymond Zachariasse | www.miralovesbooks.com
Fonts: Antonio - fontsquirrel.com

WWW.MARIAGENOVA.NL

CONTENT

PREFACE

ID theft, fraud and data breaches have reached epidemic levels through phishing, hacking of usernames and passwords and stolen IDs. In addition, police and justice are not prepared to help the victims. When your identity is stolen, your life can turn into a living hell. Victims describe how they suddenly had houses full of drugs registered in their name, how they had to pay enormous bills, how they lost their jobs, could not apply for a mortgage, and how they stayed in prison until the police found out that they had locked up the victim, but not the criminal.

Identity theft and fraud should be eliminated. That this is not just necessary but also deserves to be a priority, is shown by the numerous real-life stories described in this book. To support this goal, Biocryptology has joined forces with its writer, Maria Genova, to enable the widespread availability of this book. Being now accessible to international readers in many countries worldwide, the book will not just increase awareness, but will also stimulate the implementation of an effective solution to solve the enormous problems that are caused by ID theft and fraud.

Biocryptology offers this solution. It is the first organization that

provides users with an all-in-one platform with just one enrolment procedure for all online and physical access and identification. This avoids the need to register your data for each local solution separately. And it avoids using different apps and identification methods for all these different places, which causes not just a security risk, but also great inconvenience.

We are proud that we have been able to create a frictionless access method to free yourself of the Achilles heel of IT: passwords and usernames. Although we are not the only company who does this, we are the only company that has made one single platform suitable for all kinds of uses. And we eliminate the need for consumers to leave their ID trail related to physical access and identification. Examples of situations where they still ask for your personal (and sensitive) information, are when you check in at a hotel or when renting a car.

In addition to fighting ID theft and fraud, we also help victims of ID theft and fraud. Biocryptology supports associations where these victims are registered, among others with legal assistance and support from IT security experts, That will help the victims to reclaim their identity and get their life back on track. Our social engagement is also one of the reasons that Spanish actor Antonio Banderas has chosen to become Biocryptology's global ambassador.

If you want to find out more about Biocryptology and how we help companies and governments, please visit our website: www.biocryptology.com.

We hope you enjoy reading this book while gaining useful insights and we look forward meeting you at one of the many worldwide events in which we participate. Let's eliminate identity theft and fraud together.

The team of Biocryptology

1

1737 cars registered to your name

'It started with a bank statement which was stolen from my mailbox. Then they applied for a bank card and then they emptied my bank account. How can the bank just hand over my money to someone else? Will I start receiving bills and direct debit charges? I'm so upset.'

I read that on a forum on the internet. The fear and astonishment of this woman jumps off the screen. This seems to me to be the most difficult part: that you have no idea how far these criminals will go. In the horrific scenario of identity fraud, you're always up against an invisible enemy.

Steve Romet is a good example of this. Every day he receives fines and payment reminders after someone stole his driving license at a nightclub. In just a short space of time the criminals have registered 1737 cars using his name. Romet was arrested and spent months in jail. He simply can't prove that he can't buy 1737 cars on his unemployment benefits. He can't convince the Department of Motor Vehicles that it is impossible to register new cars from jail. The logic of a system overpowers the simple logic of an individual. His unemployment benefits are revoked, because according to the Department of Labor, anyone who can buy so many cars no longer needs benefits.

Before the case is finally resolved, seventeen years pass by, years of fear and misery for Romet. He finally gets justice at the European Court for Human Rights. As the victim of a clerical error he receives € 9.000 compensation.

The worst thing is that you don't have to lose your driving license to become a victim of such practices. There is an active international trade in copies which are just as useful when committing fraud. I wonder how many copies of my passport and driving license are

floating around? Hotels, car rental companies, government agencies, banks, telephone companies, almost everyone requires a copy.

Those who have become victims of cybercrime complain that the policemen are digital novices and don't understand it. I came across an 'Agent Digital' on Twitter who educates people on the subject of identity fraud.

'If I want to, I can easily steal your identity,' the policeman says when we first get in touch.

'How would you do that?'

'I would send you a reliable looking e-mail. When you open it, you will unintentionally give me access to your computer. Forever.'

'Hmm.'

'Do you want to try it out? I can also copy your LinkedIn details and send messages as if I were you to different people. If you want to stop me, then you need to prove that you are being harmed by this and in practice this is not so easy.'

I try not to put too much private information on the internet, but if you have a profile on the well-known social media sites, that in itself can be too much. Missing details are often filled in by other sites. The Chamber of Commerce puts all my details online because I own a company, Google Maps lets everyone zoom into my home. Even my telephone number is listed, despite the fact that it is not registered to my name. Every company wants a full set of personal data, because this is much more worthy.

'How far can someone go with my details?' I ask.

'How far do you want to go?' the policeman responds.

'I just want to know what is possible.'

I hear a chuckle at the other end of the telephone line. 'I'll send you some information by email.'

1737 cars registered to your name

2
Innocent, but in jail

A detached home on a new housing estate in a town in North-Holland. Ron Kowsoleea opens the front door and shows me in. A little while later he says: 'You are now talking to me in my home, but I'm actually in jail.'

'What do you mean, you're in jail?'

'The person who has stolen my identity is in jail. So, on paper I am now in jail.'

'That's strange. Couldn't they fix this error when they discovered the identity fraud?'

'No, because then they would have had to release him.'

'Weird.'

'My whole life is weird. At least, since the identity fraud. Before that everything was fine.'

What has happened to Ron Kowsoleea, is incredible. A criminal selling hard drugs passed himself off as Ron when he was arrested in 1994. Since then Ron remains registered as a criminal in numerous databases.

'The police and Department of Justice kept on promising me that things will be alright, but I kept on being arrested and handcuffed. Sometimes it happened on the street, sometimes at Amsterdam Schiphol Airport and once they raided my home. I was supposed to have been laundering drug money. A public prosecutor even suggested that I take another identity so that I wouldn't be bothered by this anymore. But I am who I am; I don't want to be anyone else,' says 52-years old Ron.

It all started with a summons. 'I had supposedly been arrested for a drug crime,' Ron says. 'I was dumbfounded, because I hadn't been arrested at all. I went to the police station. I can still see the incredulous look on the face of the police officer who had arrested

me a few weeks earlier. That's when they realized that the man they had arrested had given them my name. He was an acquaintance from primary school.'

The court promised to clean up his file and Ron thought everything was resolved. It seemed to be like that until he was arrested during a traffic control a few years later. 'I was handcuffed and taken away in a police van. You can't imagine what goes through your head when you know you've done nothing wrong. You get frisked and put in a cell. You need to hand over your shoelaces and your belt. "But sir, that's not me." "Yes, that's what they all say." And the cell door slams.'

When the police discovered that it was a case of identity fraud, the officers released him, with numerous apologies for the poor treatment. 'I just thought: finally, I can go home,' Ron says. When he says that his eyes well up with tears.

Because the government couldn't delete the false data in the computers, he was arrested over and over again. In total more than two hundred times. Ron says he has piles of compromising material against the government when it comes to identity fraud. I can look at it during our next appointment and make copies.

When we say goodbye, Ron says: 'I don't believe in conspiracy theories by the way. Otherwise I would have been broken a long time ago. I believe in myself. Do you know the song It wasn't me by Shaggy? That gives me strength.'

The first thing I do when I get home is switch on my computer. The email from Agent Digital has arrived, a report filled with sad and shocking cases of identity fraud. For example, Sven, who receives a telephone bill for thirteen thousand euro for one month's calls. His ID from his stolen wallet seems to have been enough to take out telephone subscriptions, loans and orders from mail-order companies. Sven can't buy a house because he is registered as a payment defaulter. And he can't sleep well any more because of that.

The consequences are also huge for 24-years old Niels. His new ID disappears in transport to the council offices. Scam artists register a company in his name. The damages have already run up to hundred thousand euro when Niels discovers the fraud. He gets heart palpitations and becomes depressed. His medical ailments mean he has to quit work and he lands in financial problems.

The policeman's list is rather long: a man in whose name a false benefit claim was made by abusing his social security number; a woman whose female neighbor made a copy of her keys and ordered numerous products in her name; a man whose vengeful ex-partner drew up contracts in his name and who eventually ended up seeing a psychologist because it is extremely difficult to cancel these contracts.

'Nice examples,' I mail the policeman.

He replies quickly: 'Now do you believe that this could also happen to you?'

'Maybe. I'm pretty careful.'

'So were those other people.'

'But can't you prevent it?'

'It's difficult. In any case check your bank statements for strange transactions. It often starts with small amounts. If you suspect that someone has stolen your identity, then disconnect your computer from the internet. And report it to the police.'

'It seems that most police officers are digital novices and that reporting such to the police usually doesn't make a difference.'

'Well, thankfully there are also good policemen among them. But the chance of catching those criminals is small. It's difficult to trace anonymous people on the internet.'

Agent Digital suddenly suggests something odd. 'Why don't you hire a hacker? Then you can see with your own eyes what these people are capable of. And another tip: make sure you find a reliable hacker.'

A reliable hacker? That doesn't sound logical to me. But the policeman is right: if I really want to know what is possible with regards to cybercrime and identity fraud, then I need to find someone who is deeply immersed in this topic, someone who can do things that the law doesn't allow. Let's visit a hacker.

After the email exchange with Agent Digital I have become more aware. I look very carefully at all the information I receive before clicking on anything. Cybercrime specialists are surprised how easily people pass on their information to criminals. It seems we all click on suspicious links. It is just too easy: you only have to log in to view a digital birthday card and the hackers get access to your details. A 24-years old hacker used this method to collect naked pictures from hundreds of computers, which he then published online with the names of the real victims.

But even if you don't click on infected links, even if you don't do anything out of the ordinary, you are not safe. People can easily pretend to be you and sometimes even apply for an ID in your name. That happened to professional football player Kwasi Appiah, who played for a Belgian team. When he moved abroad, an illegal migrant posed as Kwasi and said he had lost his ID. He used the new ID to apply for loans and sign contracts in Kwasi Appiah's name. When the real Appiah returned to Belgium, his ID was confiscated, and he was locked up for a month. The police thought he was the identity thief.

The idea of visiting a real hacker starts to grow, but I'm hesitating to do so. Who wants a stranger rummaging around in their computer and perhaps finding long forgotten sensitive information? On the other hand, a hacker might be able to find things I would like to know. For example, if my computer can be used to send spam. That is possible, because many computers are hooked up to criminal networks, without their owners knowing that. This means that they can also read your emails and look at your pictures.

You won't notice any of that, except perhaps that your computer is sometimes really slow. My computer is often slow. Or am I just impatient?

Trendwatchers predict that the free internet will blow itself up in the long run because of the increase of cybercrime. But I feel safe behind my computer, just like most people. The overwhelming idea that someone can find out everything about you with just a few clicks of the mouse is still far away. But I also know now that real computer experts don't take any chances: they re-install their computer every six months. Us digital novices are even too lazy to make up new passwords. Perhaps because we have no idea how vulnerable we are behind the screen. Infecting a computer and taking it over from a distance is a piece of cake. The victim only has to click on a link. Some hackers install a hidden key logger which registers all your key strokes and sends your passwords to the criminals. Such a program can also intercept your credit card's number after a payment, including card validation code and expiration date. If your password isn't strong then someone can reroute your emails and become you on the internet. This is possible because many services use an email to reset passwords. While you are reading this, someone can be buying things in your name or mine, taking out telephone subscriptions or even growing a cannabis plantation. Impossible? You usually discover it after a few months and sometimes after several years.

People who are employed are registered in thousands of databases. If you live like a recluse, your personal details will be stored in 'just' 250 files.

Why do companies want to know so much about us? To find the answer to that question I arrive at a pretty detached home in a quiet town. This is where a person lives who was prosecuted for violating privacy laws on behalf of different companies.

Michel Kraaij is a charming middle-aged man with a nice smile.

He spent six months in jail because he obtained personal details by deception.

'It's really not difficult to obtain information you're not allowed to have,' Kraaij says. 'I'm talking about all your bank accounts including balances, your private telephone number, your salary, how many cars you have, if you have debts, if you have ever been convicted of a crime… I carried out a research into scammers and murderers, but also celebrities.'

'And all that time you didn't realize you were doing something illegal?'

'I found myself in a grey area. If you know who your employers are, then you feel more or less that you are safe. The state attorney, all the large banks, insurance companies, well-known television programs and magazines. I was just a small fish and didn't expect that the Department of Justice would go after me and leave the rest alone. It was all so bizarre: I was in jail and the company I worked for just carried on with trading the information. I know now how flexible the law is. Wait, I can show you,' Kraaij says and he stands up and walks away. He comes back a little while later with a bunch of files.

'Look, I saved everything.'

Kraaij takes out various faxes and letters. Fortis Bank asks for an overview of a man's bank balance and wants to know if he is wanted by the court. Obviously, this is not information you can obtain via the legal channels. A ministry wants to search for the assets of someone who sold contaminated ground. The letter states that: 'The Fiscal Research Department has tried to find out if the financial details of V. can be obtained via the usual legal channels. This was not the case.'

'You see?' Kraaij says. 'The ministry writes that they can't get the information the legal way, so I have to do it illegally. They offered me 2.500 euro if I could do this within three weeks. I was ready

in four hours. I had his address, his bank accounts, their balances, the license plates of his cars. You only have to say that you are a colleague from a different department and that your computer is down. They will give you anything you ask for. There have been only a few times when this didn't work, but that wasn't a problem because five minutes later I could get the information from one of the other departments.'

Kraaij shows me more letters. 'Here I had to trace a criminal's private telephone number. As you can see from my notes, I succeeded and charged twenty euro for that. I phoned the telephone company, the department which can access private numbers, and pretended to be a colleague from the debt collection department and asked for his telephone number and address. Simple isn't it? Everything is registered in databases.'

'Is it still so easy to access personal information?'

'Without a doubt.'

Kraaij receives a telephone call. After a few minutes he hangs up. 'I'm sorry, I have to go.'

When I leave the house, I feel discomfort at the fact that it is so easy to gather someone's private information.

3

The perfect hacker

Who are the hackers? The first name that comes to mind is Anonymous, probably because they carry out mass attacks on networks of well-known companies. In my imagination these types work completely off grid. The last thing I expect is for someone from Anonymous to contact me because of a blog I wrote. He sends me an email saying he has a scoop, a hack at the Department of Justice. If I want to publish that? I give him my telephone number and he calls me almost immediately. When I hear what it's about, I refer Anonymous to two colleagues who work at newspapers that can afford good lawyers. But I also use this chance to tell him I am trying to find out what hackers can do.

'Do you mean how to hack someone? Usually it's not that difficult. You send some files to the computer which mislead the firewall. Then I can read everything, all your emails and see all your pictures.'

'That's kind of creepy. But I understand that it's more difficult with an Apple.'

'That's right. A Windows computer takes me ten minutes to get into, an Apple computer fifteen.'

Silence.

'So, you can hack my computer?'

'Is that a challenge? It can be quite risky for you.'

'Yes, but someone has to be the guinea pig to describe how it works and if it is so easy. As far as I know, there are no other volunteers.'

'Hmm, personally I've never been asked to hack someone's computer. I usually choose the victims myself.'

'So? Shall we meet?'

Anonymous agrees to meet me in a café.

Once I've hung up I start to get second thoughts. Who says he can be trusted? I find it quite scary: meeting someone I don't know in an internet café and giving him the key to my personal life.

After thinking it over for a day I make the decision: I'm going to find another hacker, someone who can be easily traced afterwards if something goes wrong. And I'm not going to meet up in a café somewhere. I would prefer the hacker to invite me to his home, because then I have his address.

When I tell my husband that I want to have my computer hacked, he looks at me in a shock.

'Hacked? Have you gone mad? Before you know it all your personal details will be out there for everyone to see. And then your friends and thousands of followers on Twitter will be sent those links they need to click on. You should't do that.'

'I know, but I want to know from personal experience how the hackers work.'

'That's quite a risk you're taking. It's insane.'

'It's all theoretical, the hacker won't actually do anything with the information.'

'And you believe that?'

'Yes, I do. We will agree to it before we start.'

My husband doesn't look happy. 'Please be careful,' he says. 'People sometimes change their minds, despite the best of intentions.'

In my search for the perfect hacker I look at dozens of social media profiles. Whom can I trust? I sometimes enlarge their profile picture, but from experience I know how little facial features actually say about being trustworthy. Cold stare, thin lips, stiff appearance: often it's just between your ears. A friendly-looking person could actually be a very smooth criminal. After I also read some stories about rogue hackers, my doubts increase. Emma's story especially upsets me. Someone has been stalking her and threatening her for some time, but she has no idea who it is. Her assailant mails

her an 'action plan' which says that she will be tricked into going somewhere by a girlfriend and will then be raped. The assailant has also published a sex advertisement with Emma's telephone number on the internet. A friendly hacker is helping her to gather as much information as possible. He is the only one helping Emma during this difficult time. She no longer trusts her best friends.

When the date of the proposed rape comes closer, Emma goes to a secret address. But she also receives threats there. That helps the police with their trace, because the friendly hacker and her parents are the only ones who know the secret address. During the first police interview the hacker denies everything, but the net closes during the second interview. His motive: he can't win Emma's affections the usual way, so he hopes she is attracted to him as a helping hacker. He is given community service and three years' probation. Emma continues to have nightmares for some time and needs psychological help.

After such a story I wonder if I won't get into trouble if I give a hacker carte blanche to rummage through my details, of course assuming that he can get into my computer. I continue my search, but with less enthusiasm.

I already follow dozens of hackers on Twitter, and Rickey seems trustworthy to me. His profile states 'High Tech Crime/Forensics.' He writes blogs that I can understand as a digital novice and that is why I'm confident he can explain everything to me without using too much jargon.

I read somewhere that he writes 'criminal brought to justice' about himself. That's striking, he has been convicted and must be honest to share this with everyone.

I send Rickey a message: 'Were you convicted for hacking?'

He doesn't take long to reply: 'Yes.'

'Can I speak to you about that? It's for a book I'm writing.'

When I get Rickey on the phone, he is indeed very open. He is

not embarrassed about his conviction, he sees it as a youthful transgression and as a life lesson.

Rickey's story is quite unusual. He started hacking computers when he was sixteen years old. He read 'Hack the world' somewhere and these three words stick in his head. Hack the world. He makes a start by hacking all the Dutch universities. When he has 'done' them all he moves into Europe and then into America. Hack the world.

Rickey can get in anywhere, has passwords and email addresses of students, can change grades, can do anything from a distance. But he doesn't, because his aim is not to cause damage, his aim is to 'Hack the world', just to prove that no one is safe from him. A kind of boys ego-trip.

Rickey's dream is to become a digital detective to solve cybercrime. He thinks it won't do any harm to have some experience on the other side of the law. He doesn't even believe that he will be caught. But the FBI follows his trail and calls in the National Criminal Intelligence Service. They raid his dormitory room at 6.00 a.m.

At first, Ricky thinks it's a joke, he doesn't see himself as a criminal. When he hears that he might be sentenced for six years, and his whole world collapses around him.

'Six years! Even though I was extremely well behaved for a hacker,' Rickey says. 'The only thing I did wrong was free up some server space for friends, so they could download films, music and games for free. I didn't give them any passwords for the networks, I only switched on the computers for them at night from a distance. I didn't watch most of those films and I've never been a gamer, so I hardly profited from it.'

Rickey is classed as being a danger to the state. The judge, however, sees things differently. He concludes that in the long period awaiting his trial, Rickey has shown that he is not a criminal. He

gests only a three months' suspended sentence, with a probation period of one year.

'I'm still on probation,' Rickey says.

Wow, I think to myself, the perfect hacker. If he hacks my computer with my permission then he cannot be arrested, but if he abuses my details, then he will go to jail, because he is in his probationary period.

I could kiss Rickey, but of course he doesn't know that yet. First, I need to get him to work before I can rejoice that I have found the perfect hacker.

'Can you hack any computer?'

'Why do you ask?' He responds with some suspicion.

'Just wondering, curiosity.'

'Perhaps not every computer, but most of them if I have enough time. I can't type very fast and I'm not good at games, but computers and I understand each other. The current generation of hackers doesn't even have to understand the computers, because there is a huge amount of software out there to carry out the hacking and steal data. Most hackers I know are very young and they think they are invincible. I recently warned a 17-year old boy. 'They won't catch me,' he said. We bet on it for a bottle of beer. He hacked a database with private details of police officers and published it, including their bank account numbers and telephone numbers. They found him. I won the beer.'

'You're still on probation, but you continue to keep in touch with people who break the law.'

Rickey sighs: 'I belong in the hacker scene. But I don't feel the urge to do it myself.'

'And if someone asks you to hack her computer?'

'Hmm. Why?'

'To see what hackers can do and how they go to work.'

'That's a dangerous plan, I'm on probation.'

'If I give you a written permission to hack my computer, then that's not illegal.'

'I need to think about it,' he says.

When I hear from Rickey a few days later that he will do it, I jump with joy all over my living room.

My husband looks at me incredulously. 'What is wrong with you?'

'I've found the perfect hacker: he has a criminal record and he is on probation.'

'That doesn't sound so perfect,' my husband says. 'I think it's a ridiculous plan to have yourself hacked and then to let someone with a criminal record do it.'

'Probation, dear, that's the magic word. That gives more protection than a 15-digit password.'

'I don't believe you got any further than a five-digit password'

'I'm up to seven now. I've added two numbers.'

'Your date of birth probably?'

'Am I so predictable?'

'Half of humanity is predictable.'

My husband is really strict when it comes to computer security. He makes up ridiculously long passwords and even remembers them. Every time he switches on his computer, he has to type in his extremely long password. I get frustrated just looking at it.

'I'll secure my computer better before I have it hacked,' I promise.

'It's better if you put most of the sensitive information and photographs on a USB-stick and delete them from the hard drive instead of securing it,' my husband replies uptight.

4
Careless authorities

The next time I ring Ron Kowsoleea's doorbell, he has prepared a pile of important documents. All proof of how he was degraded from a pharmaceutical wholesaler to a drug criminal due to identity fraud. Ron shows me a lot of letters and faxes: from the Dutch Anti-Fraud Agency visiting his business associates to discredit him, to the Public Prosecutor who says it is impossible to check in which government databases a citizen is registered.

