Quiz Internetveiligheid

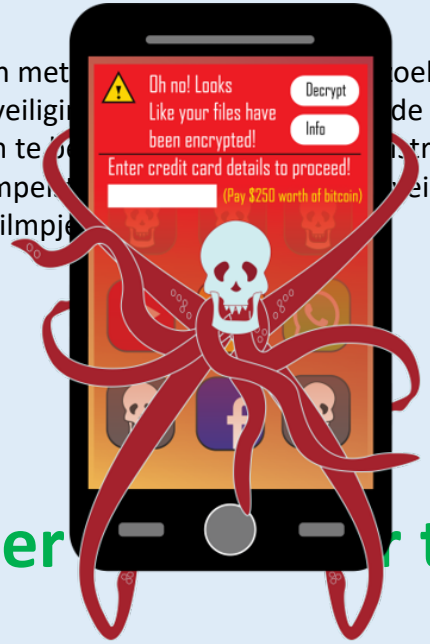
Hoe bescherm je jezelf en je organisatie tegen hackers en diefstal van privacygevoelige gegevens?

Klik hier om verder te gaan

Hoeveel procent van de MKB-bedrijven krijgt te maken met cybercrime?

• A. 20 procent.	✗
• B. 34 procent.	✗
• C. 52 procent.	✓

Antwoord C is juist. De helft van de MKB-bedrijven krijgt te maken met [illegible]oek Alert Online). Ze zijn om meerdere redenen geïnteresseerd in kleinere bedrijven. Ten eerste omdat die minder investeren in beveiligi[illegible]de medewerkers, dus een veel gemakkelijker doelwit zijn. Ten tweede omdat ze de back-ups vaak niet op orde hebben en bereid zijn om te [illegible]tratie met de klantgegevens terug te krijgen. Ten derde omdat kleine bedrijven vaak leverancier zijn van grote bedrijven en dat is de simpel[illegible]eiligde grote bedrijven binnen te komen. Dit filmpje laat zien hoe simpel het is om een computervirus te maken, klik hier voor het filmpje



Klik hier [illegible]r te gaan

Klik bij elk filmpje op het scherm om het filmpje te starten.
Klik aan het einde van het filmpje op de groene balk rechts om naar de volgende vraag te gaan.

Wat is het grootste risico bij een hack van een (relatief) klein bedrijf?

• A. Slechte publiciteit in de media.	✗
• B. Boze en teleurgestelde klanten.	✗
• C. Faillissement.	✓

Antwoord C is juist. De helft van de MKB-bedrijven kr (onderzoek Alert Online). Ze zijn om meerdere redenen geïnteresseerd in kleinere bedrijven. Ten eerste omdat die minder invest ng aan de medewerkers, dus een veel gemakkelijker doelwit zijn. Ten tweede omdat ze de back-ups vaak niet op orde hebben en ber administratie met de klantgegevens terug te krijgen. Ten derde omdat kleine bedrijven vaak leverancier zijn van grote bedrijven en da ed beveiligde grote bedrijven binnen te komen.

Voorbeeld:

Veel kleine ondernemers denken dat hun bedrijf niet interes Xander Koppelmans, eigenaar van ontwerpstudio PHGR. Zijn bedrijf bestond al een kwart eeuw en de zaken gingen goed, met klanten zoals Rijkswaterstaat en Nutricia, was opeens alles kwijt. E-mail, boekhouding, 180.000 beelden klaa emaal weg. Ook de back-ups bleken onbruikbaar. Het winstgevende bedrijf ging failliet.

Klik hier te gaan

Hoeveel Nederlanders werden in 1 jaar tijd slachtoffer van cybercriminaliteit?

• A. 500.000	✗
• B. 1,6 miljoen	✗
• C. 3,4 miljoen	✓

In totaal kregen 3,4 miljoen Nederlanders het afgelopen jaar te maken met cybercriminaliteit. Ze klikten bijvoorbeeld op links in frauduleuze e-mails, ontdekten dat persoonlijke gegevens waren gestolen of kregen te maken met gijzelingssoftware. Dat blijkt uit onderzoek van Norton Cyber Security. Het ministerie van Justitie en Veiligheid constateerde dat ongeveer de helft van alle Nederlanders niet weet hoe ze zich kan beschermen tegen internetcriminelen.

