Veiligheidschecklist

Uw online veiligheid is niet gegarandeerd. Daarom geven we u in deze Veiligheidschecklist een aantal tips en adviezen om zo veilig mogelijk te internetten en om te voorkomen dat u slachtoffer wordt van internetcriminaliteit!

Uw apparaat veilig houden

Houd alles up to date

Regelmatig worden er updates aangeboden voor uw apparaat. 'Update' is de Engelse term voor actualiseren of bijwerken. Het besturingssysteem van een apparaat, denk aan Windows 10, iOS of Android, wordt door een update dus bijgewerkt naar de nieuwste versie. Het is belangrijk om dit soort updates altijd uit te voeren, zodat u verzekerd bent van de laatste veiligheidsupdates.

Niet alleen uw apparaat komt regelmatig met updates, maar ook programma's en apps worden regelmatig vernieuwd en moeten dan geüpdatet worden. Oudere versies kunnen namelijk een gevaar vormen voor uw computer, tablet of smartphone.

Maar let op: stuit u surfend op internet op een melding als 'Uw pc loopt risico en moet worden bijgewerkt'? Dit is flauwekul. Met deze meldingen proberen criminelen foute software op uw computer te krijgen. Trap er niet in. Hier geldt: negeren, niet installeren!

Lees ook
www.seniorweb.nl/tip/tip-instellingen-windows-update-controleren
www.seniorweb.nl/tip/tip-apps-updaten-op-een-android-toestel
www.seniorweb.nl/artikel/beveilig-uw-ipad
www.seniorweb.nl/tip/tip-hoe-het-zit-met-android-updates
www.seniorweb.nl/tip/tip-verschil-tussen-update-en-upgrade

Antivirus

Veel mensen denken hun computer extra goed te beveiligen door meerdere antivirusprogramma's te installeren. Dit is echter helemaal niet nodig. Het kan zelfs onhandig zijn om meerdere antivirusprogramma's naast elkaar te laten draaien. De werking van Windows kan hierdoor namelijk verstoord raken, en dat geldt ook voor de werking van de diverse antivirusprogramma's zelf.

Eén antivirusprogramma is dus genoeg. Maar welk programma moet u dan kiezen? U hebt de mogelijkheid om te kiezen uit een betaald of een gratis pakket. Een gratis pakket voldoet in de basis, maar is minder uitgebreid dan een betaalde versie. Daarnaast beschermt een betaald pakket niet alleen tegen virussen die de computer en bestanden kunnen beschadigen, maar ook tegen andere computerbedreigingen als spyware, identiteitsfraude, nepsites die er echt uitzien (phishing) en andere gevaarlijke websites, bijvoorbeeld websites die ongemerkt software proberen te installeren. Wilt u een gratis pakket installeren, dan kunt u het best één van deze pakketten kiezen:

- Avast! Free Antivirus
- Avira Free Antivirus
- AVG

Wilt u toch liever een betaald antiviruspakket aanschaffen? Dan kunt u hier bij de Consumentenbond meer informatie over vinden.

Lees ook
www.seniorweb.nl/tip/tip-een-antivirusprogramma-is-genoeg
www.seniorweb.nl/artikel/keuzehulp-gratis-virusscanner
www.consumentenbond.nl/virusscanner

Stel een wachtwoord in op uw apparaat

Om een apparaat extra te beveiligen is het verstandig deze te vergrendelen met een wachtwoord, pincode, vingerafdruk of gezichtsherkenning. Hoe u een sterk wachtwoord maakt, leest u onder het kopje Een sterk wachtwoord maken. Houd er bij het maken van een pincode rekening mee dat u ook geen makkelijk te raden cijfercombinatie gebruikt, zoals bijvoorbeeld uw geboortedatum.