'I find it impossible to comprehend that the government has no insight into what the government registers,' he says. 'This has ruined my life.'

Ron points to an adjoining room: 'Come, I want to show you my archive.'

As someone notorious for throwing things away, I look in surprise at all those boxes and files.

'Wow, do you keep everything?'

'I have to. Keep and sort, that is the only way not to drown. The government is a star in losing documents, but I have them all. The Dutch Anti-Fraud Agency raided my house and took everything away. They thought I didn't have any more records, but I also store everything digitally. So, I printed it all out and sorted it.'

When I dive into the topics of cybercrime and identity fraud I come across many careless authorities, who don't seem to care about good security of privacy-sensitive data. Some examples are even ludicrous. The members of parliament in Brussels receive a very easy to guess password when their accounts are updated. This is the first letter of their surname, followed by the first letter of their first name and a standard word. If you know the name of the member of parliament, then you can read all his/her emails. A couple of

members of parliament tried it out, and yes, it worked.

The ease with which databases can be hacked is also astounding. It almost sounds like a joke: what is the easiest way to get into a government website? Ask a civil servant for their login details. And yet it happens. Two students pretend to work for a council which is working on improving its computer system. Within a few hours civil servants give their passwords to the students without batting an eye and with that they have access to the computer system.

The amount of personal data that companies have from us doubles every three years. Security is usually an afterthought. This is how a leak in the control system of the public broadcasting corporation meant that two million personal details such as names, emails and functions were out in the open. By leaking just one password it was possible to access the websites of 160 television companies and radio stations.

LinkedIn messed up with an iPhone-app which means that people's private email addresses were made public, even those of Barack Obama and Bill Gates. And Sony proves that even large companies don't have their privacy affairs in order: the account details of millions of PlayStation users were stolen, because Sony didn't encrypt the passwords.

The most embarrassing data leak is probably that of YouPorn, one of the most popular websites in the world. Via a poorly protected server, thousands of emails and passwords are made public. Many people use the same name or the same password for other, non-pornographic websites and are identified as an 'enthusiast'.

Experts claim that there are only two kinds of companies: companies that are already hacked and companies that will be hacked in the future.

A lot of companies collect data about us, even if we are not their customer, Experian for example. On the basis of that profile numerous companies decide if they want to do business with me. The

question is how reliable these kinds of databases are, and what happens if your details are incorrect. I easily come across someone who has been affected. Ralph Hupkens wanted to take out a telephone subscription. This was not possible because he had a 'negative credit rating'. This was based on the previous occupant of the home he owns, but that was never updated in the system.

When I ask for my file from Experian, I see that telephone companies have asked for my financial status numerous times. Thankfully my details are correct. The old man who lived in the house I bought before me apparently paid his bills on time, because I never had any problems with his digital shadow. Except that I continued to get bills and letters in his name for several years.

I am curious whether Kraaij, as a dealer in personal data, knows about Experian. He has experience with a company which was taken over by Experian. 'I parked my car outside the door and asked for specific information, not even under my own name,' Kraaij says. 'During that short time, they had traced my license plate, because they came to tell me that I wasn't Mr. Van den Berg. That was the first time I found out how much companies know about me, even when I use a false name.'

As a dealer in personal data, Kraaij also knew a lot about the people he had to trace. 'When the police suspected me of fraud and tapped me, the information the agents were hearing was too much to handle,' says Kraaij. 'My file counts 1200 pages, including the taps. Do you want to see a few? They clearly show how I got my information.'

I grab one of the police taps.

'What? An employee at the Employee Insurance Agency gives you 150 national insurance numbers during just one telephone call?'

'Yes, I was on the line for about 45 minutes writing them down.'

'Do you need such silly people to get lucky?'

Kraaij looks insulted: ‘No, most employees I speak to are very helpful. I just let them talk so I don’t arouse too much suspicion. Once I thought a name belonged to a man, but it was not true. When I called the employee, he said straight away: "You don’t sound like a woman." ‘I’ve recently had gender reassignment surgery,’ I replied. I coughed a bit and adjusted my voice. Then I got the information I requested.’

‘Hmm, a gender reassigned trafficker in personal data.’

‘Why not?’ Kraaij laughes. ‘Lately, companies have been paying more attention to their customers’ privacy, but I am certain it’s still possible.’

5
Anti-hack measures

The day I agreed to meet Rickey comes closer and I become more nervous. Just to be sure, I change my password. It's not going to be so easy now. I didn't think it would be that easy, because I didn't use a regular word, but according to my husband I could do much better.

Computer specialists are surprised how often people use regular words as passwords. For example, 'secret', 'password' or 'access'. Randomly choosing a word out of the dictionary offers just as little protection, because hackers have computer programs which first screen all the words in the dictionary. If a hacker deciphers your password, then this key usually fits on numerous 'doors', because many people use the same password for different sites.

You can insure yourself against identity fraud. One of the insurers advertises with the text: 'You are unique, make sure it stays that way.' Yes, I am unique, but it's no longer that difficult to clone me if someone steals one of my passwords. If I want to prevent this, then in the future I would need to swallow a special pill. I know this sounds crazy, but technology is moving at a fast pace and experiments are already taking place with a password pill. You only need to swallow it to get access to your computer or your bank account. Even though I am a strong advocate of 'let's make things easy', I am hesitant to swallow a pill with a chip and a transmitter. It's a neat invention that your stomach acid acts as fuel to the minuscule computer, but I still think it is weird that I more or less need to be robotised so they can't steal my identity. Of course the inventor has a more attractive story attached to the experiment: the password pill prevents fraud and saves us time. It seems that on average we log in 39 times each day. And if you belong to the group of heavy computer users, this can add up to 100 times each

day. I have no idea if I belong to the heavy computer users, but my husband has set up my computer in such a way that I need to log in each time. For security reasons of course, but that means that each time I have emptied the dishwasher or read the newspaper I need to enter a password again. Thankfully I only need to type seven digits and I can type the password in blindly now. So, I'll hold off on the password pill for now.

As an alternative I could consider getting a tattoo with sensors and an antenna. How cool do you want to be? The creators think that mostly young people will be interested in this, a cool tattoo which remembers all your passwords. And which the parents will probably hate, but then again, that only makes it more attractive.

I don't know how secure my passwords are for hackers without a password pill, but it seems I'm not safe from a police wiretap. There are programs which, based on your social media contacts, calculate the chances of you being tapped. With 23.000 followers on Twitter and thousands of contacts on LinkedIn and Facebook my results are not that surprising; 100% chance that I am being tapped now or will be in the future. The Public Prosecutor always has to give permission to tap someone, but you don't need to be a suspect yourself. Just having regular contact with a suspect is enough. I am often approached by vague people via social media. And I always respond, because I don't want to seem arrogant. If they write back again, then I respond again, even if I try to stop the conversation in a friendly way. Can you create suspicion by linking innocent information and interpreting things wrongly? The experts are unanimous in this: yes. Tunnel vision in the Department of Justice is not a new phenomenon. And there is more and more data available which can be linked. So, 100% chance that I am being tapped now or will be in the future? Perhaps that shouldn't be a surprise, but I am still alarmed by this result. As a conscientious citizen this type of vulnerability creeps me out.

I don't like the idea that the government can read what I am typing and see each and every website I have visited. Out of curiosity and for research purposes I sometimes land on dubious sites and I'm curious what kind of risk profile this gives me. My son played a game on my computer and in a few mouse clicks he landed on a site selling all different kinds of weapons.

'Cool, mum, I've never seen so many weapons'.

I didn't think it was cool at all, but I bet it's in my risk profile: 'she also visited a site selling weapons.'

As a good citizen I still think that my chances of ending up in jail are zero, but the Netherlands has the dubious honor of all EU-countries of making the most arrests of innocent people. In ten years' time we have all paid € 79 million in damages for people who were wrongly put in prison.

6
Plundered

Rickey sends me a message: 'What kind of computer do you have?'
'An Apple.'
'Then I'm not sure if it will work. I'm specialized in Windows. Not that the Apple computers are that more difficult to hack, but I've never done it.'

I think quickly. Everything seemed to be ready and now my dream hacker is about to abandon me. I suddenly remember that I still have an old laptop which runs on Windows. Why didn't I think of that earlier? That hardly contains any sensitive information.

'I'm going to send you an email from a Windows laptop,' I say to Rickey. 'That will be your target. I don't use it for wireless internet and it is also password protected. That might make it more difficult for you. Tonight, I'm first going to delete all my naked pictures.'

'Don't bother. I ALREADY HAVE THEM,' it says in capital letters on my screen.

Joker.

I check to see what is on the laptop: a lot of holiday pictures, but for the rest no important information. My son has just started writing a paper for school. Quite an unusual subject: the woodlouse. Rickey probably isn't expecting any information on woodlice. I am starting to enjoy the thought that he will come across this kind of information. A few hacked woodlice, that won't do any harm. Rickey will learn that male woodlice are in big trouble, because the females can give birth without mating. Another funny fact: woodlice drink water from their behinds. I hope this will amuse Rickey, because I'm going to delete the pictures.

At that moment the phone rings. My smile soon disappears when I hear how upset my friend Marjan sounds.

'They've emptied my bank account. What should I do?'

'Who are "they"?'

'As if I know,' Marjan replies. 'During online banking I got an error message on the bank's website. I logged in again and a little while later all my money had disappeared. I looked up on the internet how this was possible. I probably had a Trojan virus in my computer.'

'And you didn't enter your details in some phishing email?'

'Of course not,' Marjan protests. 'Who do you think I am? The bank's website also seemed fine. It was encrypted. I always pay attention to that.'

I asked how Marjan got infected with a Trojan virus. I know her as someone who is pretty careful, she doesn't just click on strange links. But you find infected links everywhere, even trusted websites of national newspapers were infected with a virus which the unsuspecting visitors spread like wildfire. Perhaps Marjan also got infected by a virus on her computer from a trusted website. Criminals can easily use such a virus to spy on her internet usage and siphon away money when she does online banking. A virus scanner doesn't recognize the newest malware. The € 1.000 that you transfer has suddenly become € 5.000 and the receiver's account number has been changed.

The European Union Agency for Network and Information Security (ENISA) says that banks must work on the premise that all computers are infected, but they don't. They are becoming more stringent and shifting the responsibility to the consumer, because internet crime is costing them enormous amounts of money. Dutch banks even demand that you check your balance when you are on holiday, at least every two weeks. Otherwise you are 'grossly negligent' and in the case of fraud you can even pay for the damages yourself. But most people don't read the small print which says they need to log in every two weeks.

I think it's ridiculous that banks oblige us to use computers when we are on holiday. Being offline for a bit is great. Besides, many people use wireless connections which allows cybercriminals to easily intercept your entire data traffic and then consumers are once more the victim.

Until recently I refused to take laptops and iPads on holiday with me, but I've given in. Not because I can check my bank balance by the way, I still don't, but I've noticed that people expect you to answer your emails and also reply to questions on social media, because most people do. Many people are addicted to their inbox and that has even been given a name: internet addiction disorder, a psychological condition. I am not addicted to my inbox, but the reason I also start to check this during my holiday is that I will otherwise have to deal with hundreds of messages when I come home. I can't dump everything in the virtual bin, because there are also important mails, but you can't find them if you don't go through everything. The person who figures out a way to pick out the important mails from the junk mail will probably become a millionaire.

Of course, you can set up a standard 'out of office' notice, but that is only sent once you have received an email and that email will still be waiting for you. I am a promoter of a more radical solution: when somebody sends an email, he receives for example the message: 'This mailbox is closed until 20 August and all emails will automatically be deleted.' I admit this doesn't sound very friendly, but if we all do it then it will soon be accepted as the norm and then we can all calmly go back to work when we come back from our holiday, without having email stress. Bill Gates gets about four million emails each day and he has hired an entire department of staff to select and organize these.

About 70% of all email traffic is spam, but thankfully most of the providers hold back the most evident ones. Yet I still delete

suspicious emails on a daily basis. When I receive another one my eyes stay fixed on the content for a little while longer. This mail is so badly written that it's almost endearing.

'Dear customer,

When discovering we irregular activities, to help us crime prevent, we must to confirm your identity. This means proof that you are and where you live. In first instance, make used of an online verification and if this is success, that is all we need to do. With regards to this click HERE your identity to confirm.

Internet Support Team ABN Amro Bank.'

With a smile on my face I delete it: such a poorly written email will probably not even persuade an 80-year old digital novice to give his login. Yet the cybercriminals are often successful, even after a poor translation.

Money is nowadays nothing more than data stored in electronic bits and bytes. Whoever controls the computers, controls the economy. The banks accept billions of cybercrime losses each year so that they don't lose the customers' trust.

Another 'ping'. A warning appears on my screen that criminals are sending fake emails on behalf of ABN Amro Bank. The bank asks for cooperation, for control purposes I must enter my old details. Of course, this is another email sent by the hackers, only this time the writing is professional. This time more people will fall for the trick and their bank accounts will be plundered. This happens every day, despite all the warnings.

I sometimes long for the good old days, when phishing was an unknown phenomenon and spam was so innocent: cheap Rolexes and pills for endless erections. Modern spam is very tricky. You follow the news about a concert and suddenly you see a link on Twitter with pictures. Great! When you click on it you don't see pictures at all, but advertising. You click it away, annoyed, and think there's nothing wrong, but that one click has given them access to your

computer. And then you see yourself sending tweets about diet pills. Before I realized, I had already infected some unsuspecting victims, who in turn infected other people. And with just 23.000 followers, this is still fairly innocent. Lady Gaga's account was also hacked. Her millions of followers received tweets which promised free Apple products. Within a short space of time thousands of people clicked on the infected links.

If you think spam is innocent because most intelligent people delete it, then the statistics about the sales as a result of spam are probably an eye-opener: € 160.000 each day. And that is just the profit for one spammer: the Russian network Glavmed. Whoever clicks on one of those links usually allows his computer to send out more spam unnoticed. A small network can send a million spam messages in an hour. The Spanish police rolled up a gigantic spam network: 12 million infected computers in 190 countries. The police called the three Spanish people they arrested 'very normal', none of them had a criminal record.

Such a network is used to force important sites offline and blackmail companies, until they pay. They earn millions this way. While we lock our front doors to keep burglars out, we don't do that when we are online. That is why more and more criminals are turning to digital burglary. There are enough open doors. Some people don't even know how to close those doors, others still think that it won't happen to them. Meanwhile, cybercrime became more lucrative than illegal trade in marihuana, cocaine and heroin combined. If the fraud industry were a state, then it would be the fifth strongest economy in the world.

My bank account can be plundered, my bank card can be copied and even my car can be cloned. The license plates of a friend of mine were stolen from his Renault Twingo. He discovered that a day later and reported it. He then received high fines for speeding violations which he had to pay, because he had been too late in re-

porting it. The thieves had also used the plates for a black Twingo. Exact the same car with exact the same license plate: try to prove that it's not your car.

Identity fraud is lucrative and difficult to stop. I know only one case where it wasn't lucrative. A car driver gave the wrong name and date of birth during a traffic control in The Hague. The result: it turned out to be someone who had seven unpaid fines.

7
Famous

The lady visits a hacker… Rickey calls me and tells me that he isn't available on the date we agreed. That's a bummer, because he's going to keep me waiting longer now. We set a new date for our appointment.

I voluntarily want to be hacked, but if I were a malicious nerd, then I would rather hack a private banker who just got a € 1 million bonus, instead of an author who earns € 1,50 per book. Of course, I'm not the only one who can figure out that you can get a lot more from those people. Two Americans write down the names of the richest people from the magazine Forbes, then they gather a lot of personal data about the celebrities such as Steven Spielberg and Oprah Winfrey and finally get their credit card numbers. How do you access the computer of the rich and famous? I'm not sure, but the chance is great that they just use the name of their favorite pet plus, for example, their wedding anniversary as a password. Most people share lots of personal information via social media and all their preferences lead to tips about possible passwords. Celebrities might share less information about their private lives, but they are often interviewed, and all those crumbs of information lead to useful tips when you bring them all together.

The fraud comes to light when the 32-years old mastermind behind it wants to transfer $ 10 million from one of his victim's accounts. Of course, it's stupid that you try to transfer that in one sum, as a non-nerd I would have divided it into smaller less obvious amounts.

The bank becomes suspicious with that amount and that leads to an investigation. The arrest wouldn't look out of place in a film: a policeman crawls through the open roof of the moving vehicle into the criminal's car. The officer cuffs him, while he is hanging upside

down.

You don't have to be a hacker to become a millionaire with the help of a computer. A Belgian harbour custom's officer discovered that you can do this with just a few clicks of the mouse. Tim D. had financial problems but suddenly he was ordering champagne costing hundreds of euros per bottle. Gossipmongers whisper that he is in the drugs trade, but no one has an idea of what and how. Until the Department of Justice starts to investigate after receiving a tip. And so they discover that shipping containers filled with drugs are leaving the harbour without being checked. Tim D. is given information in which containers the drugs are hidden and ticks the box in the computer to say they have been checked. After that the container can be picked up by the criminals without any problems.

Up until now many people have proven how simple cybercrime is in practice. Hackers have more and more tools to mess up your life. But many hackers don't, they call the criminals 'crackers' to distance themselves from them. It would be interesting to meet an 'ethical hacker' to find out what is so ethical about hacking. After a Google search I decide to choose Jeroen van Beek. On the CNN website I read that a few years ago he was able to mislead the scanning machine at Schiphol Amsterdam Airport with a false passport. The passport had a photograph of Elvis Presley and Jeroen had manipulated the chip in such a way that the scanners verified it. It's quite a nice joke to appear in front of customs as Elvis Presley, firing up the beliefs of people who believe the King of Rock-'n-roll is still alive.

Jeroen is waiting for me in a restaurant, he has his laptop open to show me how easy it is to hack a person or a company. 'If you don't do daily updates of your computer programs, then you are vulnerable,' he says. 'The easiest thing is to send someone an invitation through the mail for something they might be interested in.'

'How would you know that?'

'I would send you an invitation to the Book Ball from your publisher, because I know you write books. Would you open it or not?'

'Probably yes.'

'Then I can get into your computer, I can read all your emails, see all your passwords and maybe even find a copy of your passport. Many people have saved a copy somewhere in their computer.'

Hmm. Mea culpa. The last time I had to send a copy of my passport to a company, I didn't delete it from my computer.

'Do you have your passport with you?' Jeroen asks.

'Yes, but why do you need it?' I am starting to become more and more mistrusting.

'I just want to see it.'

When I give him my passport, he looks at it and writes something down. He then puts my passport closed on the table and puts his mobile phone over it. It only takes a few seconds, then Jeroen shows me the screen on his mobile phone. The inside of my passport has been scanned, even though the passport was closed!

'Look,' Jeroen says. 'Everything is in high resolution, I can easily make a copy.' He enlarges my photograph to show me.

I am too surprised to react. I stare at my photograph and suddenly realize it's in color while my passport photograph is just black-and-white. I open the page to check. It's correct.

'That's weird, you've got my picture in full color.'

Jeroen smiles. 'Some digital copies are better than the original papers. My mobile phone just read the details that are included in the chip. They once thought that the chip would make passports safer.'

'Aha.'

'By the way, passports are well secured compared to numerous access cards for companies and institutions. If I copy the chip from one of those passes and put it on a blank pass, then I would have unlimited access, for example, to government buildings.'

'Is it that easy?'

Jeroen nods. 'The blank cards can be bought everywhere, you can download the software for free.'

Jeroen isn't only hired to hack computer systems as a test, but also to get access to offices with fake passes.

'You should see the incredulous looks on management's faces when I gain access,' he says.

'How does the management know they can trust you? You could be stealing sensitive information.'

'That's correct, they don't. I have a certificate of conduct, but otherwise…'

'Otherwise you are not to be trusted.'

'If I were you I wouldn't trust any hacker. And certainly not hackers who say they can be trusted,' Jeroen smiles. 'But in my case, it's easy: I have a good job, earn enough as a security consultant and this way I also don't get into trouble with the law. If I make one mistake then my good life is over.'

I have to go to the toilet. I always leave my handbag on the ground, but this time I take it with me. All those cards in my bag and someone who can scan them in the blink of an eye doesn't seem a good combination. Trust is good but prevention is even better, at least that is what Jeroen just tried to explain to me.

'I want to show you something else,' says Jeroen when I come back. 'How careless companies are with your personal data.'

He types into Google something with 'filetype:pdf paspoort site.nl' and '1900'. The entire screen is filled with personal details and copies of passports. I am dumbfounded, especially when I see the name of my notary on the list.

I point at his name. 'I know this office. That is where I signed the contract of sale for my house.'

'That's a coincidence,' Jeroen says. He zooms in.

'What an idiot, he hasn't secured his computers well at all, look:

driving license numbers, passports, addresses. On such sites you can find everything companies ask when they want to check your identity.

I can't believe it, my notary in his fancy office. Perhaps I should send him an email that I didn't pay him thousands of euros to leak my data.

Jeroen isn't surprised. It's business as usual for him. 'At least half of all databases have leaks,' he says.

'Half? But then our personal data isn't safe at all?"
'Correct.'

While we are still talking, the waiter hands me the wireless pin machine to pay the bill.

'Should you be doing that?' Jeroen asks. 'Wireless means that anyone with a laptop can intercept the signal out of the ether. How do you know they won't intercept your pin code?'

'I was once given a very good tip, I first type in an incorrect pin. Then I know for certain that I am connected to the bank.

'That's smart, but it is also no guarantee, because they could also intercept your pin code at the second attempt.'

'Sure, but the waiter wouldn't like it if I didn't pay.'

After meeting Jeroen I am suddenly very careful with my ID. The influence of an ethical hacker! I haven't even been hacked yet and I am already starting to change my habits. But it's not easy because numerous companies ask for a copy of my ID and I don't know when that is obligatory and when it is not. How they do save the copies, so they don't fall into the hands of criminals, is unclear. Most victims find out too late that their identity has been stolen. Their friends receive emails they didn't send, amounts are charged to their bank accounts for products they never ordered, they get a letter from a bailiff or their application for a mortgage is rejected because of debts they are unaware of. It can also be discovered in numerous other ways, because people suddenly find themselves

registered as living at a different address or they discover that someone has applied for benefits using their name, has made a new social media profile or has added files to their computers that they don't know about.