Voorbeeld:

Identiteitsfraude gebeurt niet alleen bij particulieren, maar ook bij bedrijven. Oplichters doen alsof ze een bekend bedrijf vertegenwoordigen, bijvoorbeeld een supermarktketen en bestellen voor miljoenen euro's aan goederen. Alles lijkt te kloppen, ondervond de Nederlandse wijnhandelaar Delta Wines toen er een order van ruim een ton binnen kwam van de Franse supermarktketen Simply Market. De oplichter gebruikte namen van mensen die daar werkten. Ook de e-mailadressen klopten, met als enige verschil dat zij op .com en niet op .fr eindigden. De wijnhandelaar wilde vooruit betaald krijgen, maar dan zou de deal niet doorgaan.
Iets vergelijkbaars overkwam het bedrijf Smith-Holland, dat voor 70.000 euro aan airconditioners zag verdwijnen richting een zogenaamde klant uit Frankrijk. Ook in andere landen werden bedrijven de dupe, waarbij de schade soms opliep tot 250.000 euro.

Klik hier om verder te gaan

Kan iedereen hacker worden?

- A. Nee, daar heb je best veel computerkennis voor nodig. ✗
- B. Ja, vrijwel iedereen zou het kunnen. ✓
- C. Nee, hackers zijn vooral jonge mensen die heel handig zijn met de computer. ✗

Hacken is niet zo moeilijk als de meeste mensen denken. Veel kwaadaardige programma's zijn online te vinden en zelfs gratis. In theorie zou zelfs je schoonmoeder het kunnen. En als ze dat niet kan, dan kan ze altijd nog een hacker vinden die het voor haar doet, want die diensten worden gewoon aangeboden.
Programma's om computers te gijzelen kun je al voor vijftig dollar kopen, inclusief een gratis helpdesk als je er niets van snapt. Voor 50 dollar kun je ook grote bedrijven platleggen. Iemand anders doet het werk, je zegt alleen maar welk bedrijf ze moeten aanvallen en betaalt voor de dienst.

Voorbeeld:
Een aardappelteler krijgt een e-mail van zijn bank. Hij moet op een link klikken, zijn gegevens invullen en de Rabobank stuurt hem zijn nieuwe bankpas per post op. Als zijn partner hun bankrekening controleert, ziet ze tot haar schrik dat alle rekeningen die aan het account hangen, leeggeplunderd zijn. De schade is 215.000 euro.
De aardappelteler doet aangifte. Er zijn nog veel meer slachtoffers. De politie komt op het spoor van vijftien verdachten die phishingmails versturen, mensen opbellen om ontbrekende codes te krijgen, de postbode met de nieuwe pas opwachten en bestellingen plaatsen.
In mei 2019 deed de rechtbank Zeeland-West Brabant uitspraak in de zaak. De twee hoofdverdachten kregen een gevangenisstraf van vijf jaar opgelegd. Ze moeten ook samen ruim 124.000 euro terugbetalen aan een slachtoffer. De verdachten waren volgens de rechtbank de leiders van een bende die bankklanten voor meer dan 1 miljoen euro dupeerde.

Klik hier om verder te gaan

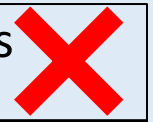
Je ziet op het internet veel foto’s van beroemdheden. Zijn die veilig?

- A. Ja, foto’s zijn veilig. Virussen worden vooral via linkjes en bijlagen in phishingmails verspreid. ✗
- B. Het opvragen van een pagina met foto’s van beroemdheden is veilig, het klikken op de foto niet. ✗
- C. Foto’s van beroemdheden kunnen virussen bevatten. Soms hoef je niet eens de foto te openen. Alleen door te kijken wordt je computer besmet. ✓

Cybercriminelen maken graag gebruik van foto’s en filmpjes van beroemdheden om computers en mobiele telefoons over te nemen. Als je op zoek bent naar informatie over een bekend iemand, kun je zomaar op de verkeerde link klikken en dan is het gebeurd. Kim Kardashian, Doutzen Kroes en Adéle verspreiden dus ongewild virussen. Lil’ Kleine, Max Verstappen en Armin van Buuren ook. Antwoord C is juist en dat is best slecht nieuws: alleen kijken naar zo’n foto is voldoende om je computer te besmetten. Als je niet kijkt, helpt dat niet, want je hebt al een besmette webpagina opgevraagd en eigenlijk ben je al te laat. Hoe kun je in zo’n geval voorkomen dat je computer overgenomen wordt? Ja, meestal kan dat heel simpel: als je updates altijd uitvoert en een goed antivirusprogramma hebt, maken de kwaadaardige Adéle en de slechte Max Verstappen weinig kans om je computer of mobiel over te nemen.

Klik hier om verder te gaan

Je checkt in bij een hotel in een niet EU-land. De medewerker wil een kopie van je paspoort maken. Wat doe je?

