Cybersecurity

Vandaag gaan we het hebben over Cybersecurity.
Het meest voorkomende vorm van oplichting is wel Phishing in verschillende vormen.
Een ieder heeft er wel eens mee te maken gehad.
Het is niet meer dan oplichting via internet of telefoon.
Criminelen maken gebruik van het vertrouwen en de angst van mensen om te proberen inloggegevens van bankrekening te stelen of losgeld te vragen.
Al in de 70-jaren kwam Cybersecurity voor. Vanaf 1996 ging men het Phishing noemen. Dan praten we al over een kleine 30 jaar geleden.
Phishing komt over de gehele wereld wel voor. Met name vanuit oost europa, Rusland, India, Pakistan, China en Afrika. Vrij recent nog zijn een aantal jongeren in de leeftijd van 12 tot 15 jaar in Nederland opgepakt voor phishing. Zij zouden minstens 6 slachtoffers gemaakt hebben.
Doordat de computers tegenwoordig zo dicht gespijkerd zijn voor hackers neemt Phishing alleen maar toe.
Het is nu bijna een dagelijkse uitdaging voor een gemiddelde internet gebruiker om Phishing te ontdekken en af te stoppen.

We gaan de verschillende vormen van Phishing bespreken zoals phishing zelf, Vishing, Smishing, WhatsApp-fraude, randsomware, Ddos-aanvallen, identiteitsfraude, malware, virussen en nog veel meer.
Hoe je verschillende vormen van Phishing kan herkennen.
Wat je zelf kan doen om je er tegen te beschermen.
Waar je het kan melden. Ook als je toch slachtoffer ben geworden.

Mijn grootste aanval die ik mee maakte was een randsomware via Kick-Ass. Het had toen heel Nederland in zijn greep. Criminelen lieten voorkomen alsof de FBI uit America de download site Kick-Ass hadden overgenomen. Kick-Ass is te vergelijken als Piratenbay. Een ieder die inlogde bij Kick-Ass werden bij hen een aantal bestanden versleuteld. Om je bestanden weer terug te krijgen moest je bij een bepaalde site melden. Dat heb ik nooit gedaan.
Ik heb de versleutelde bestanden als verloren beschouwd. Nu werk ik met twee desktop. Één met onbelangrijke zaken waarop ik download en de ander waarop ik foto’s bewaar, bankzaken en serieuze mails op doet. Bestanden die mij heilig zijn heb ik op een externe harddisk bewaard. Deze harddisk staat los van netspanning en computers.
Kick-ass is wel uiteindelijk door de Amerikaanse autoriteiten uit de lucht gehaald.

Wat ook onder cybermisdaden vallen zijn zaken als 'wraakporno', cyberstalking, intimidatie, pesten en seksuele uitbuiting van kinderen. Dit kan heel veel impact hebben op de slachtoffers en kan ook grote gevolgen voor hen hebben. Met name psychisch.

Wat is phishing.
Phishing is waarbij criminelen via valse misleidende e-mails, telefoontjes of sms'jes proberen inloggegevens zoals wachtwoorden, bankgegevens, creditcardnummers met wachtwoorden, online inloggegevens voor sociale mediaprofielen en meer te stelen.
Het lijkt alsof ze van een betrouwbare bron komen, zoals een bank of een bekende dienst.
Het kan ook een e-mail zijn die lijkt alsof hij van een familielid, of een beroemd iemand af komt of van een grote organisatie, zoals deurwaarde bureaus, PayPal, Amazon, Microsoft, ziggo, kpn, banken, overheidsinstantie en zelfs van de HCC.
De berichten lijken echt en dringend. Dit om angst te zaaien, waarbij ze de slachtoffers verleiden om op links te klikken, malware te downloaden of worden omgeleid naar valse websites om inloggegevens, financiële gegevens af te geven of om geld over te maken.
De niets vermoedende slachtoffer is hierdoor kwetsbaar voor identiteitsdiefstal en financieel verlies.
Phishing is bijzonder effectief omdat het misbruik maakt van de menselijke psychologie in plaats van geavanceerde technische tactieken. Vaak vermomd als dringende mededelingen van gezaghebbende figuren, maken phishing-oplichtingen gebruik van het vertrouwen en de angst van mensen.