I am afraid to gift my old mobile phones and computers to charity since I read how easy it is to recover deleted information. The entire address book and text messages on my mobile phone can be retrieved. Even wiping your computer is rather useless, seeing as everything can be retrieved using a simple internet tool. The only thing that seems to help is breaking the hard drive, but that is quite a radical way of staying in control of my personal details.

I look at my old computer in doubt. Am I brave enough or not? I want to get rid of it, but I never thought about a violent parting. We have had some good times together. And yet, I must do it to protect my own privacy. I walk to the garage and grab a hammer.

'Mum, are you really going to do it?' my youngest son asks.

Yes. A good way to warn my children of the digital dangers. They will probably disregard my well-meant advice, but a mother with a hammer should impress them.

Here we go, first screwing it open, taking out the hard drive and then hitting it as hard as I can. After a few hard blows it is in pieces. My children look at me incredulously. When I put the hammer down they come to me to inspect the damage.

Everything is now gone, even the manuscript of my first book. I must admit that I am finding this hard: some unusable things have a sentimental value, even for someone who throws everything away.

'So, this is the only way to protect your privacy?' my youngest son asks in a timid voice.

'Unfortunately, it is.'

'Are you going to do that with my computer when it is outdated?'

'Probably.'

He looks at me with a bit unhappily face. I'm glad it made an impression, perhaps now he won't ask for a new laptop sometime soon because the other one is becoming slow because of all the modern games they play nowadays.

I write on social media that I destroyed my old computer and that I am also working on a cybercrime book. The reactions flood in. One woman asks if she can call me. When I give her my telephone number she calls straight away.

'I'm in trouble. My ex has all sorts of things delivered to my address,' she says.

'But can't you return them?'

'That's all I do. Washing machines, beds, sofa's. You don't want to know how angry the delivery men are. As if it's my fault.'

'Have you been to the police?'

'They can't help me, because I can't prove that my ex had all these things delivered. They won't even let me file a report. Once I had to pay cash on delivery costs. And I think this is just the beginning.'

'Why is he doing that?'

'He wants to be part of my life one way or the other. My ex has now applied for driving lessons using my name, which you are obliged to pay. If you don't, they will send the bailiffs. At the police department they just shrug their shoulders and say that this happens often, and they can't do anything about it.'

I can't give her any good advice. Further enquiry at the Central Hotline Identity Fraud doesn't provide hopeful information. 'In the case of identity fraud, the police often don't file a report. Even though creditors demand such a report. It puts you in a catch-22 situation.'

Good to know. I must make sure I don't get a vengeful ex. Perhaps I can avoid that, but what about non-exes who do this? Just because they can easily get your details from the Chamber of Commerce if you own a company.

One of the people who responds, frightens the life out of me. 'I got a phone call from Vodafone on Monday afternoon,' writes businessman Dirk-Jan Huizingh. 'Good afternoon Mr. Huizingh, a strange question perhaps, but did you order three new iPhones last week with subscriptions and did you place a lot of calls this weekend?' Of course, I hadn't done that. First, they connect people and then they verify it, very handy. Amount of money lost: € 3.000. Vodafone had an authorization form with which I authorize a Roy K. to act on my behalf. With a signature which did not match my signature at all. Roy had also sent Vodafone a scan of my passport. The joke is that I don't have a passport, I have an ID card. It couldn't be any more fraudulent, but apparently it worked. The phones were delivered to my office address. Roy waited for the courier and signed for them. The courier scanned his ID. I thought this would be an easy case for the police, because now we knew who Roy was.'

When I read that I get the idea that the case was more difficult to resolve then at first glance. Dirk-Jan confirms my suspicions. 'I took all this information to the police to report a crime. Two weeks later I received a phone call. Mr. K. was already registered in the police database because of other fraudulent practices, but they couldn't find him. How can someone be untraceable? Within a few minutes I had found his father's mobile phone number on internet. But the police didn't think it necessary to contact his father. I did. His father wasn't surprised. The last thing the police said to me? 'Unless you are hurt, for example because this man abuses your identity again, then we can't do anything about this.'

Unbelievable, someone gets my details from the Chamber of Commerce database, whips up a false passport, sends it to Vodafone, who doesn't even bother to check my signature and then I go to the police, who also seem to have other priorities. And then they're surprised that hundreds of people are victims of identity

fraud every day.'

Identity fraud is also getting easier, because there is so much information about us. Databases are quickly linked to each other. Even if you reply anonymously on an internet forum, they often know who you are. A large website sends me a letter from a commercial organization which wants to use their files for 'scientific analysis'. The letter clearly explains how the company will do this: 'When users of numerous websites have made a profile or account then these can be linked by using the email address, user name or IP-address. On the basis of these linked profiles systematic data from these people can be gathered.' The letter confirms that many well-known forums have already given this company permission to analyse their users' data and to find out who is behind the anonymous profiles. I doubt the 'scientific 'character of a commercial company, but apparently this is not something the administrators are questioning before they hand over our data.

As soon as I go online, all sorts of trackers become active. They are placed on most sites and follow closely what I do. They save every bit of information about me. Many companies earn scandalous amounts of money by selling my personal data. This is the largest hidden economy on the internet. We don't know exactly what all those companies with mostly unknown names collect. Well-known sites admit that they don't even know with which third parties they share the data. Do I have a choice? Hardly. Sometimes I refuse to accept certain cookies and then a site says: tough, for you there are ten others who don't mind their preferences being saved. With sites which I deem trustworthy, I accept the cookies, but how reliable are the webmasters who have no idea what advertisers who track me do with that information? According to the law they are obliged to tell me. That is difficult if you are not aware.

Imagine you knew that many unknown companies were collecting data about you behind the scenes, would you still click on 'yes,

I accept your cookies'? Perhaps more people might start to think twice. Or perhaps not, because that is what experts call the 'privacy paradox'. People are concerned that trackers follow their every move but click without hesitation and without further reading on 'yes, I accept cookies'. We accept far worse things out of naivety and ignorance. Every day many people fall victim to identity fraud. If you think this mostly happens to people who aren't very smart or less educated, then you will be wrong. They are also among them, but it is the well educated people that fall into the trap twice as often. There are very smart people who do stupid things with their computer.

8

Among the Hackers

Almost all machines and devices become more and more advanced, but also dangerous. I don't think of television having viruses, but most modern TV's can be hacked just like a computer. 'Simple' machines such as a printer have become wireless and so someone with bad intentions can send print jobs from a distance or get a copy of documents printed previously. A webcam can be accessed from a distance. A criminal can be watching you even when you are not using the webcam. The rise of wireless connections on nearly every machine is hard to stop and that gives some surprises.

A lady meets a hacker and asks him:

'What did you do today?'

'I hacked a toilet via Bluetooth.'

'What, we're not safe anywhere nowadays! But wait a minute, I don't quite understand. Why does a toilet need a Bluetooth connection? Whoever thought of that can go flush himself.'

The Japanese manufacturer Satis came up with a luxury toilet which you can flush using an app. I have no idea what the advantage of this is, but as soon as this was publicized, the luxury toilet was hacked. Not that it is too drastic: you can't do much with a toilet except make it flush continuously. According to the hacker nowadays more and more machines communicate with each other, so why not the toilet? The internet itself also looks a lot like an unfiltered sewer.

Hackers can turn your heating up and down in your house, open your garage door from a distance or switch off your home security system. Just try to figure out how that works. Many elderly people don't understand it at all. They are gifted an iPad, so they can keep up with the times, and are given instructions how to visit their

grandchildren's Facebook pages, but they don't get any information how to protect themselves from cybercriminals. Apparently, we think they are old and wise enough. Perhaps they are, but not when it comes to modern machinery. I am sometimes busy for hours trying to explain a gadget to my grandmother and then she still looks at me glassy-eyed. She eventually gets it, but a week later she has forgotten how it works.

My grandmother is no exception. I had to laugh when I read a recent newspaper article about an old lady who kept on calling the emergency telephone number. The woman was pressing the buttons on her television remote control, but it wasn't working. Instead of the remote control she had her mobile phone in her hand. When the police visited the woman, she was relieved that her remote control wasn't broken!

Ten years ago, there were about 50.000 computer viruses. That number has risen to 40 million. Making and selling viruses has become a lucrative business. But who are the makers? To find out I manage to get a ticket for a leading hackers conference. Looking at the price of the ticket I see that it's not a place for wannabe-hackers, because they will probably not be keen on spending hundreds of euros on a ticket.

As a journalist I come in many different places, from prisons to chocolate factories, but this time I'm very curious. Hackers have mythical proportions in the eyes of a digital novice. With rows of numbers and codes they can rob large banks for millions of euros and knock out an entire country's information systems, as happened in Estonia and Georgia. No one can find them, because their servers change address and location every few minutes and stay untraceable.

The possibilities for hackers are virtually infinite. They don't only work on the wrong side of the law but are also contracted by governments. Everyone is secretive about this, but many coun-

tries gather information for cyberattacks. Targets are services which affect many citizens, such as banks, the telephone companies and the electricity grid. It is very telling that conversations have already been held between the United Nations, America and Russia about limiting the use of internet for military purposes. Digital warfare is really not that difficult. As a secret service you just make up a game, such as Angry birds. Millions of people install it on their smartphones and give you unlimited access to all their contacts, network traffic and GPS details. They don't look to see who the maker of the game is and in whose hands all this information lands. They don't even ask why you need these details (usually not for the game to work properly, but the game makers still ask for the information and they get it). Many people download free apps. These apps gather heaps of information about you. They practically have access to everything, from your agenda to your contact list and from personal details to your location. That is why you see adverts from companies in Amsterdam when you are in Amsterdam. If an app-maker refuses to send your location to advertisers, then he will get paid at least 50% less.

My smartphone often connects to different servers around the world, because it has some common apps on it. I knew that, I just didn't know how often this happened until the British television channel, Channel 4, looked into how many details consumers 'leak'. A smartphone with 30 common apps exchanges information about 350.000 times per day with servers all around the world. This data is mostly passed on to advertisers. A telephone which lay on the table unused, makes 30.000 connections in less than an hour with servers in the U.S., Ukraine, Singapore and China. Each app wants different information, but some know the unique IMEI-code on your telephone and can constantly track your whereabouts.

Without realizing it we have become extremely dependent on

mobile phones and computers, because we can no longer live without them. Hospitals, ports, airports, police departments: they function because of computers, which often run on Windows without the latest security updates. Terrorists or hostile countries which can take these over, have our society in a stranglehold. In various cities, the control of bridges and locks can be taken over by malicious-minded people. Drinking water facilities, power generators, the transport and the chemical industry often work with outdated computer systems. Hackers can easily disrupt these systems with a simple attack.

Servers which are used for criminal purposes are often registered to unsuspecting citizens. This way the criminals erase any trace of themselves. Security expert Kapersky says: 'How do you find a Chinese hacker who set up Russian spy software on a server in Tonga and saved the stolen data on a provider on the Cayman Islands?'

I hope to find those hackers at an international conference, because according to the press release there will be hundreds of hackers attending from all around the world. It does sound exciting: a lady among the hackers, as if I'm going undercover. I would rather blend in, but I have no idea what hackers wear or don't wear. I'm sure Google can help me and I type in my question as clearly as possible: 'What do hackers wear?'

Google apparently has a nervous breakdown, because instead of information about preferred types of clothing and accessories I get tips for decorating my bedroom, a news item about the death of a well-known hacker and even a link to 'Islam for Dummies'. I have rarely seen such a confusing and curious top-10. To avoid delving into Islam by accident, I leave Google for what it is and look in my closet. The reason I always think carefully about what I'm going to wear has to do with a journalistic trauma. When I had just started in my profession I had to sail along on a container ship for an article. Without thinking about it, well I put on a skirt. I never realized

you needed to do a lot of climbing on a container ship. The male crew helped me a few times, but they mostly found it more interesting to stand at the bottom of the ladder. Try climbing a ladder and keeping your legs together. Since then I think carefully before putting something on that suits me, but not the job at hand.

My assumptions about hackers are that they all wear glasses and are scruffy. I haven't worn glasses since I had my eyes lasered and when I open my closet there are not many items which fall into the 'scruffy' category. I still love high heels and pretty dresses, even though they are not so short any more.

In the end I grab a black pair of trousers and a green sweater. Very simple, but I think it will be suitable. I've rarely looked so plain and spent so much time in front of the mirror. Hoping that hasn't been for nothing.

Before I leave the house, someone rings the doorbell. A parcel. The address is correct, but the name is not. Before I can tell the postman that, he has disappeared. That's great, now there's nothing else to do but open the parcel.

I unwrap a new laptop. Another computer in my home, over my dead body! Our family is computerized enough, so I don't believe someone ordered this laptop from mail order company Wehkamp. But who did? The name on the invoice is the same unknown woman with my address. I suddenly remember that I read something about a trick with wrongly delivered parcels. And then the doorbell rings. The same delivery man appears at the door.

'I just delivered a parcel, but that's for someone else.'

'Yes, but I saw that the invoice uses my address.'

'That's a mistake, I already have the correct address.'

'That's fine, but I'm not giving you the parcel.'

'Why not?' the delivery man looks at me perplexed.

'I'd prefer to return the parcel myself. Then I have proof.'

'But that will cost you money, you'll need to pay the postage

yourself.'

'Otherwise it will probably cost me a lot more money. Have a nice day.'

The man becomes angry. I no longer doubt that this is a scam: everything is pointing in that direction. Well, 'everything' is just a wrong name, but linked to my address it can mean that the mail order company comes knocking on my door for the bill. It's your own fault if you hand over delivered goods to strangers. Anyone can pretend to be a delivery man.

9
Vulnerable

‘Switch on your webcam!’

‘No, I won’t.’

‘Then I’m going to hack your computer. Of course, you can also just switch on your webcam and give me a striptease.’

‘You’re not serious!’

He was.

Thankfully this never happened to me. It did happen to an acquaintance. Her hotmail was also no longer working. The hacker had read all her emails and sent her another message.

‘Strip for me and I will give you back your access.’

Some hackers hack websites for personal data, they read your emails and blackmail you if they come across delicate messages, they amend the text on your website or make the entire content disappear.

The problem is that they can get into your computer through so many different ways that it is nearly impossible to defend yourself against everything. For example, they use the names of your friends on Facebook and send you a message. When you click on it, the computer installs software that enables the hackers to copy all your important details. Research shows that most internet users will fall victims to cybercrime sooner or later if the current trend continues.

The hackers conference takes place in Hotel Okura in Amsterdam. I arrive just before lunch. When I think of hackers I think of people who quickly eat a sandwich so they can get back behind the computer, but in the Okura there is no such thing as a simple lunch. There is even caviar. It looks like the hackers aren’t keen on that, so I eat a lot of caviar for lunch. In the meantime, I try to inconspicuously check out everyone who passes by. The scruffily dressed hackers are in the majority, but I also see a lot of men in

suits. And there are just as many hackers with glasses as without glasses, talking about assumptions….

An international competition is taking place in a large room. Teams of three hackers per country have been given tasks such as hacking a website as quick as they can or downloading a program and guessing what it does. 'Hacking is nothing more than understanding how something works and using that in a way they don't expect,' says Dirk van Veen, who is keeping an eye on things on behalf of the organization. The hackers stare at the computers and try things out. Rows of numbers and codes sweep past. They started yesterday, and they do this non-stop for eight hours each day.

'Won't they get square eyes?' I ask.

Dirk shrugs his shoulders: 'Well, they already have.'

I see that many hackers are drinking something I don't recognize. When I look at the label I understand why it is so popular here. It contains five times more caffeine than a cup of coffee and they probably need this to keep their eyes open after hours of computing.

At first I am afraid that I won't be able to follow the technical explanations of the top hackers during the presentations, but although I don't understand all the codes, I do understand how it works. In one of the rooms they explain how you can hack cameras which people use to secure their homes. Most are so poorly protected that it is possible to add an extra user from a distance to see what is happening inside those homes.

The home security systems are also easy to hack. Someone demonstrates how he can send thousands of false alarms at a time, so the alarm emergency call center and the police become confused. This means they won't go out to the real burglaries, because they can't distinguish them from the fake ones.

The scariest demonstration is perhaps that you can hack the software of an airplane. This way the hacker can take over the controls

from the ground.

Further along in another room there are mostly funky gadgets on show, such as a home-made 3D printer. I am given a pink plastic key. 'I just made it, for opening police handcuffs,' says 25-years old Peter-Paul.

'You mean for toy handcuffs?'

'No, it works on real police handcuffs. Doesn't look like it, right?'

'Not really. Can I test it?'

'There's a security guard walking around with handcuffs. Perhaps you can ask him.'

Armed with the pink plastic key I try to find him. The guard looks at me smiling when he sees me coming.

'You're not the first one,' he says. 'Someone else just came to test it. It doesn't look much, but it really does work.'

Right, a pink plastic key from a printer can open all police handcuffs. The world is changing, nothing is what it seems to be.

When I get home my husband shows me a newspaper article. The title is: 'Do you want to be hacked?' Because the writer didn't expect that anyone wants to be hacked, he gives lots of tips how to prevent it. For example, don't use 123456 as a password. Thankfully I don't. Every year hackers publish the most used passwords to help other hackers. 'Password', '123456' and '1234567' seem to have been favorites for a number of years. 'Jesus' and 'Ninja' also, but I wouldn't have thought of them. Jesus, I really don't understand who would want to log in with the word 'Ninja'. 'Welcome' also scores highly, because it is often the standard password in computers. If you don't change it, then hackers are indeed welcome.

I'm not that good at making up strong passwords. It should be something new at least five times in a row, not the name of your partner, preferably nothing that is legible for a normal human and it needs to include exclamation marks, numbers and letters and, if possible, it also needs to be 34 keys in length… sigh. It's nice

that security experts come up with these tips, but who is going to remember a password like that? Most people choose something simple. Research of Google shows that not only do pet names score highly as a password, so do the birthdays of their husbands or wives. That is probably because otherwise they might forget their birthdays. Less popular as a password than the names of pets, are the names of their own children. I have no idea if that says anything about the order of importance. The funny thing is, that the names of exes also score highly. I don't want to think about being confronted with exes on daily basis, but apparently there are enough people who like that. Or they change their partner so often that it's impossible to make up new passwords all the time.

I also find it difficult to make up strong passwords for many different websites. Of course, someone has made something for this: The Password Changer. 'Many people are not aware of the risks of passwords which can easily be deciphered,' the site says. 'Click on "start" and answer five simple, personal questions. The Password Changer will combine this information and show you a safe, unique and strong combination of letters, numbers and signs.'

I'm curious about the type of questions, but more so about the password the computer will advise me. Here is question number one: 'What was the name of your first love?' Eh, I can't remember, he didn't really leave behind a lasting impression. What should I fill in? Honesty lasts the longest, right? I fill in 'I don't know'. I wonder if the computer will register 'Idontknow' as a name.

Question two is possibly worse: 'What is your target weight?'. At a certain age you shouldn't ask that question, but again I give an honest answer: 57 kg.

Question three is another tough one: 'What is your favorite film?' There are so many films I like. How can I compare a nice comedy to an action movie? I decide to drastically limit my choice to the subject of cybercrime and fill in The Net, one of the first films

based on the internet.

'What is the name of your street?' the computer asks next. Finally, a question I can answer without having to think about it.

At last I get to choose my favorite symbol from a list. There isn't a great choice, from star to dollar sign and from percentage to exclamation mark. A question mark suits me better, but that's not on the list. Then it has to be the exclamation mark. And then my super strong password is ready: Str57!hetn.

To be honest, I wouldn't have come up with that myself. I can see straight away how it has been built up: the Str for the name of my street, 57 for my target weight (something to think about every day), the exclamation mark I didn't want and the abbreviation of the film title. If I remember that order, then it's not a bad password. But now I've revealed it, so I'll have to come up with something else.

Some people think up very strong passwords, but it still doesn't help. A young hacker, who has made a fake website and promises people on Twitter that they can see how much they have in common with their followers, shows how. When the victims sign in, the fake website gets access to their accounts. The screen states that the website is given access to tweet on behalf of the user, but for 20.000 people on Twitter that is still not a deterrent to leave behind their logging details. The hacker then sends a tweet from their account with the text 'How people poorly protect their Twitter account… regards, Damiaan Reijnaers.'

I don't think I'm careless on the internet and yet my website has been hacked. Everyone who visits the website gets a malware notification and Google puts me on some kind of black-list. Rickey?

When I contact him he swears it wasn't him. 'I'm not going to do anything before we meet,' he says.

That's great. I've arranged a hacker, but someone else hacked me faster. And I have no idea who. I know this happens to thousands

of websites, but one way or the other I still don't believe it will happen to me. Who is interested in a website with books, which doesn't contain any personal details or bank account numbers?

When I ask via social media who can help me close the leak, a few candidates step forward. That is what digital novices are good at: they surround themselves with people who are good with computers.

I give my password to the first whiz kid, with some trepidation, but I can't solve the problem myself, so I don't have much choice. Funny enough, the corrupted file is nowhere to be found. After several hours searching for it the whiz kid gives up. Then someone else takes over. But he can't find anything either. In the meantime, Google flashes a red screen which seems pretty scary. Now no one will want to visit my website. Time for heavy artillery. Are there really people out there who know a lot, and I mean a lot about computers?

A new group of experts contact me via social media. This time I've decided not to give my password to the first one who replies. Someone sends me a message that sounds good. 'I'm Holger, 40 years young, and I have been working with computers from 12 years of age. I was senior programmer at an IT company when I was 17. I speak more than ten programming languages, but my grammar is rubbish :).'

I feel brave enough to give my passwords to someone like that. So, Holger gets them. He gets to work straight away to see what is wrong and a little while later I get a message:

'You've picked up a virtual STD because a plug-in wasn't well-protected from the outside world. My plan of action is as follows: your site is temporarily offline, so that new infections can't be put back. Then I will ensure that the method they used to inject the virus onto your website is closed.'