- A. Ik geef mijn paspoort. Het lijkt me logisch dat ze willen weten wie daar gelogeerd heeft als er schade is ontstaan. 
- B. Ik weiger mijn paspoort te laten kopiëren. Ik heb van tevoren een kopie gemaakt en schrijf daar zelf op voor welk hotel het is en wanneer ik ingecheckt ben. 
- C. Ik ga vragen waarom ze het nodig hebben, maar als ze moeilijk blijven doen, geef ik het af, want ik ga niet mijn vakantiepret om zoiets onbenulligs verpesten. 

Of een hotel een kopie van je paspoort mag maken, verschilt per land. In Nederland is dat wettelijk verboden om de klanten tegen identiteitsfraude te beschermen. In andere landen is het slim om te weigeren.
Antwoord B is juist: een zelfgemaakte kopie waar je opschrijft waar het voor is, is minder bruikbaar voor het plegen van identiteitsfraude dan een originele kopie. Doorstreep ook je BSN. Of vraag of je ze ter plekke een kopie van je paspoort kunt mailen en gebruik de gratis KopieID app van de Rijksoverheid om een kopie met een soort watermerk te mailen. Daarop staat waar het voor is en wanneer het gemaakt is. Als hackers een hotel hacken (wat geregeld gebeurt), hebben ze wel je gegevens, maar niet een originele kopie die nog waardevoller is voor het plegen van fraude op je naam. Klik hier voor een filmpje over de app ‘KopieID’ (een app die ervoor zorgt dat je veilig een kopie van je paspoort kan sturen. Deze app is gemaakt door de overheid en gratis te downloaden in de Google Playstore en de App Store).

Klik hier om verder te gaan

Klik bij elk filmpje op het scherm om het filmpje te starten.
Klik aan het einde van het filmpje op de groene balk rechts om naar de volgende vraag te gaan.

Je hebt iets online besteld. Bij de meeste webwinkels kun je dat ook op je werk laten bezorgen. De volgende dag ontvang je een mail: ‘Belangrijke informatie over de bezorging van uw bestelling’.

- A. Ik denk niet dat dit een phishingmail is. De hackers kunnen niet weten dat ik iets besteld heb. ✗
- B. Ik twijfel of dit een phishingmail is. Ik open het bericht niet thuis, maar op mijn werk, want op mijn werk zijn ze beter beschermd. ✗
- C. Ik ga eerst checken of het een phishingmail is. Ik weet hoe ik dat moet doen. ✓

Antwoord C is juist. De hackers weten inderdaad niet dat je iets besteld hebt, maar versturen op goed geluk miljoenen van dat soort mailtjes. Namens PostNL, Bol.com, DHL, Zalando, Wehkamp, CoolBlue, etc. Ze hopen dat de mensen die net iets besteld hebben, erin trappen. PostNL bezorgt ongeveer 68 000 pakjes per dag.
Zowel thuis als op het werk kan je computer of laptop ‘gegijzeld’ worden. Op het werk is de schade vele malen groter omdat soms door een simpele klik het hele computernetwerk platgelegd kan worden. Sommige mensen sturen zelfs bepaalde mails die ze privé ontvangen hebben door naar hun werk, omdat ze denken dat de IT-afdeling schadelijke mails kan blokkeren. Dat doen ze natuurlijk wel, maar ze kunnen niet alles blokkeren, want ze zijn afhankelijk van antivirusprogramma’s die niet alle nieuwe malware herkennen.
Hoe check je of iets een phishingmail is? Ga met je muis naar de afzender van de e-mail en klik er op. Bij de meeste phishingmails verschijnt een heel vreemd e-mailadres. Als het e-mailadres goed lijkt, zweef dan met je cursor boven de link, **zonder er op te klikken.** Bij phishingmails zie je dat er een heel andere site verschijnt. Sommige phisingmails bevatten een bijlage. Aan een bijlage is lastig te zien of het kwaadaardig is, maar je kunt het wel vermoeden. Bijlagen met .exe of .zip extensies zijn vaak kwaadaardig. Als je twijfelt of iets een phishingmail is, google de site (bijvoorbeeld PostNL en check via die website hoe laat je pakje aankomt i.p.v. op de link van de mail te klikken).

Klik hier om verder te gaan

Hoeveel procent van de phishingmails wordt gemmideld geblokkeerd door de IT-afdelingen en niet afgeleverd, omdat het vermoedelijk om spam en phishingmails gaat?