Lees ook
www.seniorweb.nl/artikel/beveilig-uw-ipad
www.seniorweb.nl/tip/tip-wat-is-touch-id-op-ios
www.seniorweb.nl/tip/tip-samsung-galaxy-tab-beveiligen

Veilig internetten

Thuis veilig verbinding maken met wifi

Een draadloos netwerk moet worden beveiligd. Wie dat niet doet, verstuurt een open signaal. Uw buren zouden dan gratis van uw internetverbinding gebruik kunnen maken. En computercriminelen kunnen proberen op uw computer in te breken via het signaal. Een wifi-signaal is meestal door de internetprovider al beveiligd met een wachtwoord. Het wachtwoord staat op de modem/router vermeld op een sticker. Het is aan te raden het standaardwachtwoord te wijzigen. Verander het in een woord dat bestaat uit cijfers en letters, hoofdletters en kleine letters. Zo maakt u de kans dat iemand uw netwerk binnendringt, zo klein mogelijk.

Lees ook
www.seniorweb.nl/artikel/draadloze-netwerken

Wat wel en niet doen via wifi-spots?

In veel cafés, winkels, hotels en zelfs in het openbaar vervoer en op de camping kunt u het internet opgaan met behulp van wifi-hotspots (ook wel wifi-spots). Handig, want u kunt overal uw e-mail bekijken of de vertrektijd van de trein opzoeken. Maar openbare wifi-netwerken zijn in principe wel onveilig. U kunt prima het nieuws lezen of het weerbericht bekijken. Maar privacy- en fraudegevoelige handelingen, zoals internetbankieren, kunt u beter niet via een openbare wifi-verbinding uitvoeren. Moet u toch die ene betaling doen of even controleren of uw saldo nog hoog genoeg is? Gebruik dan de app in plaats van de website van de bank.

Lees ook
www.seniorweb.nl/artikel/veilig-wifi-gebruiken-onderweg

Herken een veilige website
Elke website begint met http:// Er zijn pagina's die omwille van uw veiligheid extra versleuteld zijn. Denk aan internetbankieren, uw eigen pagina van uw provider of andere webpagina's waar u persoonlijke informatie achterlaat. Deze websites herkent u aan https:// De 's' staat in dit geval voor 'Secure'. Staat er geen 's' achter http, terwijl u wel op een website zit waar u moet inloggen of waar u persoonlijke gegevens in moet vullen, doe dit dan niet!

Zit u op een beveiligde website dan ziet u naast de 's' in de adresbalk ook een gesloten slotje en (vaak) een groen element terugkomen.

Lees ook
www.seniorweb.nl/tip/tip-herken-een-veilige-website

Anoniem surfen op een openbare computer
Maakt u gebruik van een openbare computer in bijvoorbeeld een internetcafé, dan is het raadzaam te internetten via een privésessie. Hiermee voorkomt u dat u gegevens (zoals cookies en browsergeschiedenis) achterlaat op de computer die de gebruikers na u kunnen zien. U stelt een privésessie als volgt in voor Internet Explorer, Edge en Chrome (hoe u dit instelt voor de andere browsers leest u op onze website):

Internet Explorer 11

- Klik rechtsboven in beeld op het plaatje van het tandwiel.
- Klik op **Beveiliging**.
- Klik op **InPrivate-navigatie**.
- Er opent een nieuw venster waarin staat dat InPrivate is ingeschakeld. U kunt in dat venster anoniem internetten.
- Sluit het venster als u klaar bent met anoniem surfen.

Edge

- Klik rechtsboven op de drie puntjes.
- Klik op **Nieuw InPrivate-venster**.
- Er opent een nieuw venster waarin staat dat u kunt 'browsen met InPrivate'. U kunt in dat venster anoniem internetten.
- Sluit het venster als u klaar bent met anoniem surfen.

Chrome

- Klik rechtsboven op de drie puntjes.
- Klik op **Nieuw incognitovenster**.
- Er opent een nieuw venster waarin u zonder sporen achter te laten kunt internetten. Linksboven ziet u een mannetje met hoed in beeld.
- Sluit het venster via het kruisje rechtsboven als u klaar bent met anoniem surfen.