A method can't be closed, but Holger already said his grammar

was poor and that he knows a lot about computers, so I trust him. A virtual STD? Holger is very good at explaining, because I more or less understand what he is going to do. He explains everything step-by-step. 'I need to read through every file in order to delete things which have been added to your site. This is very secure work. If just one is skipped over then it will infect the other files. Once I am confident I am ready, then I will make a back-up of your cleaned site, so we have something to fall back on if it is hacked again.'

'If it is hacked again? Well, I think once is more than enough. They can't keep on hacking me.'

'You never know in advance,' Holger replies. 'I have also done it sometimes, but I only test my own sites or sites with the knowledge of the administrator. Programmers usually make mistakes and the hackers profit from that. On average there are at least ten programming mistakes in every thousand lines of code.'

'And how many lines does a program have?'

'That depends on the program, but a bit of software has one million lines, and this can go up to 100 million lines.'

Wow, then ten mistakes per thousand lines quickly adds up.

Within a few hours Holger has discovered the infected plug-in and deleted it. I don't need to know all the technical details, but I am curious if I could have prevented this.

'It's difficult to say,' Holger replies. 'I think someone has used you as a test model, so they could infect larger sites.'

In any case I am relieved that no one has a personal vendetta against me. It is but one of the many viruses in cyberspace. Us. digital novices are the first to be hit and some of us are so naïve that they even pay for viruses. If you click on an infected link, you get a message that your computer has been infected and that only a certain type of software can remove the virus. The software is just a new virus, but people don't know that and gladly pay € 40 for it.

This deal has been so successful that the makers have had to set up special call centers to help those interested. In helping to install the new virus, of course.

10

Cyber lovers and fake people

Many people are influenced by other users' reviews when they buy a product. Me too, I won't buy something that has a bad review. I do find it confusing that reviews are sometimes wildly different. How can a hotel get a 1 from one guest and a 10 from another guest? And what do you do if some readers love a book while other readers think it is rubbish: do you buy it or not? People are herd animals, that is why other people's reviews are apparently important. If most people give five stars, then apparently it is good. That might be true, if it weren't for the fact that most of the reviews are fake. Companies sometimes use software which creates reliable fake people. They are given a full profile, including a made-up name, email address, website and social media profile. The software ensures that these 'social bots' place reviews which praise the company's products and complain about the competition's products. Research shows that many of the reviews for hotels, restaurants and mobile phones are fake and yet we let them influence us.

Even Wikipedia, the site that many see as a trusted encyclopedia, can't escape this. People are changing articles at the request of companies. A company from Texas had registered with 300 false identities to amend articles and thousands of companies are prepared to pay for such a service.

Companies use fake people, but fake people also use the companies, for example to phone on their behalf. The man on the other end of the line is from Microsoft and he speaks English with a thick accent. Digital leaks in my Windows software are causing problems, but thankfully he can solve that easily. I only have to follow his instructions. I think it will be easy to get rid of this scammer, because as an Apple user I don't have any Microsoft software. But

I am mistaken in the tenacity of the man on the other end of the line. He insists I do have Microsoft software in my computer and that I am in danger if I don't close the security leaks.

The entire discussion reminds me of the marketeers who phone you while you are eating your dinner and try to sell you a product you don't need. Of course, they can't know beforehand what I do or don't need, but with a little bit of psychological knowledge they can figure out if being pushy will be effective.

'Am I speaking with Mrs. Genova?'

'Yes.'

'I would like to ask you some questions about your computer. Recent research has shown that most people are poorly…'

'Sorry, I'm not interested.'

'May I ask why not?"

'I've already taken care of it.'

'But we offer you a free check.'

'That's nice, but I'm not interested, because not that long ago I discussed this with an expert.'

'It won't take you long, Mrs. Genova, and then you will know for sure.'

'I put a nice black sofa for sale on eBay yesterday. Are you interested in that?'

I hear silence on the other end of the line. The man is apparently confused. Good.

Then he says 'no'. But I already have his attention and I'm not planning on letting go easily.

'May I ask why not?'

The annoying marketeer ends the call as quickly as he can. Great. When the next commercial seller calls I am going to ask if he is interested in my son's bicycle. And I'm pretty sure I can think of other things to sell as well.

It's unfortunate that this strategy doesn't work for a fake Micro-

soft caller. The next time I'll just tell him that I don't have a computer. Of course, I can also just hang up, but I know people who have been called five times. I prefer to find a way that makes them so desperate that they will put me on a black list.

I am so focused on infected links that I immediately delete any suspicious files. Then I get an angry client on the line: it seems I deleted a contract for a lecture because I thought it was spam and all this time he has been waiting for my reply. The next time when I'm not so paranoid I'm sure it will turn out to be a phishing mail.

How far can you go? A swimming pool asks for my finger prints. I don't want to give them, so I may not swim there. Apparently, all those cameras they've put up there are not enough to guarantee my safety, only finger prints work. Criminalizing all customers to catch a few troublemakers, is this the future? That cameras follow my every move is just about acceptable, but finger prints to be allowed to swim, I find that a step too far.

As a married woman, at least I don't have to worry about cybercrime through dating sites. There you can find numerous criminals with convincing stories who steal money from naïve victims. The stories are quite diverse, but they always end the same way. A captain in the US army is in reality a Nigerian scammer. But before the victim discovers this, she has lost thousands of euros, because she advanced him funds in order to buy himself out of the army. In exchange for this, and as a guarantee, she was granted access to his pension rights (documents signed by an actual general, she had checked that).

The problem with internet is that it is often difficult to distinguish the good from the bad people. An acquaintance was dating a woman on the internet, but by chance found out that Dana was not her real name and she was much older. He cut short their new relationship, but Dana started calling him, sometimes 150 times each night. She set up accounts on his name and emailed all his

friends. She was eventually arrested and was given community service. Yet he is not certain that she won't do it again.

11

At a James Bond location

Is there such a thing as coincidence? No idea, but it's interesting that I am targeted by internet scammers while I am busy writing a book about cybercrime. They choose me as a victim because I put my car for sale. Mr. Laurent Gauthier wants to pay the asking price, because his wife has fallen in love with the car. I can imagine that, because it is an attractive cabriolet which has been out of production for some time, but I frown when I read his email. I don't believe that Gauthier wants to transport the car to Africa, because he is working there on a temporary contract. If you've ever been in Africa and saw the potholes in the roads, then you know why a four-wheel drive is better than a cabriolet. But I am curious how he is going to try to scam me, so I reply to his email. And then it comes: he wants a copy of the car papers and a copy of my ID. Of course, he also needs my bank account number, otherwise he can't transfer the money. Time to check if he is known as a swindler.

I don't get far when I just google his name, but in combination with 'car' I get a hit. People are discussing this man's modus operandi on a forum. It seems he's also bid on a Fiat Panda! Then you know you're dealing with a swindler, because who wants to drive a Fiat Panda?

Some people are further down the line in the transaction process than I am and have already received a copy of his passport and his wife's passport. Both are white. That was to be expected, the pictures are probably from a few people who sent a copy of their ID without realizing that they would go through life as a Nigerian. I am not certain if in this case Nigerians are behind the fraud, but this type of fraud is called '419 scam', named after the article in Nigeria's book of statutes. In any case Nigerians have embraced

this type of scam from the birth of internet. They even won the Ig Nobel Prize for Literature. A fun parody to show that internet entrepreneurs in Nigeria have enriched literature with colourful characters and have been able to reach millions of readers in a short space of time. Now, many years later, this kind of storytelling is still very much alive.

As I know the truth about Mr. Gauthier I am unsure whether to reply to his email. Of course, I can tell him I don't have a scanner, and perhaps he could advance the money so that I can scan my ID and other documents and send them to him. But something stops me from doing so. I know what it is: the fact he also bid on a Fiat Panda. That was too much.

Now I hope that someone else offers the asking price and that I actually get the money.

While I am waiting for my meet-up with the hacker, I ask myself how difficult it can be to pretend to be someone else. I already know that gathering information is more important than your technical skills. There is so much information to be found about people on the internet that I probably don't even need to search hard for it.

I choose a random person, a Mr. Hendriksen. I see he has recently set up his own company, because the Chamber of Commerce has put all his details online. I can use these details to take out business telephone subscriptions in his name and order a computer. The websites assume that the Chamber of Commerce has already checked his details. They will send the invoice to the known address, but I can indicate if I want the items to be sent to a different address. Very handy, because he just needs to get the invoice, not the goods. Let him prove he didn't order anything. The police won't help Mr. Hendriksen, nor his victims, because this kind of fraud isn't a priority.

I don't know the real Mr. Hendriksen and I will probably never meet him but trying to reach a victim of identity fraud is sometimes

quite difficult. Following a tip, I try to contact someone called Leo. He doesn't answer his phone and I send him an email asking him to call me back. Then I get a curious email.

'I wanted to phone you. But at the moment I don't have a bank account (closed by the bank), no money (no bank account) and no phone credit to make calls (no money). When your identity has been stolen, you are really in trouble. You keep on banging into brick walls. Can you try to call me again?'

'Fine, thankfully they haven't disconnected your internet,' I reply.

He replies a while later: 'They have. I can use my neighbour's wireless connection for free.'

I hear the next day how hopeless Leo's case is. It all started with a copy of his ID.

'I have no idea how or where it was made,' he says. 'They ask for a copy everywhere. Then it falls into the wrong hands and the problems start. Someone travels on public transport without paying for his ticket and gives my address for the fine, someone orders a credit card on my name, someone buys things using my name. Without knowing, I was placed on all kinds of black lists and the police came to arrest me. Of course, they first warned me that I had to pay the fines, but since I didn't know what the fines were for, I didn't pay. They arrested me at a network party in front of all my business partners. I guess they don't want to do business with me any more.'

Leo was detained for eight days in a police cell, it took his lawyer that long to prove it was identity fraud. 'We had a file full of evidence that I couldn't have been travelling on public transport without paying for the ticket, because at the same moment I was giving a lecture on the other side of the country.'

'What a nightmare.'

'My biggest nightmare has yet to start,' Leo says. 'The fight with the organizations to repair everything. Unfortunately, not everything can be repaired.'

I need some time after talking to Leo to process what he has said. Just a copy of your ID can change your life into a living hell. I don't want to think about all those companies that have a copy of my ID.

I find an invitation for a congress about cybercrime in my mailbox, it will be held at a KPN-data centre which stores much of our data. Visitors will also get a tour of the premises which outsiders usually don't get to see. I decide to attend.

The first speaker is very knowledgeable on the subject of computer security, but also has experience as a victim. Once he received an email from a friend that she has been mugged while she was abroad. He transferred the requested sum of money for a new passport and hotel as quickly as he could. Later on he discover that his friend wasn't abroad at all. Someone had hacked her email account and sent this kind of emails.

The speakers at the conference agree that most consumers have little knowledge of computer security, but what is even worse: companies are no better. Many computer systems are vulnerable, which can have severe consequences. A good example of this is Diginotar, which issued insecure certificates and disrupted whole branches. Court cases were postponed because lawyers couldn't accept the files, the government couldn't collect taxes, notaries couldn't register real estate transactions and no digging work could take place, because contractors were dependent on the digital map of the Netherlands which shows where all the cables and pipes are buried.

Just like physical security, real computer security is an illusion. One of the speakers told a true story to illustrate this: he had secured his new home with expensive locks. He then had a small crack in a window and in two minutes the glazier had removed the entire window. 'I looked incredulously at the big hole. Just like the glazier can gain entry to my home without any problems, so can I gain entry to a computer without any problems. Can I do that with every computer? Yes.'

Then it's time for the tour: with my own eyes I see how well protected the servers are in the enormous data centre. Of course, the doors are well-secured, and you can only enter with a pass. Above our heads are voltage tracks which feed boxes filled with data from two sides. If something happens to one set of cables, then the other seamlessly takes over. If the electricity network goes down, six high-tech machines with a six-ton flywheel take over. The flywheel can deliver about ten seconds of power, then a shackle closes, and the diesel generators start up. The generator room is very impressive, especially the noise.

There are cameras everywhere in the building, about 200 in total. With a group of ten people we are allowed to take the elevator to a higher floor. The doors close, but nothing happens and after pressing the button a few times still nothing happens. So, we take the stairs instead, it doesn't need to be that high-tech. As long as it is safe.

The heat all the servers produce is extracted to gigantic cooling towers on the roof. That is as big as a football field. When you walk between the grey cooling towers, you feel like you're on some kind of James Bond location. But I'm guessing you don't need to be James Bond to enter this server centre. A fake elevator repair man would also probably be able to do it. Security is as strong as its weakest link.

When I leave the building, I receive a text message: 'Congratulations! You are the winner of the day!' I have won an iPad and I am redirected to a website. Rather obvious spam, but how did the spammers get my telephone number? I'm afraid I will never find out, because there are so many ways to get telephone numbers. Some companies sell your details, others just protect them badly.

My mobile phone number can also fall into the wrong hands when friends link their contacts to an app. The free app 'Talk-

ing Tom Cat', where a virtual cat copies what you say, steals your phone number and sells it for advertisements. More than 50 million people have already downloaded the talking cat.

I delete the spam message and take a last look at the building where many of our personal records are stored. It looks very boring from the outside, just as grey and square as an average industrial warehouse. But I'm sure the digital James Bond knows how to find it.

12
Big Brother

Most people think that they have nothing to hide, even the people who do things that aren't quite legal. It is becoming easier to check if someone is hiding something. People on benefits who cohabit and don't report that, are committing fraud. The organizations just look at Facebook for clues or check on their water usage. Councils stop benefits if people use too much or too little water. Although linking such data might lead to major errors, the greatest dangers come from a different corner. All those databases, often poorly secured, make us vulnerable. New kinds of viruses try to steal our identities. The Pixsteal Trojan for example focuses on photographs on computers. A scan of a driving license or passport is then easily transferred into the hands of criminals. Sexy pictures are used for extortion.

I have nothing to hide, but privacy is much more than doing things the law doesn't allow. It is the freedom to decide for yourself what information you hand over and also the right to do what you want without every step being traced and registered.

Unfortunately, the free world isn't so free anymore. Our freedom is affected by protecting us against terrorists who hate our freedom. That reminds me of George Orwell's Big Brother, but then everyone thought it would remain fiction. Orwell's book 1984, written as a warning against totalitarian regimes, seems to be a popular read again. Quite strange when you think the book appeared in 1949. The famous phrase 'Big Brother is watching you' comes from that book. Big Brother in the book is the almighty leader who also watches what people are doing and saying. With whom I am speaking on the phone, for how long, who is sending me a text message, which words I google… he can follow each and every step. In Orwell's time it was incredulous to think that there would be cameras

hanging everywhere to keep an eye on us. But now it is all fact and we are used to it. In the Netherlands, there are more than 200.000 cameras keeping a watchful eye in public spaces and in buildings. The number is much higher when you add in companies and consumers. In America, the police wear helmets with cameras so they can quickly scan the citizens' faces. The motto is: 'Don't tell me who you are, we'll tell you.'

As a good citizen I assume the cameras won't be used against me. But you never know. A Dutch politician who had sex with a colleague in a parking garage, saw it all back on the internet. A Belgian mayor was also embarrassed by a film on YouTube which showed her having sex in a romantic spot. The cameras used by the police, councils and even amateur filmmakers are constantly watching us without us realizing. When something is leaked, only by then that we realize that there was an intrusion in our privacy.

Nowadays every citizen is presumed to be suspicious. The government is checking us more strictly, but more unobtrusively than ever. This doesn't lead to a better society, because the feeling of insecurity has actually increased. Why doesn't the government trust us? I'm really not interested in what our minister of justice is doing with his computer and I also don't ask him to give some DNA just in case he ever does something wrong. Yet this is what the government now wants: total control in advance. The Rotterdam police collected license plate numbers from innocent citizens and saved these until they were reprimanded, because it was against the law. And so, they changed the law: the police are now allowed to do that. It is also possible for the Department of Justice to access our medical details, just like it is possible for police to hack computers. It's funny that the Minister of Justice thinks that is a good way to catch criminals, as if experienced cybercriminals don't have programs to arm themselves against it.

Computer security expert Ronald Prins understands why the

police want more digital authorizations. 'Otherwise their investigations draw a blank each time,' he says. 'Cybercrime is very international. If you want to dismantle a botnet, because thousands of infected Dutch computers are attached to it, then you need to submit legal requests in different countries. That doesn't work. That is why I understand the need for the police to be able to hack computers. At the same time, we need to make sure that those authorisations don't become too broad and start to threaten the security of citizens.'

Prins' worst nightmare is probably the American wiretapping service NSA and I have to say that I was also quite shocked by his behaviour. He gave me his email to make an appointment and who did I email? Right, the NSA. 'That joke impressed many people,' Prins says.

'How did you get an NSA email address?'

'I bought it fair and square for 139 dollar. The only difference with the real one is that my NSA email address ends in '.org' but most people don't notice that.'

That's true. I hadn't noticed it at first either. I thought that Prins had gotten the NSA email address via a back door. Now I know you can purchase this legally, I think it would make a nice birthday gift. I might then also get rid of all the spam, because I don't think they send those spam mails to the NSA.

Now that I know more about cybercrime I notice how easy it all is. You really don't need to do much to become a victim. Boudewijn Duijvesteijn received a letter from the police that he had to report to the police station for violation of the opium law. A mistake, he thought. But the police took his mugshot and his fingerprints. He was then questioned for hours. They asked him if he knew a certain address, if he was growing hemp and if he knew people who did. He has no idea what they were talking about. He was sent home, but a few months later he was questioned again about hemp

farming at another address. This house had also been rented on his name. As a suspect he noticed how easy it was to have the evidence point towards you. Good friends started to doubt him, and even his own girlfriend asked him once: 'You didn't do it, right?'

'You can't imagine how powerless you feel at that moment,' Boudewijn says. 'Especially if you also receive an electricity bill for more than € 15.000 and they register you as a payment defaulter. Then you ask yourself: what is all this, how is this possible?'

Boudewijn knew he was a victim of identity fraud, but he didn't know what he could do about it. He also knew how it had happened: the criminals used a copy of his passport to do various things using his name. 'How did they get a copy? I have no idea,' he says. 'As a citizen you leave behind a copy in numerous places. Like many people, I also kept a digital copy of my passport in my computer. Looking back on it, that wasn't so safe.'

People are not rational beings. We often know what is good for us, but we don't do it. Everyone tells us that we shouldn't keep a copy of our ID on the computer and that we shouldn't use the same passwords everywhere and yet we do. When I try to secure my computer, I am just like a goalkeeper in football. Research has shown that professional goalkeepers know they have the greatest chance of stopping a penalty if they stay in the middle of the goal area. But they don't: 94% dives to the left or to the right. This way the goalkeepers try to show that they did their best. As a goalkeeper of my computer I also do that: do things that I know are not smart. Such as forgetting to delete a copy of my passport after a company has asked for it. I wrote an article for a magazine recently and their financial department wouldn't pay the invoice without a copy of my ID. I'm sure it's a legal requirement as I get this question from nearly all of the magazines I work for. I just don't know where all these copies disappear. I usually delete them from my computer after a while, but I wonder if the magazines do the same. I'm pretty

sure they don't.

In the end Boudewijn is charged for drugs and has to appear in court, including an expensive lawyer.

'Thankfully I was acquitted, because their evidence wasn't strong enough for a conviction,' he says. 'But the consequences of identity fraud are still visible. I can't be accepted as a volunteer with the neighbourhood watch team and my registration as a payment defaulter has not yet been expunged. The worst thing is the looming threat. You never know when it will start again. They already have a copy of your ID and there is nothing to stop them using it again.' This is the biggest nightmare for many people: you have an invisible enemy and you don't know when it will strike again. Someone submits fake tax returns with your name and you only notice when you receive a message that your bank account number has been changed. But then it's too late, because everything you have been reimbursed has already been withdrawn from the bank in cash.

What you also see is that entire online shops suddenly disappear. One of the thousands examples is digitalshop-online.nl. The strange thing is that before the online store disappeared it had well-known internet certifications, which weren't even fake. 'I'm upset,' writes Jack, who spent hundreds of euros on a mobile phone. 'Internet certification and checked the Chamber of Commerce number, looked at reviews and checked to see if the payment methods were good. Everything seemed legitimate.'

Another well-known method is recruiting home workers to receive returned parcels and relocate them. The employer wants a copy of your ID for the contract. And then it starts: he sets up a fake email account with your name and orders numerous things using your name. The mail order company brings the parcels and you sign for them because you think these are the retuned parcels. You label them with the stickers which the employer sent you. The parcels are sent abroad, and you get the invoices for laptops and

iPhones. They were delivered to your address. And even worse, you signed for them.

The Dutch Foundation Opgelet receives many complaints from people who have been scammed this way, but the police can't do anything to help them. They see a trend in the abuse of identities. Scammers look at sites such as eBay to see who is looking for what and respond to them. They don't need to pay a deposit they just want a copy of the buyer's ID. And the clueless buyer doesn't think this is a problem. But then the games begin. The identity thief makes an email with the name of that person and sends hundreds of emails to people who are looking for something. He has all these items for sale and can prove he is reliable, because he mails a copy of his ID and the name is the name in the email. He also gives a bank account number with the same name, because banks no longer take the trouble to check if the name belongs to that account. The bank account numbers belong to intermediaries who reply to advertisements about so-called home work. It sounds complicated, but it works without a hitch and thousands of people fall into the trap. When victims contact the person whose identity has been abused, he knows nothing. The real swindlers are usually untraceable.

In the future many banks and other important companies will be disabled because the cybercriminals, thanks to naïve citizens, will have control over a growing number of zombie-computers. If I buy a simple blender, I get a whole book with safety certifications, instructions and warnings, but if I buy a computer, it has absolutely no security against viruses or malware. The message is clear: figure it out yourself.

With my limited computer knowledge, I have to install a good antivirus program and firewall and also play system administrator, because with a new computer it is standard that everything is set to 'open'. How am I supposed to do that if nobody has explained to

me how it works?