• A. 23 procent	✗
• B. 57 procent	✗
• C. 80 procent	✓

C. is het juiste antwoord. Ongeveer 80 procent van de mails die we ontvangen, is ‘troep’ en wordt tegengehouden. Toch is het nog steeds mogelijk dat er spam en phishingmails doorgelaten worden. En daar moet je zelf op letten en niet op klikken. Meld gevaarlijke mails (bijvoorbeeld mails waarin om inloggegevens wordt gevraagd) bij de IT-afdeling. Die kunnen ze blokkeren, zodat de collega’s er ook niet op klikken. De IT-afdeling heeft vaak geen idee wat voor mails de medewerkers ontvangen. Waarom kan de IT-afdeling niet voorkomen dat je dat soort mails ontvangt? Ze kunnen natuurlijk de anti-spam-filter strenger instellen en dan worden alle verdachte mails tegengehouden, maar dan worden mogelijk ook goede mails ten onrechte niet bezorgd. Het is altijd een beetje schipperen tussen veiligheid en gebruiksgemak.

Voorbeeld:

Ook al worden er de meeste gevaarlijke mails weggefilterd, moet je blijven oppassen. Klik op de afzender om die te checken of zweef boven het linkje voordat je een mail opent, ook al twijfel je maar een klein beetje. Als je … mail … opent, kunnen de gevolgen heel groot zijn. Bekijk hoe ondernemers die gehackt zijn dat ervaren hebben, klik hier voor het filmpje.

Klik bij elk filmpje op het scherm om het filmpje te starten.
Klik aan het einde van het filmpje op de groene balk rechts om naar de volgende vraag te gaan.

Wat moet je doen als je op het werk per ongeluk een mail met persoonlijke gegevens naar de verkeerde hebt gestuurd?

- A. Meteen een mail sturen, excuses aanbieden en zeggen dat ze de verstuurde mail als niet verzonden mogen beschouwen. 
- B. Melden als een datalek bij de Functionaris Gegevensbescherming 
- C. Dat soort fouten gebeuren nu eenmaal, dat is zeker geen datalek. Maar ik ga wel de betrokkene even informeren. 

Persoonlijke gegevens naar de verkeerde sturen is altijd een datalek (antwoord B). Dat moet binnen 72 uur gemeld worden aan de Autoriteit Persoonsgegevens. Niet gemelde datalekken kunnen tot boetes leiden. Let altijd bij het versturen van mails of de computer niet toevallig een andere naam selecteert die erop lijkt.

Voorbeeld uit de praktijk:
De Autoriteit Persoonsgegevens verstuurt een email naar 38 journalisten, redacties en relaties om ze te wijzen op het persbericht ‘Wat betekent de privacywet voor jou(w bedrijf)’. Datalekken voorkomen ligt voor de hand, maar in het cc-veld staan 38-emailadressen. De woordvoerder schrikt zich rot en probeert de e-mail in te trekken.
Incidenten met de cc-knop worden vaak gemeld bij de dienst. Bedrijven die niets melden, lopen het risico dat één van de ontvangers zich meldt bij de Autoriteit en dat ze een boete ontvangen wegens het verzwijgen van een datalek.
De Autoriteit Persoonsgegevens kiest ervoor om het datalek te melden bij… de Autoriteit Persoonsgegevens. Een deel van de e-mails is immers herleidbaar naar personen en ze willen het goede voorbeeld geven.