Tip: controleer bij het afsluiten van een openbare pc of u bestanden hebt opgeslagen. Hebt u dat gedaan? Verwijder ze dan van de computer.

Lees ook
www.seniorweb.nl/tip/computertip-anoniem-surfen

Een sterk wachtwoord maken
Voor veel internetdiensten hebt u een wachtwoord nodig. Een wachtwoord is een combinatie van cijfers en letters en soms ook andere leestekens, waarmee op internet uw gegevens worden beveiligd. Het is de 'sleutel' tot uw gegevens. Er is nooit een 100% garantie dat een wachtwoord veilig is, maar er zijn wel een aantal zaken waar u op kunt letten.

Tips voor het maken van wachtwoorden
Gebruik voor elke dienst een ander wachtwoord
Gebruik een combinatie van cijfers, letters (groot en klein) en leestekens.
Gebruik een programma als Lastpass als geheugensteuntje om de wachtwoorden niet te vergeten
Pas de wachtwoorden regelmatig aan

Truc voor het maken van een sterk wachtwoord
Een sterk wachtwoord bestaat uit een reeks van 6 tot 8 willekeurige letters en cijfers, en vaak bent u ook verplicht leestekens te gebruiken. Hoe beter het wachtwoord, hoe lastiger het is te onthouden. Maar gelukkig zijn er trucjes om sterke wachtwoorden te maken die toch redelijk eenvoudig te onthouden zijn. U bedenkt dan voor uzelf een schema dat u altijd toepast. Bijvoorbeeld: [Datum huwelijk][Naam website][Postcode ouderlijk huis][Leesteken]

Een wachtwoord voor een Google-account ziet er dan bijvoorbeeld zo uit: 21031953Gmail1314AA!

En voor de site van SeniorWeb wordt het dan: 21031953SeniorWeb1314AA!

Zo hebt u steeds wisselende sterke wachtwoorden en hoeft u alleen maar te onthouden welk schema u altijd toepast.

Lastpass helpt u uw wachtwoorden te onthouden
Hebt u moeite met het onthouden van alle wachtwoorden van uw accounts, dan kunt u het programma Lastpass gebruiken. Lastpass is een gratis online dienst die binnen uw account alle wachtwoorden bijhoudt van de sites die u gebruikt. U hoeft dan alleen uw hoofdwachtwoord van Lastpass te onthouden.

Lees ook
www.seniorweb.nl/tip/tip-maak-een-sterk-wachtwoord
www.seniorweb.nl/artikel/omgaan-met-wachtwoorden
www.seniorweb.nl/software/lastpass
www.seniorweb.nl/artikel/lastpass-gebruiken

Wat zijn cookies?
Een cookie is een klein, op zich onschuldig tekstbestand dat door een website op de harde schijf van de computer, tablet of smartphone wordt geplaatst wanneer u deze website bezoekt. De belangrijkste functionaliteit van cookies is het onderscheiden van de ene gebruiker van de andere. Er zijn verschillende soorten cookies, waarvan dit de belangrijkste zijn:

- Functionele cookies zijn nodig om een website goed te kunnen laten functioneren. Bijvoorbeeld voor het onthouden van een inlognaam of de inhoud van een winkelwagentje. Deze cookies worden ook wel first party cookies genoemd, cookies die door de website die u bezoekt zelf worden geplaatst.

- Analytische cookies houden bij hoe vaak een website wordt bezocht of hoe vaak een advertentie wordt aangeklikt. De eigenaar van de website of derden kunnen deze cookies plaatsen. Daarom worden deze cookies ook wel third party cookies genoemd, cookies van derden.

- Tracking cookies maken het mogelijk om te volgen welke websites mensen bekijken op internet. Adverteerders maken hier gebruik van om gericht hun advertenties aan de juiste personen te tonen. Deze cookies worden ook third party cookies genoemd.