I might be from the old generation that hasn't grown up with computers, but what my sons learn about digital security at school is also very limited. When I give lectures at schools, most teenagers raise their hands when I ask if they would sell me their bank card for a foreign transaction if I pay them well. Those that don't raise their hands can't explain where the danger lies. Welcome to the modern society where young people grow up with computers without seeing the dangers. If they allow their bank account to be used for such a transaction then they are an accomplice in whitewashing criminal money, because that is what it is used for. Of course, their bank accounts are also emptied. In one of the classes a boy raises his hand and says: 'I won't do it, because my brother lost 2.000 euro this way.' Then all eyes are on him, because everyone wants to know how his brother could have been so stupid. But just a short while ago most of them didn't think it was a problem to loan someone their bank card in exchange for money.

13
Digi-stalker

Social media show many examples of identity fraud, of people who pretend to be you by setting up an account under your name. Sometimes that is just annoying, but other times it is disgusting. A politician in the Netherlands who was outed as a paedophile, has written on his profile: 'Let's see how I can get some interesting followers. Dear children, I have a whole room filled with toys! Follow me on Twitter and perhaps we can meet up. It will be our secret.' Of course, this is a fake account that has been used with a real picture.

The victim often isn't aware there is a fake account. I also don't know that a fake account has been set up using my name until an acquaintance tips me off: 'That's not you, right?' Well no, but @MariaGenova3 looks exactly like me, because my picture has been copied from my website. My profile is quite complete, because the link to my website also works. I have for more than a year a digital stalker, who is also probably the creator of my fake profile and uses it to share nonsense. One of my colleagues, Rhija Jansen, has her photo copied off the internet, this person pretends to be her and asks women if they want to collaborate on a book about love. In just a short period of time this man has entrapped a number of women and they tell him every detail of their sex lives.

But it could be worse: someone publishes racist tweets on your name, that 'Muslims at university make you sick'. This shocks you, but what frightens you the most are the reactions to the tweet: 'Natalja Laurey, I will slit your throat when I find out who you are. I will cut you up into little pieces.'

It's not that difficult to find out who Natalja is. The culprit uses her real name and photo, copied from the university website. Natalja is stunned that it is so easy to clone someone digitally and so

difficult to revert is. Her fake account was deleted in a matter of hours, but when she googles herself she comes across racist comments she never made.

Social media enlarges everything, sometimes unfairly. When you are reading a boring story and asking yourself why so many people recommend it, the explanation can be very simple. An author confesses: he paid for all those people's reviews. Just two dollars per hour gets you a botnet, which spams thousands of people with the story.

One of the dark sides of social media are the people with bad intentions who twist your words and people who have an opinion about you without ever having met you. I don't respond to malicious people, afraid of being entangled in an endless discussion. But not responding doesn't help with people who get their satisfaction from bullying other people and ruining their reputation. My digital stalker makes so many other victims that he seems to be a professional. Even though I completely ignore him, and I have blocked his account, he continues to write about me, things like 'Maria is a stupid Bulgarian cow' and 'Genova has blood on her hands.' This man even alludes to me having connections to a Bulgarian gang which commits fraud with rent allowance. Not that I have ever had a rent allowance.

After hearing my story, a police officer says that it would be wise to file a report. It seems there are no police officers available in my hometown for this specific issue, so I am referred to the neighbouring town.

I hope to meet a detective specialised in these cases, but when I see that the police officer belongs to 'the older generation' I fear the worst. Of course, these are assumptions, but unfortunately my assumptions are often correct.

'Do you understand how social media work?' I ask before sitting down.

'A little,' the police officer says.

That doesn't sound comforting. Especially as he has already started to file my report and asks if 'tweets' is a real word.

Half an hour later, and we haven't made any progress. The officer doesn't know if it is possible to file a joint report on libel and stalking, because linking things up in the old police computer system isn't easy. It takes him ages to find the right entry field. At a certain point I have to tell him where the incident took place.

'On the internet,' I say.

The officer stares at his screen. 'That option isn't available. Shall we fill in your home address?'

'My home address? The stalker isn't harassing me there.'

'I understand, but I have to fill something in, otherwise the system won't let me continue.'

I am not being harassed at my home address, but that doesn't matter, as long as we can file the report.

14
Identity Fraud

Many of the government databases are linked, but that doesn't mean that mistakes are automatically passed on. Michel Savelkoul at the Central Hotline Identity Fraud knows all about this. 'Sometimes the cases are horrible,' he says. 'We have been working on a case with a man with 51 criminal offences to his name without having ever broken the law. He kept on being arrested by the police and was even subjected to an armed raid at home. They also arrested him at airports, because he was registered in the database as a criminal and payment defaulter. He sometimes had to pay a fine just to enter the country.'

'Is that Ron Kowsoleea's case?' I ask.

'No,' says Savelkoul. 'This is another man. I actually think his case is worse, because it nearly killed him. The man was extremely embarrassed because he kept being arrested by the police and he didn't talk about it to his friends or colleagues. His own wife eventually left him, because at a certain point she no longer believed in his innocence. Because why are you in trouble with the authorities so often if you say you are doing nothing wrong? How can you convince other people that criminals are using your identity and that this can carry on for a long time? We eventually managed to clear his file and he received an official apology from the Department of Justice. The words "You are not guilty" written on paper were extremely important to him, probably more important than the compensation he received.'

According to Savelkoul, you don't have to be particularly careless to become a victim of cybercrime. 'That's the scary thing, it can happen to anyone. Victims are usually chosen at random. Savelkoul is annoyed with large mail order companies: 'They don't do much to protect their customers against fraud. A few years ago,

the telephone companies started with debiting one cent from your account when purchasing a mobile phone as a preventative measure, and since then they are no longer on top of the fraud list. Many mail order companies refuse to do this, because they are afraid they will lose customers in the ordering process. But that one cent can prevent me from ordering something in your name.'

'How easy is it to order something in my name?'

'Easier than you might think. I know people who ended up paying the bill, because they didn't want to appear in court.'

According to Savelkoul, most of the victims he meets are unable to prevent themselves becoming a victim. 'Unless they take drastic prevention measures, but you can't expect that from regular citizens. We see the strangest of things: even people who have pretended to be other people and eventually receive official confirmation that they are that person. Then you have the people who are registered as payment defaulters, because someone has ordered things using their name or taken out a loan. They often aren't aware of this, but if they want to buy a house they find out that they cannot get a mortgage because they are registered as a payment defaulter. You usually only get a couple of weeks' time to arrange a mortgage. Before the fraud is resolved, you can lose your dream home.'

Savelkoul says most identity fraud is invisible and elusive. 'If you lose your passport, then scammers will stick other details on top of it. Then they can pretend to be Maria Genova in Nigeria or Argentina for example. You have no idea how many clones of yourself are out there and what traces they leave. You just need to hope that the police don't come to arrest you for crimes that you are not aware of.'

'I can't imagine that there are clones of me, it sounds weird.'

'Most people don't believe that they are cloned. We recently had a case about a man who couldn't imagine it either. Someone had used his passport details in Spain for criminal activities. The

scammer didn't look anything like the victim, but the fraud wasn't discovered. When the Dutchman went on holiday to the Canary Islands (which belong to Spain) he was taken to the police station for questioning. He wasn't the only victim. The offender used 26 aliases.'

Everything someone needs to steal your identity, can be found online within an hour. In many countries, identity fraud is one of their biggest problems at this moment.

The 26-years old American Rogelio Hackett, lived on stolen credit cards for 10 years without being noticed. He spent 36 million dollars. Hackett obtained the credit cards via hacking, but of course you can also say that a dog needs a credit card. That sounds absurd, a dog with a credit card, but you only know it is possible when you try. It started with an email address that a man set up for his dog as a bit of fun. Clifford J. Dog soon received an offer for a credit card. The man returned the application form and didn't withhold information that it was a dog. Apparently, no one bothered verifying the information: the dog received a credit card.

How can someone manage to buy something with just a fraction of my details, for example just my name and my account number? Jeremy Clarkson, the host of the popular TV show Top Gear, thinks the fuss about data breaches is hyped and publishes his own account number in one of his columns to show that troublemakers can't do anything with it. Within just a little time a large amount of money is debited from his account. The money has been transferred using a one-off authorization to a charity. The bank can't guarantee that this won't happen again.

A well set-up hack is nothing more than social engineering: finding out what the victim is interested in. If I share something on social media about electric cars, then it's probably quite easy to send me a mail about the newest electric car. Sometimes it's just luck. I recently drove to the airport to pick up a friend and I received a text

message that she had already arrived and was waiting in the Hilton hotel. I was just about to click on the message to see why she wasn't waiting at the gate when I hesitated. I read the text message again. Just a regular case of phishing, but perfect timing!

Later on, another one, this time via my computer: 'You have exceeded the storage limit of your mailbox. You will not be able to send or receive new mail until you upgrade your email quota. Click the link below to upgrade your account.'

Why did I hesitate with such an almost standard phishing mail? Because not that long ago I received an email that I was close to exceeding the 'storage limit' on my website and that was a real mail. I paid an extra ten euro and received extra 'storage'.

I can't blame my naivety when even my husband, who is ten times more careful on the internet, recently forwarded me an email: 'Can you translate what it says, it's something in Bulgarian and you still speak ik fluently.'

'Not Bulgarian, but a Russian spam mail, just throw it away,' I mailed back.

But my dear husband had already clicked on the link, because he couldn't read the message. He trusted it, because it had been sent by a good friend.

'And now? He asked. 'Is my computer infected because I clicked on the link?'

'I have no idea, but that's enough to install malware on your computer. And then they can do a lot of things from a distance, such as stealing your passwords and your pin codes for internet banking.

I am very curious whether Rickey is able to hack me. When he e-mails me a file I don't open it, because I already know what he is planning. He probably knows that he has to come up with something more creative. I don't doubt the hackers' creativity in any way, because I read about the most bizarre hacks on the internet.

Some are so strange that I wonder if they are real. What about a sound sculpture being hacked? In a video a councillor in the town of Enschede in the Netherlands explains what has happened: the hacker had replaced the bird sounds with porn sounds. The council is trying to fix the problem. The video with passers-by who turn around when they hear the porn sounds is rather funny. The reactions are interesting: from 'real taboo breaking sound art' to 'how symbolic, now everybody knows that the council of Enschede has been screwed, because they paid more than 100.000 euro for this sound installation.'

What makes it believable is that a similar hack is possible in practice. The famous hacker Kevin Mitnick hacked the speakers at a McDonald's drive-in. He sat in his car to observe the reactions of the people ordering on the 'out of control' speaker. He offered a woman a free hamburger if she showed her boobs. This woman was so enraged that she grabbed a baseball bat and ran into McDonald's to air her grievance. But the employees had no idea who the voice in the speaker was.

15
Unreliable companies

A friend books a holiday home on the internet. She shows me a picture, a pretty chalet in France.
'Did you check the credentials of the person renting it out?' I ask.

'You've been completely brainwashed through your cybercrime research,' she replies. 'Not all sites are managed by criminals. I saw the advertisement in the newspaper, I phoned for information and they answered my questions helpfully. I also checked the address of the company. It's close by, in the next town.'

A few weeks later my friend has been conned out of € 438. Vakantiehuisjeonline.nl is one of many internet fraud companies. The name is just one letter different from that of a trustworthy site: 'vakantiehuisjes' (with an 's' at the end) instead of just 'vakantiehuisje'. The scammer has tried his best to come over as the real thing, with a permanent address, staff to answer the phone and a registration with the Chamber of Commerce.

Of course, once my friend's payment had been received the phone line no longer worked. She drove to the address the company was registered at, but the door was opened by someone who didn't know the company in question. Apparently, they were abusing his address, because he was getting bills for newspaper advertisements he had never placed.

One phone call to the newspaper tells me that companies can place an advertisement on account if they give their Chamber of Commerce registration number. That is what this company did: pass on the number of another company.

It's not only the Netherlands in which institutions are careless with people's privacy. In Bulgaria for example, they steal entire companies with millions in turnover via details from the Chamber

of Commerce, because you can also find everything on the internet there. They 'just' change the name of the company and re-register it. First you have nothing, then you have a profitable company on your name.

When I tell some friends that I am working on a book about cybercrime during a holiday in Bulgaria, I hear one strange story after another. There's an experienced hacker in the group, Ivan. He keeps pretty quiet, but suddenly different people start to encourage him to tell me something about a 'pophack'. Not that I have any idea what that is, and Ivan doesn't really want to talk about it at first. But his friends keep on pushing and then he tells me that he stole one of the main pop music sites, a kind of Top 100.

I pull my chair closer.

'Stole? How and why?'

'I work in the IT and usually I stay on the good side of the law, but a well-known singer asked if I could dismantle the site, because they were publishing nasty things about her all the time. She paid me, and I did it.'

'But how do you steal a website?'

'I hacked them, changed the administrators' passwords and sent them a friendly email telling them I was temporarily taking over their website and that they would get it back in two years.'

'And then?'

'Of course, they were very angry, they sent me various threatening mails, but they didn't know who I was, so at the end they had no choice but to accept it.'

Hmm, quite a modern way of censorship, I think to myself. If they write something bad about you, hire a hacker and he makes sure the entire website disappears.

What I also find a fascinating trend are the drones. If I can believe the experts, we will all soon be filmed from all angles. Drones have already become so affordable that you can buy them at a toy

store: for less than hundred dollars you can buy one that stores hundreds of pictures. You can follow celebrities or peek into your ex-partner's back garden. Some of the richest Dutch people were furious when business magazine Quote took close-up pictures of their homes and gardens with such a drone and published them on the internet. I could understand their reactions.

In many countries the impact of drones and their use is already being discussed. In America it is about the 'Burrito Bomber,' a drone which delivers Mexican food. It sounds cool, until the drone malfunctions and drops hot beans over a passer-by. If you are not the victim, you might still find this funny.

The drones have become known for their use in war zones. Future wars will most likely be fought out with drones and computers and less with weapons. Defending the country with a keyboard and a joystick is a reality. Every day the Department of Defence fends off more than one thousand attacks on the Dutch army's computers. The attackers can install viruses which disable weapons systems and air defence.

The Belgian military intelligence service recently asked the Americans for help with the removal of a complicated computer virus. The Belgians probably didn't read the messages about global American espionage. Their military secrets are no longer secret any more.

Hackers seldom make themselves known when they are in your computer, or it has to be something they found that they can blackmail you with. Some computer experts think that a third of all computers is infected. You can download programs from internet which remove the infection. Many programs are fake and do nothing else than add another virus to your computer, this time for their own use.

You are more vulnerable with wireless connections. I have seen with my own eyes how a full room of people interested in privacy

have been duped. I was talking about identity fraud and then it was the turn of hacker Brenno de Winter to show how easy cybercrime is in practice. He had renamed the signal on his laptop 'KPN' and most people in the room thought this was the free Wi-Fi signal of the KPN telecom company. Many phones are configured to automatically log in to a known network. Brenno could then tell people who was doing what: 'you are tweeting, you just sent an e-mail that man over there, he's listening to Spotify…' Lesson learnt: never trust well-known network names. And also, don't trust those you don't know.

Brenno shows me his fake ID. It is a card the size of a regular ID, light blue in color. Brenno had it made at a hacker's conference for fifteen euro. He thought it looked cool and was funny. He didn't expect many institutions would accept it. But they did. Brenno could buy sim cards at T-Mobile and Vodafone. Even the Lower House of Parliament, the Dutch Intelligence Agency, the police, the European Parliament and various ministries accepted the card as a valid ID and gave him acces to their buildings. Under the pretext of security, we need to sacrifice more of our privacy and at the end, it is all for nothing.

Many companies swear that they are taking the protection of our data seriously. Their employees are trained to ask for verification so that they can also confirm via the phone that I am who I say I am and not someone pretending to be me. But they don't ask difficult questions, because most people can google the requested details, such as date of birth, initial letters and address.

I phone a health insurance company on behalf of a Bulgarian friend to ask why she has to pay a few months insurance premium in back-pay. Because she doesn't speak Dutch very well I helped her with her application and now I feel guilty that she has received this high bill. The telephone operator carries out the extra checks: initial letters and date of birth. When I think I have passed the checks

she suddenly asks if my friend is with me at the moment.

'No, she is working, I just wanted to check on her behalf if the bill is correct.'

'Well, if she is not with you, then we can't give you any information about her.'

I hang up disappointed.

'Can't you pretend I'm in the room with you?' my friend says when she hears about it. 'How difficult can it be?'

'No idea.'

I decide to give it another try. This time I pretend to be my friend, so I'm committing identity fraud. It makes me feel very uncomfortable, but I answer all the security checks. And sure, I suddenly get all the information. It seems it's more lucrative to be a scammer than to tell them you are helping a friend. And the security of personal information seems to be an illusion.

That this isn't just possible with health insurance companies was proven by 'Leak-tober': each day in the month of October hackers showed which companies were leaking their customers' information. Those were hacks on which many people commented: 'Yeh, but that's not that difficult.' That's what makes it so scary, that many people can do it. Even a child that cannot yet read or write, can learn to hack. For the project One Laptop Per Child, researchers left behind tablets in far-away villages in Ethiopia, without any instructions. They expected that the children would play with the boxes. Thanks to tracking software they saw that something else happened instead: the children opened the boxes, found the 'ON' button and after a few days they were using 47 apps per child. After a few months they hacked the android operating system, while they couldn't read or write.

I google Rickey more extensively, because I want to know more about him before I let him hack me. Google confirms what Rickey

told me himself. In a news article I read that the national police High Tech Crime Team arrested five people who were suspected of hacking the Michigan University. They were also suspected of computer invasions at universities in a large number of countries. Michigan University discovered that a program had been installed on the servers to distribute illegal copies of computer games and movies.

When I announce on Twitter that I am going into business with a hacker I am immediately followed by a 'data specialist.' I first think that it is someone who collects data about customers for a commercial company, but she works for the police. What makes Roos special is that even with all her expertise about computer crime she has become a victim of identity fraud herself.

'I always thought I wasn't interesting enough to be a victim,' she writes to me in a personal message. 'The only interesting thing about me is that I am a nerd. As one of the few nerds with boobs I sometimes got preferential treatment. And if I looked stupid, they would all want to help me.'

'Well, I look stupid all my life when I want men to do something for me. That also works for a digital novice. But tell me, how did you become a victim of identity fraud when you know so much about the subject?'

'Just in the standard way,' Roos says. 'I handed over a copy of my passport when taking out a subscription for my mobile phone. Someone took advantage of this by taking it out the system. They used it to take out other telephone subscriptions and I received the bills. I wasn't aware of that until the police came to the door.'

'The conclusion?'

'That you shouldn't think you can't become a victim just because you are not interesting enough.'

A little while later Rickey gets in touch. Although Roos and I haven't exchanged most of the messages in public, he has seen that

we have been in touch on Twitter. ‘I get the feeling this woman is following me,’ he says. 'Were you talking about me?’

‘Not really. We joked about men in general.’

‘Roos works for the police. She keeps on turning up on the internet wherever I am.’

‘That doesn’t surprise me, most nerds have common interests, so it is logical that you go to the same places.’

‘Perhaps it is, but I find it disconcerting to know I am being followed by someone from the police.’

‘That’s because you don’t have a clear conscience. You agreed to hack me while you are on probation.’

‘Don’t rub it in, otherwise I might reconsider.’

‘You should have thought about that before you hacked all those university computers. Hacking someone with her permission isn’t illegal. Except if you abuse my details afterwards. But as you are on probation, you’ve got a very good reason not to.'

‘You’ve got it all figured out, haven’t you?’

‘Well no, our paths just happened to cross. Scoring a hacker on probation, I couldn’t even think about it.’

16
Wiretapping

My mother, who lives in the United States, didn't want to join Facebook. According to her, it is a vehicle for espionage. She hardly publishes anything about herself online. When we Skype, she prefers to write in Bulgarian rather than in English because she doesn't want our messages to be easily read by the Americans. I said she was crazy, until the privacy bomb exploded with revelations of worldwide wiretapping: the secret services had access to data from Skype, Facebook, Google and numerous other large companies. My mother was right in assuming they could read our chats and also see the pictures sent in private messages.

They have mountains of data about you and if they analyze something incorrectly you can suddenly be marked as a potential danger. It is actually ridiculous that third parties have access to what I write to my mother. They wiretap on millions of people in the hope of catching a few, the proportions seem skewed. And it doesn't even work, because the intelligence services have been often embarrassed by having identified terrorists whom they couldn't stop.

The internet has changed from a free podium into a spy network. Now I know that secret services can 'scan' our emails and private messages, that they can even read encrypted messages on our smartphones, I find it difficult to believe that we live in the free West. I grew up in a communist dictatorship where the government deemed all citizens a potential danger. The Western countries nearly tripped over each other to declare that it was an abhorrent system, but now they do it themselves under the alias 'terrorism prevention'. The American NSA takes the biscuit by tapping millions of phone calls, search results and emails. Many highly placed European politicians didn't think breaching the privacy

laws in their countries was a reason for a diplomatic scandal, until it became clear that their mobile phones were also being tapped. Then they were furious, especially the German Chancellor Angela Merkel. Perhaps this was because she also grew up in a communist dictatorship.

The Americans had even tapped the Pope. The Pope! I was most surprised about him. How long will it take before the Americans are going to wiretap God? Or do they think that through the Pope they will find out what God has planned anyway? But perhaps the explanation is a bit simpler: the Americans are convinced they have God's blessing to collect the secrets of companies and citizens. And not to forget from all the well-known soccer coaches. It is strange that the American still play soccer so poorly after illegally listening to all the hints and tactics. That's the difference between hearing something well and using something well, that is where so many mistakes are made.

When I look at my friends, most of them aren't interested in privacy. This was different in 1971 in the Netherlands when the census was announced. People had to complete a questionnaire and answer personal questions and fill in their name, address and date of birth. Many protested, because they were worried about their privacy. They still recalled how well the carefully maintained census had made the transport of Jews so much easier. But participation was mandatory and if you refused you could receive a large fine or 14 days in jail. Yet many people filled in wrong details on purpose and 268.000 people refused to collaborate to store their personal data. Nowadays we think it is normal that the government has hundreds of databases and that they are all linked to each other.

When I fly to America to visit my mother I have to fill in another ridiculous list: whether I have any STD's, a psychiatric condition or a criminal record.

Shouldn't the Americans already have this information thanks to

the possibility of following all my internet traffic and thanks to all the databases they are gifted by our government? They even get our bank account details, even though research shows that terrorists don't show any deviant payment behaviour.