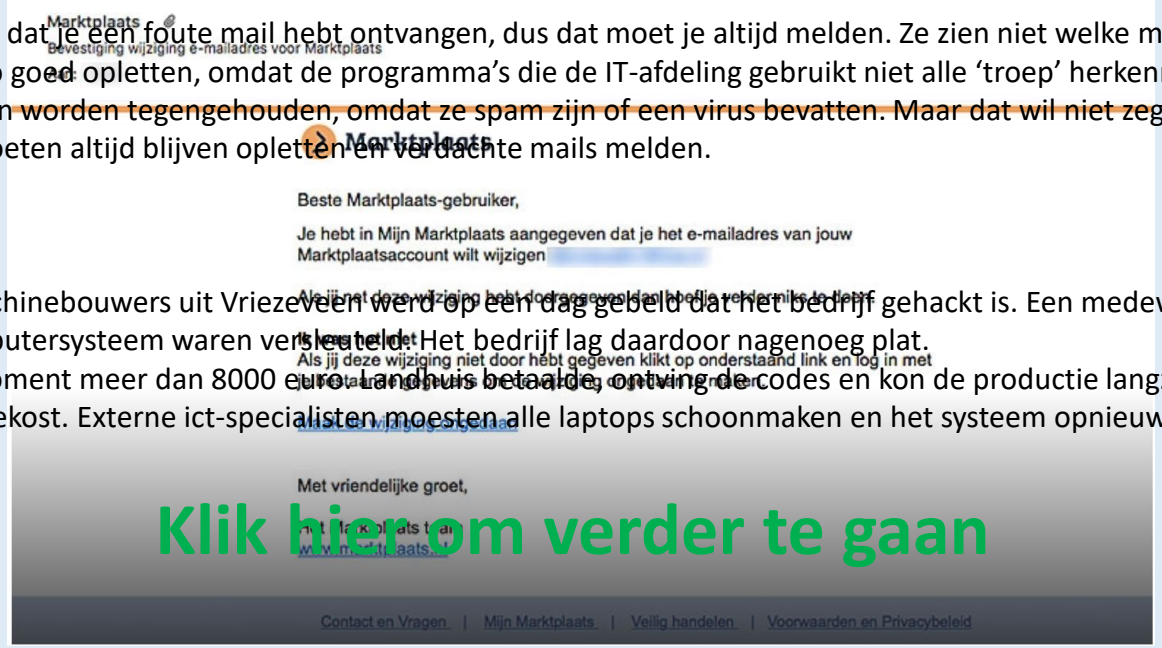
Klik hier om verder te gaan

Binnenkomend e-mailverkeer wordt op een professionele manier gescand op phishingmails, spam en virussen. Wat betekent dat?

• A. Dat de meeste e-mails die we ontvangen worden geblokkeerd, omdat het ’troep’ is.	✓
• B. Dat ik op het werk veel minder hoef op te letten dan thuis.	✗
• C. Dat de IT-afdeling weet als ik een foute mail ontvang, maar ik moet er natuurlijk niet op klikken.	✗

De IT-afdeling weet vaak helemaal niet dat je een foute mail hebt ontvangen, dus dat moet je altijd melden. Ze zien niet welke medewerkers een phishingmail ontvangen. Op het werk moet je net zo goed opletten, omdat de programma’s die de IT-afdeling gebruikt niet alle ‘troep’ herkennen. Antwoord A is juist: ongeveer 80 procent van alle mails die binnenkomen worden tegengehouden, omdat ze spam zijn of een virus bevatten. Maar dat wil niet zeggen dat de mails die doorgelaten worden goed zijn. De medewerkers moeten altijd blijven opletten en verdachte mails melden.

Voorbeeld:



Directeur Frank Landhuis van Almi Machinebouwers uit Vriezeveen werd op een dag gebeld dat het bedrijf gehackt is. Een medewerker had op een fout mailtje geklikt. Alle 1,4 miljoen bestanden in het computersysteem waren versleuteld. Het bedrijf lag daardoor nagenoeg plat.
De hacker vroeg 10 bitcoins, op dat moment meer dan 8000 euro. Landhuis betaalde, ontving de codes en kon de productie langzaam weer opstarten. Het heeft hem alles bij elkaar minstens 60.000 euro gekost. Externe ict-specialisten moesten alle laptops schoonmaken en het systeem opnieuw inrichten.

Onze organisatie is niet interessant voor hackers.

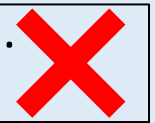
- A. Dat is waar, daar zijn we te klein voor. 
- B. Dat is niet waar, elke organisatie is interessant. 
- C. Dat is waar, want hackers vallen liever banken aan, daar is veel meer te halen. 

Geen enkel bedrijf is te klein voor hackers, ook eenmanszaken worden gehackt. Via overgenomen accounts van leveranciers vallen ze soms de netwerken van grote organisaties aan. Soms is het ook puur toeval dat een organisatie gehackt wordt. De hackers sturen miljoenen phishingmails en weten niet van tevoren wie ze opent. Dus antwoord B is juist: elke organisatie is interessant. Natuurlijk zijn banken extra interessant, maar die zijn veel beter beveiligd dan zorginstellingen en hun medewerkers zijn ook veel beter getraind om de digitale gevaren te herkennen. Dus veel hackers plukken liever het 'laaghangend' fruit. Complete sets met persoonlijke gegevens leveren op de 'Dark Web', de donkere kant van het internet, tegenwoordig meer op dan creditcardgegevens. Dat komt omdat gestolen creditcards heel snel geblokkeerd worden. Persoonlijke gegevens kunnen tientallen keren doorverkocht worden aan criminelen voor allerlei type fraude.