Hoe herken je Phishing.
1. Let op onregelmatigheden of eigenaardigheden in de e-mail. Door waakzaam te zijn.
2. Gebruik de "geurtest" om te bepalen of er iets niet klopt volgens jou.
3. Vertrouw op uw instincten, maar blijf uit de buurt van angst, want phishing scams maken vaak gebruik van angst om het oordeel van jou te beïnvloeden.

4. Bij twijfel neem zelf contact met voor jou bekende wegen met de bewuste instantie/persoon (bank, bedrijf of belastingdienst) en vraag om bevestiging dat de informatie wel of niet klopt.
5. De e-mail kan een aanbod bevatten dat te mooi is om waar te zijn. Het kan beweren dat je de hoofdprijs hebt gewonnen, een extravagant cadeau, of andere onwaarschijnlijke beloningen.
6. De afzender van een mail of sms-bericht is herkenbaar, maar niet iemand met wie je normaal gesproken contact heb. Wees voorzichtig als je de naam van de afzender zelf herkent of als het niet iemand is met wie je regelmatig communiceert of vooral als de inhoud van de e-mail niets te maken heeft met je gebruikelijke taken. Wees ook op je hoede als je op c.c. staat met onbekende personen of collega's uit niet-gerelateerde afdelingen.
7. De boodschap boezemt angst in. Wees voorzichtig als de e-mail geladen of alarmerende taal gebruikt om een gevoel van urgentie op te wekken, waarbij u wordt aangespoord om te klikken en "onmiddellijk te handelen" om te voorkomen dat de account wordt beëindigd. Onthoud dat legitieme organisaties niet om persoonlijke informatie vragen via e-mail.
8. Het bericht bevat onverwachte of vreemde bijlagen. Deze bijlagen kunnen malware, ransomware of andere online dreigingen bevatten.
9. Het bericht bevat links die twijfelachtig lijken. Zelfs als de bovenstaande indicatoren geen argwaan wekken, vertrouw ingebedde hyperlinks nooit blindelings. Beweeg je cursor over de link om de werkelijke URL te onthullen. Let vooral op subtiele spelfouten in een ogenschijnlijk bekende URL van een website, want dat is een waarschuwingssignaal voor bedrog. Het is altijd veiliger om de URL handmatig in je browser in te voeren in plaats van op de ingesloten link te klikken. Verder waar je op kan letten is onbekende afzender e-mailadressen, algemene begroetingen, spel- en grammaticafouten en misleidende URL's.
10. Controleer of de URL van de pagina begint met "HTTPS" in plaats van alleen "HTTP". De "S" staat voor "secure". Het is geen garantie dat een site legitiem is, maar de meeste legitieme sites gebruiken HTTPS omdat het veiliger is. HTTP-sites, zelfs legitieme, zijn kwetsbaar voor hackers
11. Kijk uit naar het digitale certificaat van een website. Om die bescherming te versterken, als je een e-mail krijgt van een bron waar je niet zeker van ben, navigeer dan handmatig naar de gegeven link door het legitieme websiteadres in te voeren in uw browser. Beweeg de muis over de link om te zien of het een legitieme link is. Als je vermoedt dat een e-mail niet legitiem is, neem dan een naam of een tekst uit het bericht en voer die in een zoekmachine in om te zien of er bekende phishing-aanvallen bestaan waarbij dezelfde methoden worden gebruikt.

Spear Phishing
Spear phishing is een gerichte vorm van phishing waarbij aanvallers berichten op maat maken voor specifieke personen of organisaties, met behulp van verzamelde gegevens om het bedrog overtuigender te maken. Dit vereist verkenning voorafgaand aan de aanval om namen, functietitels, e-mailadressen en dergelijke te achterhalen.
De hackers struinen het internet af om deze informatie te matchen met andere onderzochte kennis over de collega's van het doelwit, samen met de namen en professionele relaties van belangrijke werknemers in hun organisaties. Op basis hiervan maakt de phisher een geloofwaardige e-mail.
Voorbeeld: Fraudeurs kunnen zich voordoen als leidinggevenden om werknemers te verleiden tot het autoriseren van frauduleuze betalingen.
Zelf heb ik dit meegemaakt met een email die leek als of hij van de voorzitter George af kwam. Of ik hem kon helpen met cadeaubonnen voor HCC-leden. De afkomstige email adres gaf mij argwaan. Door zelf George te benaderen kwam ik er achter dat de mail niet van hem kwam.