Lees ook
www.seniorweb.nl/artikel/cookies-wat-moet-u-ermee
www.seniorweb.nl/artikel/cookies-toestaan-en-blokkeren
www.seniorweb.nl/artikel/cookies-verwijderen
www.seniorweb.nl/tip/tip-cookies-weggooien-op-smartphone

Bankieren via de app
In tegenstelling tot wat veel mensen denken, is een bankier-app uitermate veilig. Het is zelfs veiliger dan internetbankieren op de pc. Op de eerste plaats is de app zelf beveiligd met een pincode. Op de tweede plaats verloopt al het bankverkeer via de app. Dit verkeer is versleuteld. Daardoor kan niemand het dataverkeer onderscheppen. Is het toestel gestolen of bent u het verloren, blokkeer dan eenvoudig de toegang van de app. Dat kan vaak online via internetbankieren of door de bank te bellen.

Code app
Als u een bankierapp gebruikt op een mobiel apparaat, dan moet u zorgen dat u dit zo veilig mogelijk doet. Om de bankierapp te openen hebt u een code nodig. Schrijf deze mobiele code voor het bankieren nergens op. Geef de code ook niet aan iemand anders. Als u met andere mensen bent, zorg dan dat zij de code niet zien als u inlogt.

Toegangscode
Gebruikt u een app op de tablet of smartphone om te bankieren, stel dan ook een toegangscode voor het apparaat zelf in. Dat kan via het menu Instellingen. U kiest een cijfercode, wachtwoord of tekening waarmee u het apparaat ontgrendelt. Mocht u uw toestel verliezen, dan kunnen andere mensen niet direct bij uw programma's.

Lees ook
www.seniorweb.nl/tip/tip-mobiel-bankieren-met-apps

Trap niet in de neppers

Phishing, spam, malware en ransomware

Phishing, spam, malware en ransomware: het zijn allemaal manieren om mensen via het wereldwijde web op te lichten. Of men nu via nepmails probeert te vissen naar uw persoonlijke informatie, uw computer gijzelt en losgeld eist, of dat u via het downloaden van software nietsvermoedend kwaadaardige software mee-installeert; een ongeluk zit ook op het internet in een klein hoekje. Gelukkig is er genoeg dat u kunt doen om de risico's zoveel mogelijk te beperken, zie de tips onder Mediawijsheid.

Lees ook
www.seniorweb.nl/artikel/veiligheidsrisico-op-internet
www.seniorweb.nl/artikel/phishing-trap-er-niet-in
www.seniorweb.nl/tip/tip-laat-uw-pc-niet-gijzelen-door-ransomware
Speciaal voor SeniorWeb-leden de phishingchecker: www.seniorweb.nl/phishing

Nepnieuws

Nepnieuws is eigenlijk niets anders dan nieuws dat niet waar is. Maar waarom maakt nepnieuws op internet zo'n grote vlucht? Geld! Door te zorgen dat veel mensen doorklikken op de valse berichten trekt men veel verkeer naar een website. En die sites zijn volgehangen met advertenties. Hoe meer verkeer, hoe hoger de inkomsten. Dat blijkt zo lucratief te zijn dat er een nepnieuwsindustrie is ontstaan. Laat u dus niet om de tuin leiden!

Lees ook
www.seniorweb.nl/tip/tip-nepnieuws-herkennen

Nepwebwinkels

Webwinkels zijn er in alle soorten en maten. Klein en groot, betrouwbaar of juist niet. Controleer voordat u een aankoop doet, altijd of de shop wel in orde is.

Zijn de aanbiedingen te mooi om waar te zijn? Misschien hebt u wel te maken met een nepwebshop. Soms worden bestaande webwinkels nagebouwd. U denkt bijvoorbeeld dat u bij BCC webwinkelt, maar dat is dan helemaal niet zo. De naam is wel verwerkt in het webadres (bijvoorbeeld BCC-almere.com), maar de website is helemaal niet van BCC maar van oplichters. Vaak zijn deze webshops maar heel kort online. Zo kort dat ze zelfs niet in Google voorkomen.