Een voorbeeld uit de praktijk:
Verschillende kunstgalerieën werden gehackt via gelekte e-mailaccounts. Aanvallers hacken de e-mailaccounts van de handelaren en galerieën en wachten totdat die een factuur voor een verkocht kunstwerk versturen. Vervolgens versturen de aanvallers een aangepaste factuur met een ander rekeningnummer en vragen de klant om het geld naar deze rekening over te maken. Aangezien de aanvallers controle over het e-mailaccount hebben reageren ze ook op vragen van de klant over de nieuwe factuur. De schade ligt tussen de 10.000 en 1 miljoen euro. De Londense kunsthandelaar Laura Bartlett raakte zo veel geld kwijt door de hack dat ze haar galerie moest sluiten. Hackers vallen steeds vaker kleine bedrijven op deze manier aan. Dit type fraude komt in alle sectoren voor.

Klik hier om verder te gaan

Wachtwoorden verzinnen is niet zo moeilijk. Maar hoe onthoud je tientallen verschillende wachtwoorden? Kies de makkelijkste en tegelijkertijd veiligste manier.

- A. Je schrijft de wachtwoorden op op je laptop of op je mobiel, zo heb je ze altijd bij de hand. 
- B. Je maakt een supersterk wachtwoord. Dat is niet te hacken, dus veilig te gebruiken op alle sites. 
- C. Je gebruikt een wachtwoordmanager. 

Wachtwoorden digitaal opslaan, is heel onveilig. Als je op een phishingmail klikt, kan een hacker toegang krijgen tot je wachtwoorden. Opschrijven in een notitieboekje is best veilig, zolang je dat boekje niet overal mee naartoe neemt, want dan loop je het risico om het kwijt te raken. Dit is echter geen makkelijke manier, want het is niet handig om elke keer wachtwoorden in een notitieboekje op te zoeken.
Een supersterk wachtwoord gebruiken voor meerdere sites kan tot veel schade leiden. Als een webshop je sterke wachtwoord lekt, kunnen de hackers overal namens jou inloggen en bijvoorbeeld bestellingen plaatsen.
Een aparte zin voor elke website is een zeer veilige manier en het kan goed werken als je niet al te veel wachtwoorden hebt. Bij meer wachtwoorden is het echter niet te doen om te onthouden welke zin bij Marktplaats hoort, welke bij je email en welke bij een webshop.
Antwoord C is juist, maar tegelijkertijd weten veel mensen niet eens wat een wachtwoordmanager is, laat staan dat ze het gebruiken. Een wachtwoordmanager is een programma dat al je wachtwoorden in een soort kluis opslaat en automatisch invult. Je hoeft alleen maar een heel lang hoofdwachtwoord te onthouden. Het kost je misschien een half uur om alles in te voeren en te begrijpen hoe het werkt, maar de rest van je leven heb je er gemak van. De wachtwoorden worden versleuteld opgeslagen en de versleuteling is zo sterk dat het bestand is tegen hackers. Je kunt de wachtwoordmanagers zowel op je computer als op je mobiel gebruiken. Een aantal goede wachtwoordmanagers zijn gratis, bijvoorbeeld LastPass en KeePass. Op het internet vind je zeer uitgebreide uitleg hoe ze werken, bijvoorbeeld op de site van de Consumentenbond. Filmpje: Hoe kraakt iemand een wachtwoord? Klik hier Om de video te bekijken.

Klik hier om verder te gaan

Klik bij elk filmpje op het scherm om het filmpje te starten.
Klik aan het einde van het filmpje op de groene balk rechts om naar de volgende vraag te gaan.

De site mijn-ing.nl is voorzien van een groen slotje en de site bankierenrabobank.nl niet. Wat zegt dat?

• A. Alleen de site met het groene slotje is veilig.	✗
• B. Ze zijn allebei onveilig.	✓
• C. Bankierenrabobank.nl klinkt niet betrouwbaar en dan maakt het groene slotje niets uit.	✗

Let op het groene slotje! Hoe vaak hoor je dat *a*[illegible]'s ook grif gebruik van een groen slotje. Duizenden websites beschikken over een werkend groen[illegible]e inloggegevens of besmetten je met een virus. Elke crimineel kan domeinnamen registreren[illegible]ing.nl of bankierenrabobank.nl . Vroeger kostte het geld, daarom werd het niet zo vaak gedaa[illegible]en dat kan ook gratis. Een groen slotje betekent dat je op een veilige manier een verbinding ma[illegible]den met internetcriminelen. 'mijn-ing.nl' lijkt best veel op de echte loginpagi[illegible]ussen een koppelteken en een punt. Je kunt er vanuit gaan dat een koppelteken vaak fout is, maar o[illegible] B juist: dit waren allebei foute sites met groene slotjes. Wat je in geval van twijfel moet doen? Het beste is om een site te googelen en niet v[illegible]een link naar de site te gaan.