Walvis phishing
Whale phishing richt zich op prominente personen, zoals leidinggevenden, beroemdheden of C-level zakenmensen. Het probeert hen te misleiden om persoonlijke informatie of professionele details prijs te geven.

Business email compromise (BEC)
Een business email compromise (BEC) aanval richt zich op iemand in de financiële afdeling van een organisatie, vaak de CFO, met de bedoeling hen te misleiden grote geldbedragen over te maken. Aanvallers gebruiken vaak social engineering technieken om de ontvanger ervan te overtuigen dat het sturen van het geld urgent en noodzakelijk is.

Clone phishing
Bij deze aanval maken criminelen een kopie—of clone—van eerder ontvangen, legitieme e-mails die een link of een bijlage bevatten. De phisher vervangt vervolgens de links of bijgevoegde bestanden door schadelijke vervangingen, vermomd als het echte werk. Nietsvermoedende gebruikers klikken op de link of openen de bijlage, wat vaak toestaat dat hun systemen worden overgenomen. Vervolgens kan de phisher de identiteit van het slachtoffer vervalsen om zich voor te doen als een vertrouwde afzender voor andere slachtoffers binnen dezelfde organisatie.

419/Nigeriaanse oplichting
Een uitgebreide phishing e-mail van iemand die beweert een Nigeriaanse prins te zijn, is een van de oudste en langstlopende oplichtingen op internet. Deze "prins" biedt je ofwel geld aan, maar zegt dat je eerst een klein bedrag moet sturen om het te claimen, of hij zegt in de problemen te zitten en geld nodig te hebben om het op te lossen. Het nummer "419" wordt geassocieerd met deze scam. Het verwijst naar het artikel van het Nigeriaanse Wetboek van Strafrecht dat handelt over fraude, de aanklachten en straffen voor overtreders.

Vishing (Voice-phishing)
Oplichters bellen je en doen zich voor als een medewerker van een bank, overheidsinstantie of klantenservice. Ze proberen je te overtuigen of bang te maken zodat je persoonlijke gegevens te delen of geld over te maken.

Smishing (SMS-phishing)
Vergelijkbaar met vishing, maar je ontvangt dan een sms met een urgente boodschap, zoals een pakketbezorging of een probleem met je bankrekening. Deurwaarde bureau dat er een schuld open staat. De schadelijke link in het bericht leidt naar een nepwebsite die je gegevens probeert te stelen.

WhatsApp-fraude
Criminelen doen zich voor als een familielid of vriend en sturen een bericht waarin ze dringend geld nodig hebben. Vaak gebruiken ze een gestolen of gehackt account om geloofwaardig over te komen.

Nepmails van bekende bedrijven
De e-mail bevat een link naar een nagemaakte website waar je gevraagd wordt om inloggegevens in te voeren.

Phishing via online advertenties
Sommige advertenties op sociale media of websites leiden naar valse pagina’s die eruitzien als legitieme diensten. Hier wordt geprobeerd je gegevens te ontfutselen.

Catphishing
Een misleidende tactiek waarbij aanvallers nep online personage creëren om individuen te lokken in romantische relaties voor financiële uitbuiting of toegang tot persoonlijke informatie.
Dit lijkt ongelofelijk maar ik ken iemand die echt dacht verkering te hebben met een vrouw in Dubayy. Hij is zijn hele erfenis er aan kwijt geraakt en gelooft nog steeds dat die vrouw te goede trouw is. Contact had hij via videobellen.

Randsomware
Hierbij worden bestanden versleuteld en losgeld wordt geëist om ze te ontgrendelen.
Ik heb een keer een situatie meegemaakt waarbij de gehele computer werd vergrendeld.
Tijdens het opstarten werd de machine een paar secondes vrijgeven. Voor mij voldoende om de Randsomware in de opstart uit te schakelen.

Ddos-aanvallen
Hierbij worden websites of netwerken overspoeld met verkeer om ze onbereikbaar te maken.
Het enigste wat ik mij kan voorstellen is dat men die bedrijven en organisaties willen afpersen om dit soort aanvallen te laten stoppen of voorkomen.

identiteitsfraude
Hierbij worden persoonlijke gegevens gestolen en misbruikt.
Hierbij kan je van alles bij voorstellen. Dus is het zaak dat er snel actie wordt ondernomen.
Later hier meer over.

malware
Door het openen van bijlagen of bij installeren van programma's van twijfel achtige afkomst worden software ook wel virussen in de computer geplaatst en geactiveerd. Hierdoor kan je lastig gevallen wordt met reclame pop ups, jou bestanden kunnen versleutelen worden, jou systeem kan op afstand worden overgenomen of zelf jou systeem kan plat legt worden.
In meerdere of mindere maten heb ik deze zaken wel voorbij zien komen. Met een virusscanner zijn de meeste zaken wel te voorkomen. Het is wel een rare gewaarwording als je jou muis in eens ziet bewegen. Deze hacker had echt mijn machine overgenomen. Doordat ik wist wat ik het laatst had geïnstalleerd was deze malware gauw weg.