Een paar tips, zodat u niet uw winkelwagentje vult in een nepshop:

- Google op de naam en het webadres van de webshop. Wat voor ervaringen leest u, hoelang bestaat de webshop al? Kunt u niks vinden, dan is dat verdacht.
- Ga na of de webwinkel een keurmerk heeft en doe dit op de website van het keurmerk zelf. Verderop leest u daar meer over.

Keurmerk controleren
Het Thuiswinkel Waarborg is een keurmerk voor veilige webwinkels. Er zijn veel grote en middelgrote winkels bij aangesloten. Via de site Thuiswinkel.org doorzoekt u de ledenlijst. Staat een webwinkel ertussen? Dan kunt u er zonder risico winkelen. Het is overigens niet zo dat winkels die niet zijn aangesloten, meteen onveilig zijn. Het lidmaatschap kost geld en dat hebben kleinere of startende webwinkels misschien niet.

Wees verstandig
Namaakwinkels proberen vaak klanten te trekken met stuntaanbiedingen. Trap er niet in! Zelfs op internet bij betrouwbare webwinkels gelden er minimumprijzen. Als iemand daaronder gaat zitten, is het vaak niet in orde.

Betalen
Probeer waar mogelijk te betalen met PayPal of met de creditcard. Die bieden de mogelijkheid geld terug te laten storten als er iets niet goed is. Bij iDEAL gaat dat niet.

Lees ook
www.seniorweb.nl/tip/tip-onveilige-webwinkels-herkennen

Samenvattend: mediawijsheid

Iedereen wil natuurlijk zo goed mogelijk online beveiligd zijn. Hiervoor kunt u zorgen door sterke wachtwoorden te maken en gebruik te maken van een goed antivirusprogramma. Maar werkelijke computerveiligheid begint bij uzelf. Let altijd op de volgende zaken:

- ☑ Beveilig uw (mobiele) apparaten.
- ☑ Houd uw besturingssysteem en software/apps up-to-date.
- ☑ Gebruik één virusscanner om uw apparaat te beveiligen.
- ☑ Let altijd op waar u uw persoonlijke, financiële en inloggegevens achterlaat.
- ☑ Klik niet zomaar op een link in een e-mail, zeker als u de afzender van de mail niet kent.
- ☑ Open niet zomaar een bestand/bijlage als u niet zeker weet om wat voor bestand of bijlage het gaat.
- ☑ Beantwoord geen spam of andere e-mails waarvan u de afzender niet kent.
- ☑ Is een aanbieding te mooi om waar te zijn? Dan is dat ook vaak zo.
- ☑ Controleer de betrouwbaarheid van de website als u een programma gaat downloaden en klik op de juiste downloadknop.
- ☑ Klik tijdens het installeren van een programma eventueel vinkjes uit, om te voorkomen dat u tevens ongewenste software installeert.

Lees ook
www.seniorweb.nl/artikel/beginnen-met-veiligheid
www.seniorweb.nl/tip/tip-hoofdregels-voor-veilig-internetten
www.seniorweb.nl/artikel/instinkers-bij-het-downloaden
www.seniorweb.nl/artikel/in-10-stappen-veilig

Digitaal Fit met SeniorWeb

Wilt u ook graag de gemakken van de computer en internet leren kennen? Of wilt u meer kunnen doen met de tablet of computer? Denk aan contact met de (klein)kinderen via Facebook of e-mail, foto's maken met de tablet of via internet een reis boeken. Digitaal Fit zijn noemen we dat bij SeniorWeb. En daar helpen wij u graag bij!

SeniorWeb maakt de digitale wereld al sinds 1996 begrijpelijk met stap-voor-stapuitleg en duidelijke voorbeelden. Zo kan iedereen het gemak en plezier van de computer en internet ervaren. En komt u er even niet uit? Of heeft uw computer of tablet ineens kuren? Dan helpen onze geduldige en deskundige vrijwilligers u graag weer op weg.