Klik hier om verder te gaan

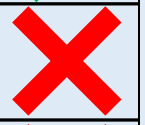
Een programma van je computer vraagt om een update. Wat doe je?

- A. Ik vertrouw dat soort pop-ups niet, dus ik open ze niet en installeer niets.
- B. Ik installeer de update.
- C. Ik doe het niet als ik alles opnieuw moet opstarten. Als ik tevreden ben met de oude versie, hoef ik geen verbeteringen.

Vergelijk de updates met de ramen en de deuren van je huis. Laat je die open als je weggaat?
Natuurlijk niet, want je wilt niet dat inbrekers binnenkomen en je computer stelen. Maar de inbrekers kunnen ook op een afstand alles van je computer stelen als je de updates niet gedaan hebt.
Hoe weten de digitale inbrekers precies jouw laptop of mobiele telefoon te vinden? Meestal is dat puur toeval. Ze scannen de digitale 'poortjes' van miljoenen computers tegelijkertijd en kijken welke niet dicht zijn. Ze komen bijvoorbeeld binnen via een besmette advertentie op een normale website. Je hoeft niet eens op de advertentie te klikken.
Als je de updates hebt gedaan, zoekt zo'n kwaadaardige advertentje naar een open deurtje, maar dat is er niet. Dan gaan de hackers door naar het volgende slachtoffer, naar iemand die de updates niet heeft geïnstalleerd.
Kijk je wel eens naar Formule 1? Als Max Verstappen te langzaam is bij een bocht, dan verliest hij waarschijnlijk de wedstrijd. De winnaar rijdt snel en neemt geen onnodige risico's. Dat doet een update voor je, zorgt ervoor dat de meeste risico's uitgeschakeld worden. Eigenlijk is dat 1 van de snelste manieren om je tegen de hackers te beschermen.

Klik hier om verder te gaan

Sommige emailadressen lijken op elkaar. Welke van die drie is goed?

- A. nieuwsbrief@mail.ing.nl 
- B. nieuwsbrief@maillogin-ing.nl 
- C. nieuwsbrief@mijning-nieuwsbrief.nl 

nieuwsbrief@mail.ing.nl is goed. Het deel achter het @-teken moet eindigen op de domeinnaam. De tekst voor de domeinnaam moet gescheiden zijn met een punt. Een goed uitziend e-mailadres geeft geen garantie, want hackers kunnen email-adressen namaken. Maar meestal doen ze de moeite niet, simpelweg omdat ze weten dat de meeste mensen niet op de afzender klikken. Een paar recente voorbeelden: een mail van bol.com met de tekst: 'Win een Bol.com pakket en een 200 euro cadeaukaart!' Als je op de afzender klikt op je computer of op je mobiel, zie je v@ptgay.tacticpvc.com verschijnen. Dat klinkt niet bepaald als bol.com. Een bericht van Netflix: 'Krijg nu gratis Netflix toegang voor drie maanden!' De afzender is: ci43ijq@insiightly.org.uk 'Een feestelijke mededeling in verband met jubileum IKEA'. Afzender: reply@exur.carbontaekwondo.com. ING heeft de app voor mobiel bankieren verbeterd. De link leidt naar een zeer goed nagebouwde website van de bank. Maar let op de naam in de zoekmachine: healav.men . Dat klinkt heel anders dan ING. Zo zie je maar, onder de hackers heb je ook best veel prutsers. Want ze kunnen ook een site zoals www.verbeterdeING-app.nl registreren. Dat klinkt al een stuk beter. Waar je ook op moet letten, is of de echte site eindigt op bijvoorbeeld nl, com, eu, be of nu. Soms is slechts één van deze van het echte bedrijf en kunnen de andere domeinnamen door hackers gekocht zijn.

Klik hier om verder te gaan

Hackers maken vaak sites na die op de echte lijken. Stel je wilt de tips over veilig internetten lezen op de Belgische site Safeonweb. Welke van de 2 is de goede site?

• A. www.safeonweb.be/tips	✓
• B. www.safeonweb.tips.be/safeonweb	✗
• C. Geen van beide.	✗

Extra tekst vóór de domeinnaam moet gescheide eiden zijn door een schuine streep (/). Antwoord A is goed.
Valse webadressen zijn bijvoorbeeld login-consu euwsbrief2016.nl (geen streep achter de domeinnaam).
Bij twijfel: google het bedrijf, dan kom je vanzelf

Steeds meer apparaten worden ‘smart’, dat wil zeggen gekoppeld aan het internet. Veel mensen hebben slimme thermostaten, smart tv’s, webcams die te bekijken zijn met een mobiele telefoon, etc. Wat moet je met die slimme apparaten doen om ze veilig te houden?