Hoe je zelf kan beschermen

1. Gebruik sterke wachtwoorden – Kies unieke en complexe wachtwoorden voor al je accounts en gebruik een wachtwoordmanager. Een wachtwoordmanager fungeert als een digitale kluis waarin al je wachtwoorden veilig worden opgeslagen. Het gebruik hiervan is tegenwoordig eigenlijk geen aanrader maar een must. We hebben zomaar 80 accounts en het is verstandig voor elk account een uniek én sterk wachtwoord te hebben. Maar hoe ga je die allemaal verzinnen en onthouden? Verzin één sterke wachtwoordzin voor je wachtwoordmanager en laat je app wachtwoorden voor al die andere accounts verzinnen en onthouden. Dan maak je het hackers lastig en zijn niet al jouw accounts toegankelijk als er één bedrijf een datalek heeft. Een wachtwoordmanager werkt als volgt. Je voegt je wachtwoorden toe aan de manager, en deze onthoudt ze voor je. Wanneer je een website bezoekt, vult de wachtwoordmanager automatisch je inloggegevens in. Veel wachtwoordmanagers kunnen sterke, unieke wachtwoorden aanmaken zodat je niet telkens een makkelijk te raden wachtwoord gebruikt. Je hebt één hoofdwachtwoord nodig om toegang te krijgen tot de wachtwoordmanager. Dit is het enige wachtwoord dat je moet onthouden! Als je de wachtwoordmanager gebruikt op je telefoon én je computer, worden je wachtwoorden gesynchroniseerd zodat je overal toegang hebt. Het bespaart tijd én zorgt ervoor dat je wachtwoorden veiliger zijn. De populairste wachtwoordenmanagers voor windows zijn Bitwarden, Dashlane, Sticky Password, RoboForm, Keeper, Proton Pass, LastPass, NordPass en 1Password. Onderling kunnen ze verschillen in gebruik van open-source, sterke beveiliging, gebruiksvriendelijkheid, automatische wachtwoordinvulling, ingebouwde wachtwoordgenerator, een versleutelde kluis, ondersteuning van vingerafdruk- en gezichtsherkenning, Werkt ook offline, controleert de sterkte van je wachtwoorden en/of een premium wachtwoordmanager met uitgebreide functies. Voor de meeste programma's is naast een betaalde ook een gratis versie beschikbaar.
2. Controleer ook met enige regelmaat je email-adres en wachtwoorden op bekende datalekken. Dit kan onder meer via haveibeenpwned.com en scatteredsecrets.com. HaveIBeenPwned controleert of je e-mailadres is blootgesteld in een datalek. Je kunt je e-mailadres invoeren en zien of het voorkomt in bekende datalekken. Scattered Secrets gaat een stap verder en controleert niet alleen e-mailadressen, maar ook gehackte wachtwoorden. Dit helpt je te achterhalen of je wachtwoorden zijn gelekt en mogelijk misbruikt kunnen worden.
3. Schakel Multi-Factor Authenticatie (MFA) in: Dit is een beveiligingsmethode die vereist dat gebruikers meerdere vormen van verificatie doorlopen voordat ze toegang krijgen tot een systeem, account of applicatie. Veel bedrijven en online diensten, zoals banken, e-mailproviders en cloudplatforms, maken er al gebruik van. In plaats van alleen een wachtwoord te gebruiken, combineert MFA verschillende identificatiemethoden om de kans op ongeautoriseerde toegang te verkleinen. Het combineren van een wachtwoord of een pincode met een of meerdere mails, code naar een sms-bericht van een mobiele telefoon, beveiligingstoken of smartcard, biometrische gegevens zoals een vingerafdruk of gezichtsherkenning. Iets wat je weet, hebt en/of bent. Zelfs als phishers uw wachtwoord bemachtigen, moeten ze extra verificatiestappen omzeilen om toegang te krijgen tot uw account. Je kan ook Multi-Factor Authenticatie (MFA) zelf instellen door het Download van een authenticator-app zoals Microsoft Authenticator of Google Authenticator op je telefoon. Ga naar de beveiligingsinstellingen van het platform waarvoor je MFA wilt inschakelen (bijvoorbeeld Microsoft 365, Google, of je bank). Selecteer MFA of tweestapsverificatie en kies een verificatiemethode (zoals een app, sms-code of hardware-token). Scan de QR-code die wordt gegenereerd door het platform met