Lid worden van SeniorWeb

Meld u nu aan voor 2018 voor slechts € 31,- en u bent de resterende maanden van 2017 gratis lid. Bovendien ontvangt u gratis het boek *Veilig en vertrouwd online*. Als lid profiteert u van de volgende voordelen:

- ✓ Ongelimiteerde online helpdesk
- ✓ Telefonische computerhulp én zelfs bij u thuis
- ✓ 4 x per jaar computertijdschrift Enter
- ✓ Onbeperkt toegang tot de phishingchecker
- ✓ Wekelijks informatieve nieuwsbrieven
- ✓ Online Cursussen over populaire onderwerpen
- ✓ Voordelige computerboeken en accessoires

Profiteer direct van onze ledenvoordelen en meld u aan via www.seniorweb.nl/actie-veiligheidsquiz Met het SeniorWeb-lidmaatschap bent u verzekerd van begrijpelijke informatie en persoonlijke computerhulp. Dit aantrekkelijke aanbod is geldig tot en met 31 december 2017. Het lidmaatschap geldt tot wederopzegging.

Vragen? Bel ons op 030 - 276 99 65.

Vragen en antwoorden Veiligheidsquiz

Vraag 1

Vraag: U zit op een openbare wifi-verbinding en moet wat bankzaken regelen. Wat is de veiligste manier?

Antwoord: Via de app van de bank

Uitleg: Wanneer u op een openbare internetverbinding bankiert via de website van uw bank, loopt u het risico dat mensen meekijken. Criminelen kunnen namelijk het signaal onderscheppen en vervolgens meelezen. Bankiert u via een app dan is dit onmogelijk, omdat er via bepaalde verificatiecodes gecommuniceerd wordt tussen de bank en de app.

Vraag 2

Stelling: De bijlage in een mail van een bekende is altijd veilig te openen

Antwoord: Niet waar

Uitleg: Simpelweg klikken op een bijlage kan er al voor zorgen dat er malware geïnstalleerd wordt op de computer, tablet of smartphone. Ook als de afzender een bekende van u is. De mail kan bijvoorbeeld uit naam van die persoon zijn verstuurd, zonder zijn of haar weten. Een virusscanner die dagelijks geüpdatet wordt beschermt tegen de meeste bedreigingen, maar een garantie hebt u nooit. Open daarom nooit zomaar een bijlage in een e-mail.

Vraag 3

Vraag: Koppel de juiste pakketten.

Antwoord & uitleg:

- Kaspersky: Kaspersky is een betaald en Nederlandstalig antivirus- en beveiligingspakket (er zijn verschillende varianten beschikbaar) voor alle apparaten.
- Defender: Windows Defender is de gratis antivirussoftware die standaard wordt meegeleverd met een Windows 10-computer.
- Avira: Avira is een gratis en Nederlandstalig antivirusprogramma voor Windows-computers.
- Norton: Norton is een betaald en Nederlandstalig antivirus- en beveiligingspakket (er zijn verschillende varianten beschikbaar) voor alle apparaten.
- McAfee: McAfee is een betaald en Nederlandstalig antivirus- en beveiligingspakket (er zijn verschillende varianten beschikbaar) voor alle apparaten.

Vraag 4

Vraag: Wat is phishing?

Antwoord: Phishing is het vissen (hengelen) naar inlog-, persoons- en bankgegevens van gebruikers. Dit gebeurt via (massaal verzonden) e-mails of berichten op social media.

Uitleg: Phishing is het vissen (hengelen) naar inlog-, persoons- en bankgegevens van gebruikers. Dit gebeurt via (massaal verzonden) e-mails of berichten op social media. Daarin wordt gevraagd in te loggen op een website die sprekend lijkt op die van bijvoorbeeld een

bank. Het is echter een nepsite. Als u inlogt, worden de inloggegevens meteen doorgestuurd naar de fraudeur. De oplichter probeert vervolgens met die gegevens de bankrekening te plunderen.