The list I have to complete costs me fourteen dollar and I also have to pay the same amount for my under-age children to declare that they haven't been convicted and don't have any STD's. I can't help it, but I think that I am sponsoring the illegal collection of data, because the same list used to be free-of-charge. Wiretapping millions of people costs money, and someone has to pay it.

Some people don't understand what I am upset about if I have nothing to hide. Well, my eyes have recently been opened. For example, I thought it was impossible that I couldn't gain entry to the United States if I had smoked a joint. I have done it twice, because I wanted to know what it felt like to get high. The first time nothing happened so I wanted to try it again. As a non-smoker I'm not very good at inhaling and the second time nothing much happened either.

I wrote a funny blog about it, because I don't see myself as a drug user. Can something like that be harmful? I didn't think so, but the Canadian psychotherapist Andrew Feldman was denied entry to the USA after a border guard had googled him and read that he had used drugs in the 1960's for an experiment with LSD. In the 1960's! The internet has an eternal memory and even remembers things before the computer era. The American authorities denied Feldman entry to the United States for an indefinite period of time.

Wiretapping programs use all the information they find about us and calculate suspicions based on algorithms. If you can be charged as an innocent person in real life, then it is so much easier online, because it is almost impossible to correct false information.

The real cases show how this worked. For the conviction of Lucia de B., an innocent nurse who spent six years in jail for murdering

patients, various facts were linked to each other. She rarely had lunch or gossiped with colleagues, she was an ex-prostitute, she had forged her high school diploma and she liked tarot cards. All these things have nothing to do with murder, but they made her suspicious in the eyes of the judges. Another factor was that a nurse had said that Lucia de B. had been in the vicinity after the death of a baby.

Using modern technologies, the police always know if we have been in the vicinity of a crime, because our mobile phones register that, even when they are switched off. Google saves all your strange preferences and the picture is complete: you were in the area and your preferences are very suspected. Lucia de B. couldn't convince the judges of her innocence, why could you?

I wonder how online data can be analysed and if these analyses are correct. There are many programs on the internet which emulate the intelligence services in miniature. A computer program such as Tweetgenie promises to predict my sex and age just from the words I use in my tweets. They don't look at my name, photograph and profile and they only use my last 200 tweets. The program looks at combinations of words which are associated with man and woman and with old and young. Common words for women are apparently: 'my husband' (I usually don't tweet about him because of his right to privacy), 'bye' (I say that to friends, but not on Twitter), 'OMG' (I still think this is a strange expression, and I don't use it), 'hihi' (I'm a happy person, but I seldom use 'hihi'), 'Mum' (I don't tweet about her), 'girlfriends' (I don't usually mention them on Twitter), 'nails' (that's about the last thing I pay attention to). From the entire list of female words, I only use 'sweet' and 'nice'. I don't really come across as female and I'm curious as to what sex the program will guess I am.

Tweetgenie also has examples of male words: 'bro', 'Ajax', 'Fifa', 'mate', 'beer', 'nice', 'my wife', 'game', 'old man'. I don't recognise

anything in that list either.

The site also has characteristic words used by younger and older people. Young: 'real', 'haha', 'me', 'you', 'just', 'okay', 'thanks'. When you read that you wonder why older people don't use those words, but apparently this has been researched.

Then the words for older people: 'son', 'daughter', 'good morning', 'have a safe trip', 'good luck', 'thank you', 'beautiful', 'have a good weekend', 'wish'. Okay, great, I'm curious about my digital age.

The only thing I have to do is fill in my Twitter name and the program starts to calculate. In less than a minute the result is known: I'm a 36-year old female. They're not far off.

The program Youarewhatyoulike also promises to predict who I am. They use my 'likes' on Facebook for this. When the data is analysed I see a screen with a lot of information about myself, divided into groups.

The programmers first compare if I would prefer traditional or new things and come to the conclusion that I am 'intellectually curious' for new things, despite what other people might think. That's true. After that they comment on what type I am. I am successful because of my perseverance, they say. That is also absolutely true. I still recall that I wanted to become a journalist in a language I could hardly speak. Not a realistic goal, but that was my dream. Then you have only two options: give up or with lots of perseverance learn the language at such a level that newspapers and magazines hire you to write for them.

According to the test I am calm, emotionally stable and not someone who hangs on to negative thoughts. That is also true, because I am rather forgetful and that is also handy when it comes to problems. I solve them, or I forget about them.

Youarewhatyoulike comments about the way I look at people and make friends: I am friendly, helpful and believe in the goodness of

people, they say. I have to admit this is still the case, even though I have been hurt a few times by counting on people's integrity and decency.

So, yes, my 'likes' allows such a computer program to know my qualities and weaknesses. Kind of scary actually, a psychologist couldn't do better. And this is a rather innocent program. The governments in different countries still know much more about me under the motto 'Yes, we scan'.

When something is hard to get it usually becomes more valuable, but that doesn't count for privacy. Most people aren't worried about the sliding scale, because it's for our own good. The interfering government thinks it is fine: when an invasion of privacy doesn't bring too many complaints, they are already announcing the next measure.

Some people apparently assume they don't have any privacy in this digital era and just put everything online. They aren't embarrassed to showcase their ignorance or even pure stupidity. There are sites which collect remarkable status updates from Facebook. One Jessica asks: 'What is Obama's surname?' and someone wants to know the name of the Dutch author of Anne Frank. Two words with two typos are also funny, especially when they mention how well you are doing at school: 'Passet my exsam'. And my personal favourite: 'Yes, booked my ticket to Spain. Rome here I come!'

Of course, people are allowed to post what they want about themselves; what I find more disturbing is how poorly organizations protect our privacy. With a bit of bad luck, all my personal data is made public, including my medical file. I haven't had any embarrassing illnesses yet, but still I don't feel comfortable with the idea that everyone can see for which ailments I visited the doctor. How big is the chance that everyone will find out? At first, I didn't think very big at all, but suddenly medical and personal details of more than 300.000 employees at Dutch companies, a well-known

football club and hundreds of other companies were made public as a result of a leak in the computer program Humannet. The details could be accessed by outsiders for months because of poor security. Employees' sick leave, medical files, and reintegration programs: everything was visible.

Sites that are hacked usually react slowly. LinkedIn leaked more than six million passwords and its customers almost immediately received a warning email to enter new login details. Nice, except it wasn't Linkedin itself that sent the email, but cybercriminals. When news got out, they were quicker than LinkedIn to react.

Hackers earn enormous amounts of money with these types of 'phishing' activities, but also computer hijacks. A hacker encrypted all the medical files at a hospital in Illinois, so the doctors couldn't use them and asked for ransom. Lately this happens a lot in all kind of branches and many companies pay. Sometimes they also pay the hackers, because this is a cheaper and faster way to get back all the encrypted files then let the IT-department struggle with the back-ups.

17

Facebook and Google

We are constantly spreading information which in our eyes can't do any harm, but is often used for identity fraud. Why are we so keen on telling everyone what we are doing? Perhaps because other people do the same. Thankfully you usually determine what you share yourself, but that seems to be changing. In the American state of Louisiana, people who were once charged with a sexual offence have to put 'sex offender' on their Facebook profile. If they refuse, they can be given a ten-year jail sentence.

Facebook is now the favourite reading material for lawyers, because people talk about their misdemeanours without any shame. There are mothers who have lost custody of their children because they swore that they paid a lot of attention to their children, while Facebook faultlessly registered that they spent hours playing computer games.

Facebook tracks everything I post, and all that data provides such a trustworthy profile of my interests that the American multinational probably knows me better than I know myself. They sell my data to third parties. Positive about Las Vegas? Then I see an advertisement for a holiday to America. Book lover? I see the latest titles appear on my screen. Oh, and yes, don't forget the dresses. I first wondered why I was seeing so many advertisements for dresses, but now I know. My closet is full of dresses and Facebook knows this.

I am usually careful not to 'like' everything, but sometimes I can't resist the temptation. It is just so easy to 'like' something. I sometimes think that friends and acquaintances don't really care about the 'likes'. I recently had technical problems with Twitter and then I wrote the word 'test' to see if it was working again. I immediately deleted my tweet, but I had forgotten that I had recently redirected

my tweets to Facebook.

The next day I saw lots of 'likes' under the word 'test'. Huh?

Facebook probably knows more about me than my best friends, but how much? I can request that information, and I do out of curiosity. I receive a huge download with messages, advertisements I once clicked on and photos I have posted. The file is surprisingly large, seeing as I am not that active on Facebook. The list of areas of interest for potential advertisers is eye opening. For many things I don't even recall that I have ever looked them up. From local bike shop to Bali, and from house music to application software, I have no idea why Facebook links that to me. But most of the key words hit the mark: Toyota (our car is a Prius), New York (been there on holiday), jewellery (I've never ordered it online, but apparently Facebook knows that I keep on expanding my collection of earrings), police station (in relation to my filing a report against the stalker?) … For some topics I start to recollect that I once looked up some information about them, but for many I don't recall at all. Facebook has an impeccable memory.

The power of Google is also enormous. The search engine remembers my IP-address and places a cookie on my computer. This gives me a unique code, with which I can be traced continuously. Google has numerous services, such as YouTube and Google Maps, and all this data is combined and analysed until they have created a painfully precise profile.

The Dutch Data Protection Authority came to the conclusion that Google is breaking Dutch law. Privacy sensitive information about our location, payment details and surfing behaviour are combined in one overarching database. Experts expect that this collection of data can reveal as much about ourselves as human DNA.

Google is not the only company which combines and analyses our data. Lesser known companies also do this, such as loan company ZestFinance, which determines on the basis of 'signals' whether

someone should be given a loan. This includes your online friends, your use of language and even the times of day you visit websites.

The collecting of personal data has turned into a complete industry. The top executives at Google have never been secretive about this with remarks such as 'We want Google to become the third half of the brain' and 'We know where you are, we know where you've been. We can more or less know what you think'.

How much Google knows about you probably only becomes apparent when you think you have committed the perfect murder, such as the 27-years-old chemist Bart S. His girlfriend dies from eating a peanut butter sandwich injected with poison. The coroner concludes it is a natural death: heart failure. Bart S. only starts to draw attention when he continually enquires about the case. The breakthrough comes when his computer is impounded. The police discover that he has googled the workings of the chemicals sodium azide and cyanide, traces of which were found in his girlfriend's blood. Sodium azide forms a lethal and untraceable gas when it comes into contact with stomach acid: hydrozoic acid. A perfect murder, but not if you google it.

We consciously or unconsciously spread information about ourselves, because we have 'nothing to hide'. But many people have missed out on a job opportunity because outsiders have looked at ordinary pictures or posts through different eyes. What many people don't realize is that not only potential employers, but also benefits agencies and insurers are keeping an eye on you. Insurer Aegon once cancelled a customer's insurance policy because on his Facebook page he had written that he had participated in illegal street races.

Employers also look on the internet to see what kind of person you are, especially for job interviews. They come across the strangest of things, because many young people aren't interested in privacy. You can't blame them, because the computer education

at school isn't up to much and most schools don't think it is their business what students do on the internet. That's strange, because nowadays your online reputation when looking for a job is often more important than your diploma. An employer won't test your reliability, he will just look you up on the internet. Candidates are rejected because they have posted 'inappropriate' comments or photos on Facebook or Instagram.

If you read all the privacy statements on Facebook, you think they take care of your privacy, but Facebook and also Google spend millions on political lobby to prevent politicians drafting stricter laws. They know so much about us and they want to keep it that way. Try to delete things they have written about you which are incorrect. Some things might be correct, but they are so private you don't want to share them with the public. Former Formula 1 Director Max Mosley took out a lawsuit against Google because of photos at an SM-party which have been haunting him for some time. The court decided that the leaked photos where a breach of his privacy. Now it's the turn of Google. Man against machine.

The internet magnifies everything a thousand times. My generation made enough bloopers, but not everything was registered then. In the past, we would discuss a blooper and forget about it, because the internet didn't exist. But times have changed. If you placed a nasty remark on a forum ten years ago, then it can still be traced. Sometimes with just a few clicks of the mouse. So never change your opinion, because everything has been registered and can be used against you? I think it is horrific that you can no longer spontaneously do and say things. It is very valuable that you can change opinions. As Adenauer says: 'You don't always have to have the same opinion, because no one can stop you getting smarter every day'. But I am afraid that googling moralists have no time for that. Even worse: they wrongly interpret what you have written and then you have a problem, because then the people will attack

you for something you didn't even say. This happened to Monique Burger, owner of The New Bookstore. She wrote an honest blog about poverty in the Netherlands, which she saw when many people suddenly came to pick up a free copy of the Dream book. She described how unkempt and rough her new customers were and how large the contrast with her regular customers. After publishing the blog her shop front was vandalised and she had to hide.

I read her blog with growing surprise. Was this the piece that people were so upset about? Sure, she spoke about poor people who looked unkempt, but she didn't write that she thought all poor people were the same. That is what some readers made of it.

Years ago, I wrote an article for a newspaper about families in debt. When I went to the address I was given, somewhere in the northern part of the country, I entered a neighbourhood which took my breath away. No well-tended gardens with flowers and bushes, but stolen shopping carts, garbage and even dirty nappies on the pavement and in the gardens. These people had a widescreen TV but no money for a sofa or to buy good food for their children, they told me. I was shocked and wrote it down. It wasn't meant to be stigmatising, I just wrote what I saw. The only difference with Monique and me? You didn't have social media then and my house wasn't vandalised.

Nowadays you don't even have to have a controversial meaning to be attacked online by strangers. Sometimes just a photo is enough, as in the case of 12-years old Frank. He sets up a Twitter account with the help of his mother. A few weeks later his photo is found on many (foreign) sites which make fun of how he looks. Frank has a lot of freckles and is cross-eyed. His face is superimposed on naked women and more and more fake accounts are set up.

It is difficult to delete the photos the official way, so Frank's father decides to post messages on the timelines of the fake accounts with the urgent request to delete his son's picture. As a reaction to this the

perpetrator publishes Frank's true identity and new pictures of him appear online. They have been stolen from his mother's Facebook page. In the meantime, Google also makes the mistake of linking Frank's real name to the fake accounts and caricatures. Because it has gotten so out of hand, his parents consider changing their son's name – an extreme measure to solve a problem that otherwise seems impossible to solve.

The story of 15-years-old Angelina is similar to what Frank went through, because she also finds out how easy it is for someone to steal your digital identity. Angelina changes from a good girl into a slut. The person behind the fake account spreads pornographic photoshopped pictures in her name. Angelina no longer dares to show up at school, because suddenly boys are approaching her telling her that they would love to have sex with such a sexy chick. The only thing Angelina can do is to try to convince everyone that her identity has been stolen and that she has already reported this to the police.

Her mother is still angry with the way the police report was handled. 'The police officer didn't know what to do with it. She first had to check if it was even possible to file a report,' her mother says. 'They told us not to expect anything, because identity fraud wasn't a priority. I understand they prefer to solve home burglaries, but identity fraud can also destroy someone's life. The police sent us home without any tips what to do next. We had to figure out ourselves how to delete a fake account.'

In the meantime, Angelina continued to go to school, but she came home crying on a daily basis. She suspected who might be behind it. 'We passed on this name to the police, but they said that a computer's IP-address wasn't enough proof, because perhaps someone hacked into that computer.'

Traces of Angelina's deleted sex account can still be found on the internet, but these are not linked to her real name. 'Thankfully,' her

mother sighs in relief. 'Can you imagine going for a job interview and your future employer sees these shocking pictures, then you can expect not be hired.'

She's probably right: nowadays you are whom Google says you are. So google yourself every now and then.

18

Old computer

Since I have been telling people that I am going to let myself be hacked, I receive warnings from everyone. No one understands it, they all think it is too much of a risk.

'Did you read the Mister Penenberg article?' a good friend asks.

'Mister Penenberg? It doesn't ring a bell.'

'Well, he also wanted to be hacked and he had chosen his hackers well, a professional team specialised in ethical hacks. His identity hasn't been stolen, but they took it far enough. They googled his interests and also those of his wife and they both received an email which looked trustworthy. His wife took the bait first and opened the file. They could easily get into her computer and they found a lot of information about her husband.'

'That doesn't surprise me. If they look in my husband's computer they will probably also find lots of useful information, even though he encrypts his passwords.'

'The funny thing is that their passwords were also well-protected,' my friend says. 'The hackers made a fake screen which kept on asking for the master password. Very annoying. After ignoring it a few times his wife filled it in.'

'I'm afraid I would probably have given in myself,' I mumble softly. I am thinking of Google, which keeps on asking me for my phone number with the request: 'Help us to protect your account. Confirm your mobile phone number and we will let you know if there is unusual activity on your account.' I always ignore it, but Google doesn't give up. 'Confirm your mobile number. Most people only receive three warnings per year. This number will only be used for security purposes.'

I keep on ignoring the request, until Google sends me the same request, but this time the telephone number box is no longer emp-

ty but has been filled in. I see my telephone number. The cheek of it! The fact that Google already knows my telephone number is perhaps not surprising, but it feels as if they're saying: 'Okay, enough fun and games, we know everything about you, so just click on 'confirm' and then you'll be rid of us.'

I give up, it is no longer a fun game when one of the players cheats.

Since I have been working on the topic of cybercrime it seems that many people I know suddenly have an experience with this. Probably no more than in the past, but we didn't talk about it then. Anita discovered that she could take out an online loan with just a copy of an ID. She decided to test if she could take out a loan using someone else's name. She gave her own address details, but sent in a copy of her friend's ID, with a forged signature. Her friend wanted a loan, so they weren't worried if the application was accepted. The forged signature wasn't a problem. The money was transferred to the wrong account.

My webmaster also had a similar experience. His previous girlfriend had ordered items online but didn't pay for them on time. They had already split up a while ago, but it still got him on the black list with the Financial Registration Bureau. He only found out years later, when he applied for a new mortgage and had to prove he hadn't defaulted on any payments.

An acquaintance who is a musician complained that every bar where his band plays copies his ID. No payment without a copy. Many people don't see the danger and aren't bothered about copies. But most companies and organisations aren't allowed to ask for it, for example, hotels in the Netherlands. Yet, in other countries they are and this way your identity can still be sold worldwide. Using a privacy freak's tip, I now try to prevent this. 'You can note down my passport number, but not copy it,' I say when we arrive at our holiday destination.

'Why?' the hotel employee looks at me questioningly and somehow in a suspicious way.

'Well, in the Netherlands it is prohibited by law to copy a passport and the state can take you to court because you are copying Dutch citizens' passports.'

This is an enormous bluff, but the lady looks quite shocked. She doesn't even think to say that Dutch privacy laws are not valid abroad.

'Aha, okay,' she mumbles. 'Then I will just write down the number. That should be enough.'

I look at my husband triumphantly, it works! I've found another way to protect a piece of my privacy.

What do you do if your privacy is not threatened by a stranger, but by your own boyfriend with whom you have a child? Anna Jansen received a message from a stranger. 'You're posting quite a few saucy pictures on Facebook.' Huh? Saucy pictures? Anna didn't know what he was talking about. But she was forwarded a link and she discovered that she had had a Facebook account for the past seven years with hundreds of friends.

'When you see something like that, you don't know what to think,' Anna says. 'At first I had no idea who was behind it. I couldn't imagine that it was my own boyfriend. But on the page were photos which couldn't have been posted by anyone else. They were just too private. I discovered that he had set up profiles in my name on dating sites to chat to bisexual women.

I left with our five-years-old daughter. I couldn't deal with the fact that my boyfriend had stolen my identity. I reported him, because I was hoping for some kind of moral satisfaction, but it was dismissed, because they said they couldn't prove that he had done it. He did confess to me, but I didn't have any proof of that.'

Anna started to look for more fake accounts in her name and sent requests to delete these. But that was more difficult than she

thought. A few times her ex-partner left the accounts as they were, but just changed her name, so she had trouble finding herself by searching her name. 'That is when you realize how big internet is and how vulnerable you are. Someone can post everything about you online and no one checks it.'

What I have noticed in all my conversations with victims is how many different ways there are to steal your identity and how unpredictable the consequences sometimes are. Most victims are afraid that it will start again. Some become paranoid and find it difficult to trust people. The 31-years-old Linda Drummer also had such a moment. Anna soon realized that the perpetrator had to be her boyfriend, but Linda has not been able to find out who it is for six years. She has filed numerous police reports against her invisible enemy. She has had to appear before a judge a few times because she refused to pay for items which had been ordered in her name. 'But why does the order include your name, date of birth and address?' the judge asked. Those details aren't that difficult to find nowadays.

'Of course, I could claim that I had never received the items, but how do I prove that?' Linda says. 'I had to pay a few times. And I paid those bills because I was afraid the debt collection fees would rise, and a bailiff would impound my things. You have your back against the wall and you can only think: why would I order this rubbish? There was even male clothing among the orders. All together I have paid about eleven thousand euros for someone who had gone on a shopping spree in my name.'

Linda didn't know who to suspect. She had experienced something suspicious just one time. The doctor's assistant had swapped Linda's prescription for sleeping pills with someone using the same medication. That was soon rectified. After a while Linda went to the pharmacy to pick up her pills with a repeat prescription but they had already been picked up by someone else. This happened a

few times until Linda blocked it: from now on only someone with a copy of Linda's passport could pick up the medication. She had to pay the health insurance bills herself, because she was liable for part of the costs of the medication which the unknown person had collected.

'I have now been working on trying to solve this mess of identity fraud for the past six years,' Linda says. 'I recently received a message from the ING Bank that my current account had been converted into a student account, which meant I was entitled to a loan. I flew to the bank, what do you mean a loan? I don't want any new debts. And above all: how could they arrange this without a signature?

Linda still has two court cases pending. 'The worst one is a large amount for a mobile phone subscription. I once paid for a subscription which wasn't mine, but that was with a different provider. It's difficult to prove it's not you, that's the whole problem with identity fraud. I haven't gone crazy as a result of all this misery, but there was a period when I no longer trusted people. I tried to keep an eye on everyone, couldn't think straight. Someone has power over you, but whom? Thanks to my parents' support I became more sensible.'

I still remember the time when everything was more personal and identity fraud hardly existed. I even remember the time we didn't have computers. I actually think that is quite special. My sons haven't experienced this and they don't know how to amuse themselves for hours, days and even months without a computer.