- A. Het standaard wachtwoord veranderen en updates uitvoeren. ✓
- B. Niets, ik ga er vanuit dat de apparaten gekeurd worden en dat er geen onveilige apparaten worden verkocht in Nederland ✗
- C. Een sterk wachtwoord voor mijn wifi-netwerk thuis verzinnen. ✗

Een sterk wachtwoord voor het wifi-netwerk verzinnen is belangrijk, maar het gaat niet helpen tegen het op afstand hacken van slimme apparaten. Helaas zijn veel van de verkochte apparaten niet veilig, omdat ze voorzien zijn van een standaard wachtwoord. Deze wachtwoorden zijn bekend en zo kunnen hackers soms honderdduizenden verschillende slimme apparaten overnemen: van slimme tv’s tot koffiezetters met wifi-verbindingen. Deze gebruiken ze voor massale aanvallen op bedrijven. Er zijn ook veel sites waarop je naar binnen kunt gluren bij mensen door gehackte camera’s die niet goed zijn beveiligd. Je moet altijd de nieuwste updates van slimme apparaten uitvoeren, net als bij een computer. En ook het standaard wachtwoord veranderen.

Voorbeeld:
Met een verzameling van miljoenen slecht beveiligde slimme apparaten vielen hackers het internet aan via Dyn, een dienstverlener waarmee computers websites opvragen. Hierdoor waren populaire websites zoal Netflix, Spotify, Amazon en Twitter nauwelijks te bereiken. Een groot gedeelte van het internet werd via op het eerste gezicht onschuldige webcams, smart tv's, smart lampen en smart koelkasten. Het enige wat de hackers doen om slimme apparaten over te nemen is het standaard wachtwoord intypen. Klik hier voor een video over The Internet of Things

Klik hier om verder te gaan

Klik bij elk filmpje op het scherm om het filmpje te starten.
Klik aan het einde van het filmpje op de groene balk rechts om naar de volgende vraag te gaan.

Je ontvangt een e-mail: 'We hebben geconstateerd dat u auteursrechtelijk beschermde foto's hebt gebruikt. Via deze weg stellen we u aansprakelijk. Zie de bijlage voor meer informatie.'

- A. Het zou kunnen dat ik dat gedaan heb. Bij veel van de foto's die je op het internet vindt staat niet wie de maker is en of de foto gebruikt mag worden. 
- B. Ik geloof niet dat ik dat gedaan heb, ik verwijder de mail zonder die te lezen. 
- C. Ik ga het zekere voor het onzekere nemen en de mail lezen voordat ik het verwijder; straks sturen ze een deurwaarder op me af. 

Geen idee of je wel of niet zonder toestemming foto's hebt gebruikt, maar dit was een phishingmail. Hackers zoeken altijd naar teksten die een grote groep mensen aanspreken, want dan is de kans groot dat ze de kwaadaardige bijlage openen. Antwoord B is in dit geval het meest veilige antwoord: gewoon deze mail verwijderen. Je kunt uiteraard ook even de afzender checken, maar soms worden de namen van de afzenders goed nagemaakt. De hacker kan bijvoorbeeld de domeinnaam ANPclaim.nl registreren en doen alsof ANP de auteursrechten bij je claimt namens een fotograaf. Mail in geval van twijfel terug dat ze hun claim in de mail moeten beschrijven, zonder je te door te verwijzen naar bijlages of linkjes. Een verdachte bijlage kun je ook naar de site van Virus Total uploaden https://www.virustotal.com/nl/ , daar wordt het door tientallen bekende anti-virusprogramma's tegelijkertijd gescand.

Klik hier om verder te gaan

Brandschade kost jaarlijks rond de 600 miljoen. Daar zijn de meeste bedrijven en overheidsinstellingen voor verzekerd. Hoeveel kost cybercrime?

• A. 100 miljoen	✗
• B. 800 miljoen	✗
• C. 10 miljard	✓

Cybercrime is veel onzichtbaarder dan branden, daarom wordt de schade door veel mensen laag ingeschat. De schade aan de Nederland economie door cybercrime bedraagt maar liefst 10 miljard euro per jaar (onderzoek D

Bedankt voor het meedoen. Als je heel geschrokken bent, dan kun je altijd nog terug naar de typmachine ☺. Maar er is goed nieuws: je bent nu veel wijzer geworden en kun je zowel jezelf als je organisatie veel beter beschermen dan voorheen.

www.mariagenova.nl
Wilt u deze demo-quiz binnen uw organisatie verspreiden of de volledige quiz ontvangen, mail dan naar genova@casema.nl