Vraag 5

Stelling: Hoe meer virusscanners hoe veiliger.

Antwoord: Niet waar

Uitleg: De bescherming van een antivirusprogramma werkt het beste als u maar één antivirusprogramma gebruikt. Zijn er meer actief, dan kunnen de antivirusprogramma's elkaar gaan tegenwerken. Dit kan leiden tot gaten in de bescherming. Het is dus een noodzaak om maar één antivirusprogramma tegelijk te gebruiken.

Vraag 6

Vraag: Wat is ransomware?

Antwoord: Kwaadaardige software die bestanden ontoegankelijk maakt. Om weer toegang te krijgen moet u betalen.

Uitleg: 'Ransom' is een Engels woord. Het betekent 'losgeld'. Ransomware is kwaadaardige software die de computer gijzelt en vervolgens losgeld eist. Alle bestanden op een pc, of de pc zelf, worden versleuteld. Ze gaan op slot en de gebruiker kan er niets meer mee. Na betaling maken de criminelen de versleuteling hopelijk weer ongedaan.

Vraag 7

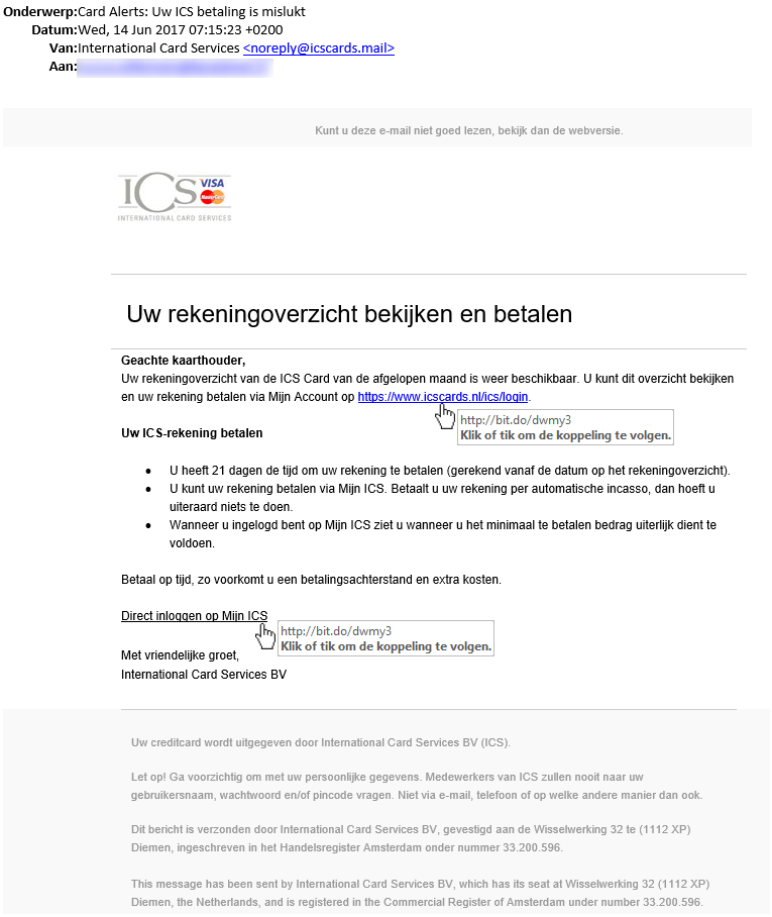
Stelling: Uw bank vraagt in een e-mail nooit om uw beveiligingscodes.

Antwoord: Waar

Uitleg: De bank vraagt nooit om inloggegevens of beveiligingscodes. Zie het als uw pincode, die geeft u ook niet zomaar uit handen. Advies: log altijd zelf rechtstreeks in op de site van de bank en gebruik niet een link uit een e-mail.