I am walking through a museum with them one day where old computers are being exhibited.

'I used to have one of those,' I say, and I point to one of the exhibits.

'What is that hole for?' the youngest asks.

'For the floppy discs.'

'For what?'

'For the floppy discs. You could save games on them, because our computers didn't have enough memory to save our games. And the internet hadn't been invented yet to play them online.'

'So, you didn't have internet? What did you use the computers for?'

His father and I look at each other. We were about to burst out laughing, but our son's question was deadly serious. How do you explain to the younger generation that you mostly used your computer as a word processor and for example to put the names of your LP's in neat tables? In his eyes this is a big 'fail'. As parents we already have a duff image and now we have another failure added to it?

'I also played fun games,' his father tries to sound cool.

Our son looks at him thoughtfully: 'Pacman, you mean?'

Caught red-handed. We have to admit that it wasn't up to much back then compared to the real-life games they play nowadays.

I try to come up with an advantage of the good old days, there must be one. After such a failure we could use some extra points to polish up our image. I suddenly know what it is: 'We were very safe behind our computers. No hackers and no viruses.'

'Yeh, duh, that's logical if there was no internet. How else would they get into your computer?'

My husband whispers in my ear: 'They could do it via floppy discs you know, I found this out once myself, but don't tell him.'

The museum doesn't display a floppy disc, that saves some explanation, so we leave it.

My son's question does make me curious. Who were the first hackers and what was the benefit of putting a virus on a floppy disc if you couldn't get out any data with it? Why did they do bother to do it? I find a book about computer history and read with growing surprise. The computers had to be manually operated. Now I also

sometimes feel like being a servant to my computer, but in the past, this was literally the case. Women usually slept on stretchers next to such a behemoth, because if the zooming stopped or sounded differently, they had to intervene. The computers were extremely slow in their calculations and it wasn't profitable to switch them off. It was no exception to have six women taking care of a computer day and night. Only women by the way, because they were more precise than men and such a valuable machine needed careful handling.

My children can complain how slow and ugly their first computer was, but in fact this is nothing compared to its predecessors. ENIAC, one of the first computers, weighted 28 tonnes, just as much as eight elephants. I can't imagine it, never mind my children, who already think a computer with a big 'bum' is a strange sight.

And the hackers? They were working more on the technical challenges than on spreading viruses. The first bug wasn't thought up by hackers. This was discovered by a woman who wanted to know what was wrong with the university's computer. She found a crushed moth in the computer, which had made the computer crash.

She glued it into her logbook and wrote 'bug' under it. The bugs I get in my computer look quite different. I can't remove them myself, I hand the 'debugging' over to the nerds.

I am sometimes nostalgic about the good old days. Okay, the computers were extremely slow, but this didn't really bother us, because our lives didn't revolve around the computer. We met up with friends for a cup of coffee instead of liking their pictures on Facebook. And we received no threats via social media.

19
Digi-dead

As if I don't have enough digital worries, nowadays I am also starting to think about my digital death.

At least, that is what large companies such as Google and Facebook advise, but also many lawyers who have thrown themselves on this issue. There are also initiatives which focus on this. Death no longer has to be definite, at least according to the website LivesOn. 'When your heart stops beating, you'll keep tweeting.' Is that a joke? I really don't have to continue tweeting after my death, it sounds rather creepy. For those people who do, LivesOn promises automatically generated messages from beyond the grave, which are personally made based on an analysis of your previous tweets and preferences.

Many social media users and owners of company secrets in the cloud seem to be mostly unaware of their mortality. A difficult subject. What does a digital cemetery look like? Who can access it? 'Death', as offered by Google and Facebook, is nothing more than all your data being automatically deleted after a period of inactivity. I am curious how you delete all traces of yourself on internet, I think it is impossible. An American journalist showed in an ingenious way how the small crumbs found about us here and there can form a gigantic mountain. She googled the Google CEO Eric Schmidt and she posted all his information about his shares, hobby's, political preferences and much more on the website News.com. The result: a furious Mr. Schmidt who complained about an invasion of his privacy and that even his safety was at risk, because suddenly everyone knew so much about him. It seems he had forgotten who had made all that possible.

Google is unrivalled, because we often use different Google services and link all that information to each other. Take an applica-

tion such as Google Now, which sends you a reminder if you are about to be late for an appointment you put in your Google Calendar. Quite useful, but some people were unpleasantly surprised when Google- Now also reminded them about obligations which hadn't been written in their Calendar. Huh, how does Google know where you work if you haven't written that down anywhere? And how does the application get your private address?

That's not that difficult, because your phone's location details say a lot about you. If you drive back to the same place every evening, then that's probably your home. If you are somewhere for many hours during a working day, then that is probably your work. Google knows what your working hours are and which days you arrive late. The search engine probably also knows your favourite pub and unfortunately also how often you visit your lover, if you have one. But we are all good citizens, who have nothing to hide, and that is why we trust Google. And for its usefulness, of course. If you are with your lover and Google knows your regular pattern, then you can get a reminder when it is time to go home to your wife.

Google knows I filed a report against my digital stalker and is aware he denies all involvement. I know that for certain because I google him to see if he is still following me. And yes: he is busy spreading news that the case against him has been dismissed, because there wasn't 'a shred of evidence'. I phone the Public Prosecutor's office in anger: my digi-stalker and Google have information about my dismissed case even before the person who has filed the report? The employee at the Public Prosecutor's office is prepared to give me information by phone if I give my name and my case number.

'How did you come to the conclusion that the case has been dismissed?' he asks.

'I saw it, that is what my stalker is writing.'

'But that's incorrect. It seems that enough has happened. In any case, the police have not dismissed the case and it is still being processed by the Public Prosecutor's office. They have two divisions: light and serious cases. I see your case was first sent to the light cases, but after reviewing it, it has been sent to the serious cases.'

I listen somehow with surprise, because personally I thought it was more suited to the lighter cases. Worse things happen after all.

After filing my report, the digi-stalker was a lot less active, but he suddenly has a surge of energy, apparently convinced the case has been dismissed. I already see numerous tweets about me, in which he calls me all sorts of names and says I have a number of psychiatric issues. Quite something then that my doctor hasn't diagnosed these, but he has. You have some talented people out there.

He also says I have a 'secret lover' (I shouldn't let my husband read this). Also nice: 'Rumours are that Genova was an ex-pole dancer in Bulgaria,' he writes. I wish I had such an exciting past.

I recently showed the cover of my new book on Facebook. The next day the title had been registered as a website by my stalker, so I couldn't use it myself. I have to admit it, I hadn't seen that coming: it was original. The content was unfortunately predictable: a dumping ground for all his thoughts about me.

This time I have other worries, more interesting. The appointment with the hacker is finally confirmed and I have been invited to his house in Amsterdam. A few more days until we meet, and I am curious if we understand each other's language. In my eyes the real hackers are nerds who think in numbers, something I can't.

My husband is still against it. He isn't keen at all that someone is going to nose around in my computer, because it doesn't just contain information about me, but also about him and the children.

Point taken, I don't want to lose my husband. But I do want to see how easy it is to hack someone.

The appointment with Rickey goes ahead. At night, in bed, my

eyes are wide open and when I close them I still can't fall asleep. What does the house of a hacker who was hunted by the FBI look like? Is it filled with gadgets that I don't recognise?

His house is much less exciting than I thought: a messy student accommodation without too many gadgets. There are few wires trailing over the floor. I sit down on the IKEA sofa and Rickey gets out his laptop.

'Are you sure you want me to hack you?' he asks. 'Or do you just want me to show you how I do it?'

'I want to see with my own eyes how it happens and not just hear the theory behind it. Start with my website, which has recently been well-protected by an expert.'

Rickey smiles: 'By an expert, huh. Okay, we'll see.'

Before Rickey starts, we talk about his newest success: he got in the back-end of a large Russian botnet and came across data from hundreds of thousands of Dutch people.

'Do I also have a Russian in my computer?'

Rickey raises an eyebrow. 'I don't know, but it is possible'. The Russians have a very structured website and when you enter you can see what they already know. Sometimes there are curious things, such as the productivity of a certain civil servant who seems to spend hours on Facebook. But most cases are serious: company secrets from a technology firm, current court cases, what the police are doing in an investigation, etc.'

The digital file is very large, comparable to a library with 37.000 kilometres in books. 'At first the police didn't want to look into the Pobelka-botnet,' Rickey says. 'They didn't have the manpower and it didn't have priority.'

'Perhaps the data isn't as impressive as it looks at first glance?'

'The data can be lethal if it gets into the wrong hands,' he says. 'You can control various systems through infected computers, from chemicals to drinking water. It is even possible to paralyse air traf-

fic.'

The list with infected companies and institutions comes to 120 million pages of data. Ministries, television companies, lawyer's offices, airline companies, technology companies… almost every sector is affected.

'With the information they have collected the criminals can carry out large cyber-attacks, but they mostly focus on manipulating financial transactions,' Rickey says. 'And now we are going to take a look at your website. I'm curious if I can find some weak spots to get in.'

He brings my website on the screen.

I recently had my website so well-protected that I am not worried. This was done by someone who secures important websites and defends them from daily attacks from hackers, so it must be good.

Rickey searches for weaknesses with a program called Nmap.

'Your site has 65.535 ports. If one of them hasn't been closed properly, then there is a chance that I can get in. Did you know your server is in Florida?

'Florida? I have a contract with a Dutch hosting company.'

'Yes, but it rents servers in America.'

Rickey types in something on the screen. 'Ten ports on your website are open. You need to encourage a port to let you in.'

'Encourage it?'

Rickey laughs. 'A computer port has to think it is letting a trusted person to enter. I am looking for software leaks which can help me with this.'

Rickey knocks on every port.

'Blocked by the firewall,' he says a while later. 'Good security. They have seen I have been knocking on various ports and have thrown me out.'

'So, you can't hack my website?'

'Not in the usual way. But I can try to hack the entire server. Sometimes servers are poorly secured and then I can get in that way. If I hack the server, then I have access to all the websites, including yours.'

'Hacking a server sounds more complicated than a website.'

'Sometimes it is, sometimes it isn't,' Rickey says. 'The program Pure-FTPd runs on your server. They usually install it on port 21, but this time it's on a different port.'

In the meantime, I see long lists of numbers appear on the screen. This is all abracadabra for a digital novice, but Rickey seems happy.

'Yes, I see a weak link here, which I can use to disable the entire server. Your website will then be off-line. All the other websites also. Let's see who they belong to.'

I read along with him, the websites which are linked to the server in Florida come from various countries: from English cricket teams to an Indian oil company – 730 websites in total.

'Look here,' Rickey says, and he points to the screen. This is exactly what I was looking for: software to hack this server. It even includes a short instruction movie.'

'And then you have access to all these websites, including mine?'

'Yep.'

I am dumbfounded. A strong password, a well-working firewall, so much trouble to secure my website and a hacker still gains easy access through a detour.

20
Possibilities

I think hacking a website might be easier than hacking my computer. Rickey doesn't have any more time for another challenge, but we agree not to leave it at this. I still hope he gets to see the photos of the woodlice and that he can explain how he got through the woodlice security. But I really hope he doesn't manage to hack me.

I see a workshop which promises to make you 'untraceable' and I register for it. At the office of the civil movement Bits of Freedom I meet a varied bunch of journalists and nerds. The aim is that the nerds teach the journalists how they can secure their computers and how they can become untraceable. The requirement was to bring your own laptops, but no tablets or mobile phones, because they are by definition unsecure. Bits of Freedom states clearly that mobile phones are listening devices with which we can also phone. If you want to make sure you are not being tapped, then it is not sufficient to switch off your phone, you have to put it in the fridge or some other steel casing. I had never considered this, but among all these nerds I seem to be the only one who isn't worried about being spied upon through her mobile phone.

One of the invited speakers is Arjen Kamphuis, a security consultant who talks about what he comes across at all sorts of companies when he lifts up the keyboard: lots of food crumbs, but also yellow sticky notes with passwords. 'Just one of those notes with a password usually gives you access to the entire company network.'

Kamphuis is good in telling anecdotes. He recently travelled in First Class with the Thalys and could make use of the train's free Wi-Fi. He noticed that the login page wasn't secured. He switched his Wi-Fi scanner on and was able to see the passwords of his fellow travellers.

'I bet you that most don't think up a special Thalys password but fill in one of the privacy sensitive passwords they also use for other things.'

Kamphuis teaches the journalists how they can make their computer as untraceable as possible. You don't order it through the internet, but in a shop, and you pay cash. You then take out the hard drive and buy a new hard drive in a different shop.

I can't believe it. 'Is this the only way to make a computer untraceable?'

Unfortunately for me this is the case. Destroying the hard drive in a new computer, I hadn't considered that. If I am prepared to run more of a risk, then I can always use encryption program to encrypt my messages. The nerds even encrypt the simplest of messages they send to each other.

'We are going to convert you all, so you will also do it,' one of them says. 'It might sound complicated, but it's easy. A free program encrypts and unlocks the messages and you don't have to do anything yourself. In fact, everyone should use it when you consider the number of wiretapping scandals that have come to light recently.'

The Windows software on my computer is replaced by a temporary start-up version of Linux, which has been adjusted to look like the Windows start screen. Not just for easy use, but also not to draw too much attention to yourself in an internet café.

'You will look like a silly tourist and not like a hacker or a journalist,' they explained to us.

Then the passwords: we should really take this chapter seriously, make up good passwords and change them every now and then. Arjen installs the program LastPass.

He himself has a few hundred passwords. For example, if he wants to log in to LinkedIn, then the program automatically looks for the right password.

'Most citizens are careless with their passwords, with installing antivirus programs and in updating software,' Arjen says. 'The government does shockingly little in education. About 35% of Dutch computers aren't being controlled by their rightful owners. Don't you think it is strange that computer education at school mostly consists of typing in Windows?'

I can see how serious Arjen takes his digital security when he received a phone call during the demonstration. He takes a very old Nokia out of his pocket. I already suspect why he doesn't use a smartphone like so many other people: 'This type of telephone is too stupid to be tapped,' Arjen says after ending the phone call. 'Not that it is impossible, but it will be more difficult to install software on a telephone from 2007 which turns on the microphone and camera without me noticing. Besides, contrary to the iPhone, you can just take out the battery.'

For most people it will be difficult to find such an old telephone. Or you need to take a trip to Africa, because these old mobile phones are still in circulation there. I need to realize that I can be easily traced, because I don't have an 'African' mobile phone and for the time being I am also not willing to replace the hard drive on a brand-new laptop.

Master criminal Frank Abagnale, whom Leonardo di Caprio portrayed in the film 'Catch Me If You Can', would have had a very easy life if he had been born a little later. In his time, you had to be smart and agile to steal someone's identity, nowadays anyone can do it. A color printer is all you need to make a perfect copy and there is no lack of information, because nearly everything can be found on the internet.

You use your iPhone to take someone's picture at an airport, use an app such as PittPatt for facial recognition and check if he can also be found on the internet. If he doesn't have Facebook, then his photo might be on his company's website or his sports club. It only

takes you a few seconds to find out who he is. If you can also find his date or birth and place of birth (most people don't keep this a secret) then you have enough to steal his identity.

Abagnale advises people never to publish full frontal photographs on the internet. Only those with a group or if you are doing something active are suitable, because they cannot be used for fraud. This is probably not a bad tip, but the problem is that nowadays the danger comes from hundreds of angles and the police don't have much capacity. Disappointed victims often leave messages on forums. Such as Ilse. Someone abused her ING bank account for direct debits and one-off payment orders for companies she doesn't know. ING has taken weeks to see if the direct debits have been unlawful, while more and more money is being deducted from her account. All the items ordered via the internet are being sent to one address and it isn't Ilse's address. She is surprised that companies don't actually need her signature, and that anyone can debit money from her account.

Ilse files a fraud report and passes on the email address and address of the fraudster, but the man continues to use her bank account number. He receives the goods and she gets the trouble, because she has to convince every store that someone is abusing her identity.

'He bought all sorts of things, such as a bicycle and for € 700 in items from an internet and television provider, including a basic subscription, extra adult channels and a tablet. Apparently, he can just do this, just by ticking the box for a one-off payment order. You can do this if you ask the bank to set this up. The fraudster then chooses a different bank account number, perhaps yours or mine.'

Cybercriminals aren't fussy. They usually don't care whose identity they steal and from whom they get their money. They often target large groups, because this increases their chances of success.

Some people even use radio commercials on trusted channels, so that potential victims are less suspicious. Thousands of people fell for the advert for Mijngratisbox.nl (My free box.nl) which was aired on Sky Radio and public radio. This professionally exercised form of fraud earned them about € 500.000. The 'sponsored' articles were never delivered, while thousands of consumers paid the postage costs.

'Your entire life is online and that can be used against you,' the Belgian banks warn in a short film which warns you about the dangers of internet. When I see the film for the first time I am flabbergasted. A medium with paranormal gifts speaks to numerous people and he can tell them everything about themselves: who is drinking too much, who has a negative bank balance, who has a butterfly tattoo, who has an exciting love life with numerous bed partners, who spends hundreds of euros on clothing each month, how much someone's house is worth…. These people are all shocked: how can someone like Dave know all this? I ask myself the same question. I would like to believe that some people have paranormal gifts, but Dave even guesses the bank account numbers of strangers passing by. At the end of the film the secret is revealed: behind the screens a group of hackers is rapidly gathering information about these people and passing this on to Dave. Nothing paranormal at all, just Google.

It will only become more difficult in the future: even details you don't share will be traceable. The experts predict there will be computers which are thousands of times quicker and can breach any security within seconds.

Hackers are focusing more and more on stealing images. I have already deleted all copies of documents from my computer, including photos where I pose sexily for the camera for my previous boyfriend. Photos are extremely valuable to hackers, because you can steal peoples' identities or blackmail them.

Not that long ago, the FBI arrested a 27-year old man who hacked women's computers looking for naked pictures and personal information. He pretended to be those women and had computer chats with their friends, where he convinced them to pose for naked pictures. He then blackmailed these women and threatened to publish their photos if they didn't send him more naked pictures. He spread some of his bounty on Facebook. The police found pictures of hundreds of women.

We are also vulnerable without hackers, because we unconsciously spread information which can't be deleted later. Even if you are able to delete it from a site, it will just turn op elsewhere on the internet. Poor consolation: we have all become immortal.

It doesn't make a difference for people like Erik Wannee. I'm allowed to know everything about him, because he places it all online: his address, his telephone number, his email address, his bank account number, how long he has been married to Saskia, what kind of work he does (medical examiner) and more. I stumble on Erik's name on an internet forum where he has posted his national insurance number. When I google him and see all the other information I think: if this is a joke, then it has gotten out of hand.

I decide to stop wondering and phone Erik (he didn't post his telephone number on the internet for nothing).

Erik doesn't mind talking about this to a stranger. 'It's not a joke at all,' he says. 'These are all details that can be found on the internet for most people, only they probably don't know it.'

'I don't think my national insurance number is on the internet. Aren't you afraid someone will abuse this when they link all the data?'

'Not really,' he says. 'Anyone can become a victim of identity fraud, even if you don't put anything online.'

'True, but you are making it quite easy for potential troublemakers.'

It's quiet on the other end of the line.

'You know what, see it as a statement,' he says. 'No one is invincible. I was a victim of identity fraud once, but that had nothing to do with publishing all this information. Someone just ordered various items and I received hundreds of emails that I had to pay. A mild form of identity fraud, because my name wasn't right, so I wasn't chased by any bailiffs.'

'So, you thought: just put everything online, perhaps next time something more exciting might happen?'

Erik laughs: 'No, thank you. But I don't think that it will be very simple to abuse my bank account.'

The certainty in his voice surprises me. I have never abused someone's bank account, but this time I'm itching to give it a try. I really want to give Erik a lesson in privacy. I am shocked at my own thoughts. How ethical is it to defraud someone to teach them a lesson, and why do I want to do that? I feel like a privacy Jehovah's witness, while just a little while ago I used weak passwords.

Erik interrupts my thoughts: 'Look, before you think I am a hopelessly naïve person: my boss wants me to scan my signature to sign letters digitally, but I'm not going to start that. It's so easy to use a scanned signature and paste it on to a loan application, for example.

'At least it's a good thing that you are protecting your signature. I think doing just that is insufficient, but I'm old school.'

My thoughts continue to swirl in my mind after hanging up. Of course, I am old-fashioned, I still place some value on privacy and hiding important data. But perhaps Erik is right to say that everyone of us remains vulnerable.

21
The final search

Although Rickey has been serious up until now, this time he lets me down. He is being watched closely by the police and because he is still on probation, he is afraid to carry on. 'I hope you understand,' he writes.

I stare into emptiness. I had prepared well for my search for a trustworthy hacker and now my dream hacker is too afraid to continue. I feel a sense of panic growing.

Rickey is quitting, he's too afraid to carry on, even if he has official permission. He has been improving his ways for some time now and he no longer wants to be in trouble with the authorities.

Has my search been for nothing? No, because Rickey has already shown me a lot, but it's certainly not finished.

I understand Rickey, I do. If I were him, then I would probably also have said: 'Till here and no further.' I also wouldn't like to feel the hot breath of the law in my neck, but how do I find a new trustworthy hacker?

I suddenly think of Holger. He helped me really well with my digital security, perhaps he can now help me to try to break into it? The best security people are experienced hackers themselves and Holger mentioned that he had started on the wrong side of the law.

The problem is that I hardly know him, only from messages on social media. Can I trust him? I had the same dilemma with Rickey, but at a certain point I made my choice and decided to trust him fully. It is actually quite logical not to overthink about Holger either, but to follow my intuition. He seems a nice guy and I want to complete my hacking project.

When I email Holger, I soon get a very enthusiastic reply. 'Hack your computer? No problem. If you like, I can also teach you how to hack someone, personally that seems like the bigger challenge.'

Hmm. Turn a digital novice into a hacker? It does sound exciting, but then I will be breaking the law. If I'm caught of course.

Days before the meeting with Holger I dub about who to hack. I don't want to lose any friends and I'm too afraid to do it by strangers. Without realising it, Holger has put me in an ethical dilemma with his enthusiastic offer.