Vraag 8

Stelling: Dit is een phishingmail



Onderwerp: Card Alerts: Uw ICS betaling is mislukt
Datum: Wed, 14 Jun 2017 07:15:23 +0200
Van: International Card Services <noreply@icscards.mail>
Aan:

Kunt u deze e-mail niet goed lezen, bekijk dan de webversie.

Uw rekeningoverzicht bekijken en betalen

Geachte kaarthouder,
Uw rekeningoverzicht van de ICS Card van de afgelopen maand is weer beschikbaar. U kunt dit overzicht bekijken en uw rekening betalen via Mijn Account op https://www.icscards.nl/ics/login.

http://bit.do/dwmy3
Klik of tik om de koppeling te volgen.

Uw ICS-rekening betalen

- U heeft 21 dagen de tijd om uw rekening te betalen (gerekend vanaf de datum op het rekeningoverzicht).
- U kunt uw rekening betalen via Mijn ICS. Betaalt u uw rekening per automatische incasso, dan hoeft u uiteraard niets te doen.
- Wanneer u ingelogd bent op Mijn ICS ziet u wanneer u het minimaal te betalen bedrag uiterlijk dient te voldoen.

Betaal op tijd, zo voorkomt u een betalingsachterstand en extra kosten.

Direct inloggen op Mijn ICS

http://bit.do/dwmy3
Klik of tik om de koppeling te volgen.

Met vriendelijke groet,
International Card Services BV

Uw creditcard wordt uitgegeven door International Card Services BV (ICS).

Let op! Ga voorzichtig om met uw persoonlijke gegevens. Medewerkers van ICS zullen nooit naar uw gebruikersnaam, wachtwoord en/of pincode vragen. Niet via e-mail, telefoon of op welke andere manier dan ook.

Dit bericht is verzonden door International Card Services BV, gevestigd aan de Wisselwerking 32 te (1112 XP) Diemen, ingeschreven in het Handelsregister Amsterdam onder nummer 33.200.596.

This message has been sent by International Card Services BV, which has its seat at Wisselwerking 32 (1112 XP) Diemen, the Netherlands, and is registered in the Commercial Register of Amsterdam under number 33.200.596.

Antwoord: Waar

Uitleg: Dit is inderdaad een phishingmail. Dat ziet u aan de volgende punten:

- De afzender klopt niet (noreply@icscards.mail is geen bestaand adres van ICS).
- Een persoonlijke aanhef ontbreekt (geachte kaarthouder).
- De twee links in de tekst zijn gek (http://bit.do/dwmy3).

Vraag 9

Vraag: Wat ziet u in de adresbalk van een beveiligde website?

Antwoord: Gesloten slotje, iets van groen, https.

Uitleg: Wanneer u via internet bankzaken regelt of ergens persoonlijke gegevens achterlaat is het belangrijk om, voordat u begint, een aantal zaken te controleren. Bekijk of de adresbalk groen is (of groene elementen heeft), deze een gesloten slotje bevat en de url met 'https' begint. Voldoet de adresbalk aan deze drie criteria, dan kunt u veilig uw zaken regelen. Zo niet, rapporteer aan de bank of het bedrijf dat er (waarschijnlijk) een valse website in omloop is. Dan kan de bank actie ondernemen. **Let op:** in Edge wordt niet altijd een groen element getoond, dit betekent echter niet dat de website niet veilig is. Websites

die in Edge een groen element bevatten zijn nog extra gecontroleerd en geverifieerd. Controleer in die browser daarom altijd goed of het slotje gesloten is en de url https bevat.

Vraag 10

Vraag: U bent op internet aan het werk en ziet deze melding, wat doet u?

Antwoord: U negeert de melding, want het is flauwekul.

Uitleg: Met dit soort nepmeldingen of nepwaarschuwingen proberen criminelen malware te installeren op uw computer. Aan de hand van deze malware proberen ze vervolgens de pc 'af te luisteren' wanneer u bijvoorbeeld internetbankiert of wachtwoorden invult.