Of course, I can ask one of my friends beforehand if they wouldn't mind, but I'm afraid no one will find it a nice idea that his or her emails can be read by a stranger. And if I announce it then I run the risk that they will be extra cautious and won't fall into the trap.

The day Holger comes to my house I feel the same excitement people feel when they go to explore new worlds. I think it's great that someone is prepared to explain the secrets of the zero's and one's in my computer.

A slender man with cropped hair rings my doorbell at the appointed time.

'Your house is difficult to find,' he says. 'It even confused my navigation device.'

'I know, and I'm happy about that. Even Google zooms in a bit off-centre. The funny thing is that I get a little more privacy that way without having to do anything.'

'You are worried about your privacy and you are letting yourself be hacked?' Holger looks at me somewhat incredulously.

'Well, it's for the greater good.'

'Sure, but this is an unusual job. I usually don't program any viruses. Although I used to do it quite a lot. Back then you really had to be knowledgeable about computers to write a virus program, nowadays you do an internet search and you find a vast array. It's boring.'

'I have a nice challenge for you. A laptop filled with woodlice.'

'Woodlice?' Holger looks at me as if I have lost my mind.

But I know what is on the Windows laptop he has to hack: my

son's paper about how interesting a woodlouse is. My husband knew that a hacker was coming to the house, and because he doesn't believe in trustworthy hackers, he deleted everything. Except for the woodlouse. My husband also installed the most recent updates and a new antivirus program. I tell Holger this.

'In that case it will be almost impossible to hack your computer,' he says. 'So it's your turn.'

I have no idea if this will end well, but I have arranged a victim. Lina is not too worried about privacy. I asked her nicely. 'It's for an experiment,' I said.

'And I will be your guinea pig?' Lina asked. 'I'm honoured. Except I don't believe in your hacking skills.'

I'm pretty sure I won't be able to get access to Lina's computer on my own, but Holger hasn't come for nothing. He opens his laptop and shows me his program with the virus. 'I used to hack computer systems out of curiosity,' he said. 'I just wanted to know what unknown computers were hiding. Sometimes it was quite exciting, for example all the profiles on a sex site were not encrypted. The ladies gave away all their details and also their telephone numbers in the assumption that only the administrator had access to this locked part of the site. Because I thought he was being careless with their information I sent him an email and explained how easy it was to hack his website. I got a quick reply: 'Fuck you.' Clear language. I then knew what I had to do. I borrowed a friend's laptop and drove to McDonald's to use their Wi-Fi and I deleted the entire database of girls and customers.'

'If this story comes out, then no one will want to swear at you again.'

Holger laughs. 'We'll see. Are you ready?'

I nod and switch on my laptop.

'Okay,' Holger says. Usually you don't need to assist me, but today you do, as we don't have much time. Suppose I send you a link

with an interesting cybercrime game, would you open that?'

'I usually ignore games, but because it has to do with cybercrime, I would be curious. I can hear in your voice that this is a trick.'

'Correct. If you received a similar email from a stranger, you would delete it straight away, but not if a good friend sends it. Most people trust their friends and acquaintances and that's the trick: the people who send these mails often aren't aware that their computer is being used to infect other computers.'

I open my email and see the intended mail.

'Holger, I said that I would click on it and that is what I am going to do. I know now that the content is infected, but if you hadn't warned me beforehand, then I wouldn't have suspected anything.'

One, two, three. Let's see how alert my virus scanner is.

One second later I see a warning on my screen. Malware. That's not good.

'My scanner has unmasked your hacking program,' I say almost triumphantly, as if I had unmasked it myself.

'I was afraid that would happen,' Holger says. 'This program is a little bit old and some virus scanners recognise it.'

'Shall we see if it works on my friend's laptop?'

Holger nods: 'If she didn't install the recent updates, then it has a chance of succeeding.'

'I hope so because she already laughed at me and told me I would be a useless hacker. But it doesn't seem too difficult with a ready-made program.'

I get behind the keyboard and type: 'Hi Lina, I'm going to send you a special game. I know you don't really like games, but this is related to your work. And knowing you, you'll enjoy it.'

I press the 'send' button.

'Can you see if she opens it?'

'Of course, I can see that,' Holger says. 'If she opens it, we will get access to her computer. It won't go unnoticed. Now we wait.'

'Coffee? If it takes too long, then I'll phone her to let her know I've sent her a fun game.'

'Don't get pushy, otherwise she might get suspicious,' Holger replies. 'If you have pre-warned her what you are going to do, then it's not handy to phone her. Just have some patience.'

Hackers often have mountains of patience, but I don't. I flit about restlessly and then I set coffee. A little while later I hear Holger shout out: 'Come and have a look!'

'Are we in?'

'We sure are. I've switched on her camera from a distance.'

Thankfully Lina isn't naked. She is walking in her house towards the kitchen. Her laptop, as always, is on the coffee table.

'Listen, I don't want to peek around extensively in her computer. I just want to know what kind of files you see and if, for example, you can intercept her passwords.'

Holger types in 'stored passwords' into the virus program.

'No passwords. That's quite exceptional, because most people save passwords on their computer.'

'Lina isn't that active on the internet, she probably only needs to remember two.'

'Aha, let's see, what else do we have. Who is Alex?'

'That's her boyfriend.'

Holger brings up a few pictures on the screen. 'This must be Alex.'

'Yes, it looks like a holiday snap. But let's stop, I feel a little uncomfortable.'

'Don't you want to see her emails?' Holger asks.

What a question! Of course, I do. I want to see it all, but at the same time I know I shouldn't want to see these things. What will win: my curiosity or my common sense?

'I think it's better if we leave it at this, Holger.'

'Wait, I want to show you something,' he says. He presses a but-

ton and a miniature keyboard appears on his screen.

'Can you play a tune on this?' he asks.

I press a few buttons and I see Lina looks warily at her computer.

'No way, she can hear what I am playing?'

'Sure, and quite loud too.'

'Poor Lina, a computer that suddenly plays music seems scary to me. As if your house is haunted.'

'Don't worry, we'll explain later that a computer can't do these things on its own accord.'

'Except if I, as a digital novice, operate it from a distance.' You should see me grinning. It is so much fun to do something you have no experience with and it works! That doesn't happen to me that often.

We are able to explain everything to Lina and even show her, because a week ago we agreed that she would come around this afternoon at about 3.00 p.m. for coffee.

We wait for Lina in anticipation.

'What we are doing now is old-fashioned hacking,' Holger says. 'We are making our presence known, and if she is paying attention she will understand what is happening. All hackers used to do that, they would send you a virus, for example, which would spontaneously open your cd-drive and they thought it was fun to tease you this way. You hardly notice the presence of modern hackers in your computer. They don't do it for fun, but for the money.'

I'm pleased that I'm an old-fashioned hacker, I find that exciting enough. Now we just need to wait for Lina's reaction.

She rings the doorbell a short while later.

'That was a weird email you sent me,' Lina says when she enters the house. 'I opened the file with the game, but it didn't work.'

'The file worked, didn't you hear music on your computer? That was part of the game.'

Lina looks at me in surprise. 'How is that possible? I don't un-

derstand.'

'Neither do I, but I hacked you.'

'No way! Did you read my emails?'

'Yes, your entire love letter correspondence with Alex.'

Lina doesn't look amused.

Holger gets involved before it gets out of hand. 'She didn't do that at all. She was very good and wasn't curious at all.'

'Not curious? That's not like Maria.'

'Well, I'm always curious, but I know when to stop. I want us to stay friends.'

'This is the last time you hack me,' Lina says.

'Oh, you think I'm addicted now? It's not like that at all.'

Holger tries to intervene before we get into a long discussion with him as the audience. 'Do you know what we thought was strange, Lina? That you don't save any passwords on your laptop.'

'That's strange?'

'No, that's actually really good. I usually find passwords or copies of documents and you are an exception.

'Well, I don't do much on the computer. The few passwords I have are easy to remember.'

'And of course, you don't change those, which is actually a bad thing,' I say like a know-it-all.

Holger looks at me sharply: 'How often do you change your passwords?'

Uhh. Caught out. That's on my list of good intentions, such as going to the sport school more often, reading more books, saying 'no' more often, trying to please people less, talking to my children more about computers and security, not letting people make copies of my passport and…. I have forgotten the rest.

That is why you have computers. They remember everything I can't, including my strange new password with seventeen digits. Why seventeen? Because that is my lucky number. Of course, the

number seventeen is also included in my new password. Because you can't have enough luck on your side when it comes to identity fraud, the crime of the future.

At least I have learned one thing from the hackers: it pays off to invest in your digital security. Compare it to some sturdy locks on your doors: burglars can enter even the most secure homes, but if you make it difficult, then they will choose a home with bad locks first. Being digitally cloned is a nightmare. You are unique, make sure you stay that way.

Author's comments

Each one of us is and remains vulnerable. I realized that even more after writing this book. I have anonymized a number of victims of identity fraud in this book, because they have already experienced enough problems.

I am not a computer expert, far from it, but I have tried my best to shine a light on identity fraud in an accessible manner.

'Knowledge is power,' they say. That is why I have asked numerous experts to provide tips for people with limited computer knowledge. The list was very long. Don't worry, you don't have to do all of them, and some tips are so easy they will hardly take up any of your time.

I look forward to meeting you on social media. No, I haven't been so spooked that I will now suddenly delete all my profiles. I remain a staunch optimist. And the good thing about social media: we can all use it to spread good solutions in just a few seconds.

- Twitter: **https://twitter.com/genova2**
- Facebook: Maria Genova (books): h**ttps://www.facebook.com/MariaGenovaBooks/?fref=ts**
- LinkedIN: Maria Genova: **https://www.linkedin.com/in/maria-genova-528bb77**

For lectures and keynotes you can contact me on www.mariagenova.nl.

After this book became a bestseller in The Netherlands I gave hundreds of lectures and keynotes on the to-pics privacy, identity fraud and cybersecurity. I have also written a book for children which you can download for free to protect them against cybercrime and other online dangers. There is also a free game based on the book,

which children can play on www.joinhackshield.com.

TIPS

- Don't save your password on your computer. Use (free) programs such as KeePass, LastPass and 1Password, which make up complicated passwords and automatically enter them for you. This means you only need to remember one password. All other passwords are saved by the program. Make sure the password that gives you access to your password manager is very strong and easy to remember.

- Be careful where you download the password program from, because there are also unreliable copies. Always do this through the official websites https://lastpass.com and for KeePass https://keepass.info or via the official apps. If you use password managers you don't have to change your passwords regularly. If you don't use a password manager, then choose different passwords for important sites and make them as long as possible.

- It is better to use password sentences instead of passwords. A password sentence is safer than a regular password because of its length. For example: IDon'tHaveTimeForGoodPasswords00! Also add punctuation marks, numbers and capitals, that makes your password much safer. Don't save your password sentence on your computer or smartphone.

- You can also use a strong standard password and add to it each time. Imagine my password is ILoveToRead123? When I go to Facebook I change it into FBILoveToRead123 and for Amazon.com, when I order a book for example, it would be BooksILoveToRead123. So, you know your standard password and per site you add something to it that has to do with the website

(it can be the name of the site itself). A good password doesn't use your name or date of birth and is made up of at least twelve characters.

- Check whether your anti-virus program is up-to-date. Don't ignore program updates. Hackers use old versions of programs to hijack your computer. If you are working on a document and you don't have time to do the update there and then and restart the computer, don't click away the update, but minimise it so it stays within range of vision. You can carry out the update at the end of the day when you shut down your computer. Switch on the automatic update for your anti-virus program and carry out regular scans (once a month) on all your devices. Always switch on an accompanying firewall.

- Only hand out copies of your ID if that is a legal requirement, for example to government agencies. Many companies aren't allowed to ask for one. Always write down on your copy of the ID that this is a 'copy for car rental company XXX' for example, and the date. This more or less makes it impossible to use for fraud. Don't send a copy if the buyer or seller on websites such as eBay asks for one, because they are widely used for fraud.

- Employers are obliged to keep a copy of your ID in their payroll administration. You can ask them how safe those copies are stored and if the database is encrypted in case hackers attack.

- Never click on links you don't quite trust, even if they are sent by good friends.

- Banks and other financial institutions don't send you emails with questions about your personal details. If you receive such an email, then you can be sure it's a phishing mail. Check if the email address from the sender is correct. Criminals sometimes use email addresses that look like the real one: they just change one letter. Companies don't use free mail boxes such as @hotmail.com, @outlook.com or @gmail.com.

- Use a search engine which doesn't save your digital trail, such as DuckDuckGo www.duckduckgo.com or Startpage.com.

- At first glance, a link in an email might look reliable but check it first to see where it leads you. You can see this by hovering over the link with your mouse, without clicking on it. If it shows a short link (for example with a bit.ly) then you can go to http://urlxray.com/ to see the destination behind the link.

- Do you worry about the security of a website, of whether a file you want to download includes a virus? You can ask for a second opinion from VirusTotal: www.virustotal.com. VirusTotal is a website which checks files and analyses them using many well-known virus scanners. It gives you the possibility of 'using' all these virus scanners at the same time without having to install them.

- If you want to surf safely on the internet you can install HTTPS Everywhere and Privacy Badger. HTTPS Everywhere forces a secured https-connection where possible and Privacy Badger blocks advertisements and trackers which follow you on the internet.

- VeraCrypt is a free and open source program to encrypt your files. You create a kind of extra hard drive on your computer, a so-called 'container'. After entering the password, the external hard drive appears on your computer and you can drag files into it. You can then upload a container-file to the cloud.

- ProtonMail is a free email service, which encrypts emails between users. Your entire inbox is also encrypted, and ProtonMail itself doesn't have access to your emails.

- Don't publish your email address on (public) websites and be careful when you fill in online forms.

- Never click on 'unsubscribe' in spam messages, because instead you are actually confirming that your email address is in use and you will get even more spam.

- To protect against the consequences of ransomware you should regularly make a copy of your files. Automatic back-ups are not recommended, because they can also be abused. Always ensure your computer is working on the latest updates because outdated software contains leaks from which the hijacking software profits.

- On Myaccount.google.com you can indicate that you don't want Google to save your search location and YouTube history and sell it to third parties. You can also delete all the saved data and prohibit Google from linking advertisements to your interests.

- Check which apps collect your personal information: https://www.mypermissions.com.

- Delete apps you no longer use and be cautious when downloading new apps, especially if they are free. Read the terms and conditions. Some apps allow you to switch off your location and sharing of contacts, even afterwards.

- Delete your browser history so that sites which track you cannot read it. You can also set your computer up in such a way that the browser does this automatically. Also delete your cookies (search for 'internet-cache'). A useful programme to tidy up the rubbish on your computer is C-cleaner.

- Make sure your computer is well-secured. Google offers an extra security code which is sent to your mobile. With an extra security code hackers have a more difficult job trying to access your data, even if they have already gotten a hold of your password. Switch on two-factor authentication for Facebook, LinkedIn, Twitter and all other services that offer it. You need to enter a code when you log in from a non-recognised device or search engine. You receive this code in a text message.

- If you say something impulsively on social media, then delete it as soon as possible. This way the damage is limited.

- If you use a computer outside of the home for social media or internet banking, then don't forget to log out. Make sure you untick the box to save your password. Some browsers remember your password, so to be safe you should delete the browser history.

- Via the site disconnect.me you can stop Facebook from following your activities elsewhere on the internet.

- If you don't want trackers, you can use programmes such as Ghostery, Adblock and Do Not Track Me.

- Check your privacy settings on Facebook. Are your friends allowed to share everything? Are they allowed to tag you in photographs? On Facebook you can use the option 'timeline and tagging' to see who can post messages on your timeline. You can also un-tag yourself from photographs on other Facebook pages. You can't stop other people from posting photographs with you on them (for example, at a party), but by un-tagging yourself it makes it more difficult to find the photographs.

- Facebook apps collect a lot of data about you, so try to limit their use. For each app you see a button 'adjust settings'. When you click on it, you can see to whom the app sends posts and what else it is allowed to do in your name. Friends can also publicise everything about you by simply using Facebook apps. The 'apps other people use' allows you to see this. Everything which is ticked here, from your biography to your status updates, are out in the open. You can untick all the boxes if you value your privacy.

- Google yourself every now and then to check your online reputation. Also set up a Google Alert if your name appears on the internet.

- If you have sexy pictures on your computer: don't save them on the hard drive, but on an SD-card or an external hard drive. Don't save a copy of your ID on the hard drive, it's much safer on a USB stick. You can also buy a USB stick which you first need to unlock before you can access the data.

- If you have a hijacking virus on your computer, then look at the website https://www.nomoreransom.org to see if you can remove it without paying. It isn't wise to pay, because this makes this kind of fraud lucrative.

- In the Google dashboard you can see what information the company has stored about you. You can check your account's activity and also what people get to see when they Google you. You can find more tips and tools to protect your privacy on the site Me & My Shadow: https://myshadow.org

- Delete your birthday from Facebook. Many data dealers such as Experian, Acxion and Rapleaf link your 'likes' to your date of birth and then they nearly know with certainty who you are, even if you have a common name.

- Be careful with personal details and don't publish your mobile number, date of birth or place of residence on the internet.

- Children are very open with sharing information about themselves, family and friends. They don't see the dangers. They won't give their address to a stranger they meet on the street, but they do on the internet. Teach your children not to fill in everything the websites ask. The only thing which needs to be correct is usually the email address, because that is where they send the password. The sites don't need to know your real name or your address.

- Schools can help by educating young people about the dangers of sexting, about the dangers of illegal downloading and too much openness on social media, about child abusers which approach young people through online games and about where

they can get more information if something is wrong. Schools usually don't have this expertise, but there are enough professionals who give workshops and lectures on this subject. On www.mariagenova.nl you can download the free book What the hack! and also the free privacy game for children.

- Secure your physical mail box, so that criminals can't steal your post.

- Don't throw away personal documents but use a paper shredder for all confidential information.

- Use programmes such as Eraser, Sure Delete and Wipe Drive if you want to delete your hard drive. Destroy the hard drive if you are throwing away your old computer.

- Don't believe everything and everyone on the internet or even better: believe as little as possible. The number of fake Twitter users is estimated to be 20 million. The internet is full of hoaxes and fake people with great stories and bad intentions.

- It is wise not to buy or sell items from an internet café or from a borrowed laptop, because you don't know if it is well-secured.

- To place your first order from a web shop you need to set up an account and choose a password. Make up a unique and strong password which you don't use for any other website. Don't use your email password.

- Only enter personal data on secure websites with https:// in the URL or with a lock symbol.

- Secure all mobile devices with a password. Many people still secure their mobile with '0000' and '1234'. If you lose your mobile, the finder can read everything on your mobile.

- Only connect to reliable Wi-Fi networks. Open Wi-Fi (for example, McDonald's) is unsafe, hackers can read all your messages and intercept passwords.

- Millions of travel documents and driving licences are lost or stolen each year. This is a great opportunity for look-a-like-fraud. Always report your missing documents to the police and apply for new documents as soon as possible.

- If you receive an email with an attachment or with a shot hyperlink, or a request to log in somewhere, then don't do it, even if you know the sender. The account might be hacked. Only accept the message if you have agreed with each other that the person would send that by mail.

- More than half of businessmen and women have become a victim of cybercrime. If you have a business, regularly check your bank statements for small amounts, because identity fraud often starts with small amounts being debited.

- Only install apps for your mobile or tablet via the official app stores. Don't use illegal copies because of the risk of viruses.

- Close pop-ups with the key combination Alt+F4 (on an Apple this will be Cmd+W). Never click on 'agree' or 'x' or 'no' to close a pop-up, because you can inadvertently install malware this way.

- File a police report if you become a victim of identity fraud. You can recognise identity fraud, for example, if you are denied a loan, receive letters which are not meant for you or suddenly don't receive any more post.

- Check on https://haveibeenpwned.com whether companies/websites have leaked your password and if so, change your password straight away (on all sites you use that password for).

- A strange email address is often a phishing clue. The part behind the @ sign has to end in a domain name. The text for the domain name must be separated by a full stop. Good: newsletter@mail.ing.nl. Bad: newsletter@emaillogin-ing.nl.

- Be careful with shortened links in the mail and on websites. Test to see where the links lead to via www.unshorten.it.

- Be extra careful with the following file extensions when they are included in an email attachment: ZIP: a ZIP-file is used to mask the contents (often an .exe file); .exe: usually always bad news; js .ink . wsf .scr .jar: never open these! They contain scripts which download malware. .doc is a Word document and is usually not dangerous, but if the file asks to install macro's when you open it, then don't do that. Unfortunately the extensions (such as .exe) are hidden as a standard setting in Windows. Activate file extensions so that you can see what kind of file it is. Press the Windows button + R, type in the screen 'control folders' and press Enter. In the tab Display uncheck the box 'Hide extensions for unknown file types'.

- Are you worried if your computer has a virus? Carry out a

free online scan on one of the antivirus websites, for example: ESET Online Scanner, F-Secure Online Scanner or Panda Cloud Cleaner.

- If you have already given the scammer some details, then you need to inform the companies and organisations involved straight away. Warn your bank immediately, you will probably then be eligible for compensation for any damages incurred. Did you fill in a password? Change this password straight away.

- You can check to see if your profile picture is used on other sites on https://image.google.com.

- Always make sure your smartphone, tablet or laptop doesn't automatically search for Wi-Fi networks and connect to 'known networks' because they might not be as innocent as they look. Deactivate the option to store networks you have previously connected to.

- Regularly make a back-up of the important items on your phone. This is common practice for computers and laptops, but not yet for telephones: install an anti-virus scanner on your phone. Anti-virus apps can be found in the app stores but pay attention to the reviews. They can warn you if the app starts to behave suspiciously.

- A free Anti-Ransomware Tool prevents your files being hijacked: https://go.kapersky.com/Anti-ransomware-tool.html.

- Go to settings on your phone and select 'security' and click on 'encrypt'. If you lose your phone, other people will not be able

to access the contents of your smartphone. They will need your password to undo the encryption. A very detailed site which compares privacy tools is https://www.privacytools.io.

- Check to see if your devices are accessible to the public on http://iotscanner.bullguard.com.

- Phishing isn't only limited to email, it can also be done via text messaging and chat-apps. Be very careful when opening links and installing apps.