je authenticator-app. Bevestig de verificatie door de gegenereerde code in te voeren. Test de MFA-instelling door uit te loggen en opnieuw in te loggen met de extra verificatiestap. Wanneer je gebruik kunt maken van multifactor authenticatie, doe dit dan! Zeker ook bij de beveiliging van jouw wachtwoordmanager. *Meer informatie over tweestaps authenticatie kun je lezen in* dit artikel *van de* Consumentenbond*. En als je een ANWB Inboedelverzekering met cyberdekking hebt, helpt de* Cyberhelpdesk *jou gratis met het instellen ervan.*

4. Houd software up-to-date – Installeer altijd de nieuwste updates voor je besturingssysteem en apps om beveiligingslekken te dichten. Zorg dat je smartphone en laptop altijd de meest recente versie van het besturingssysteem hebben. Het besturingssysteem is het hoofdprogramma dat geïnstalleerd staat op je computer of smartphone. Bekende besturingssystemen voor de smartphone zijn Android of iOS en voor de laptop en computer zijn Microsoft Windows, Linux, macOS van Apple en Chrome OS van Google de meest bekende. Updates worden doorgevoerd om zwakke plekken in de beveiliging op te lossen en met een oudere versie ben je kwetsbaar. Wacht dus niet vooral niet onnodig lang met updaten.
5. Wees voorzichtig met openbare wifi – Vermijd het gebruik van onbeveiligde netwerken of gebruik een VPN om je verbinding te versleutelen. Je bent aan het werk in een koffietentje of hebt ingecheckt in je hotel en ziet daar een bordje met netwerknaam en wachtwoord staan voor het wifi netwerk. Mooi! Dat bespaart weer mobiele data. Maar wees je bewust van de gevaren, want is zo'n openbaar wifi-netwerk wel veilig? Het antwoord op deze vraag is meestal 'nee'. Zodra je inlogt op een openbaar wifi-netwerk is je laptop of smartphone mogelijk toegankelijk voor Cybersecuritylen. Zij kunnen daardoor toegang krijgen tot je persoonlijke gegevens. Dit kan mogelijke identiteitsfraude als gevolg hebben. Betekent dit dat je er nooit gebruik van kan maken? Nee, dat kan wel, maar doe dat altijd via een VPN verbinding (een virtueel privénetwerk).
6. Een VPN (Virtueel Privénetwerk) creëert een versleutelde tunnel tussen jouw apparaat en een externe server, waardoor je internetverkeer wordt beschermd tegen nieuwsgierige ogen. Het werk als volg. Een VPN versleutelt je internetverkeer, zodat hackers, internetproviders en overheden niet kunnen zien wat je doet. Je echte IP-adres wordt vervangen door dat van de VPN-server, waardoor je online anoniemer bent. Je kunt doen alsof je in een ander land bent, waardoor je toegang krijgt tot content die normaal gesproken geblokkeerd is. Een VPN beschermt je gegevens wanneer je verbinding maakt met onbeveiligde netwerken, zoals in bibliotheek, café, hotel of luchthaven. De populairste VPN's voor windows zijn NordVPN, Surfshark, ExpressVPN, CyberGhost en Proton VPN. Onderling kunnen ze verschillen in het meest gebruikt, sterke beveiliging, snelle verbindingen, Budgetvriendelijk, onbeperkte apparaten per account, Zeer gebruiksvriendelijk, ideaal voor beginners, goede gebruikerservaring, privacybescherming, Open-source en/of sterke focus op privacy. De gratis versies van PrivadoVPN, Proton VPN, Hide.me, TunnelBear, Windscribe en ZoogVPN kunnen een lagere snelheden of beperkte data limiet hebben.
7. Gebruik betrouwbare antivirussoftware. Zorg ervoor dat je apparaten beschermd zijn tegen malware en andere bedreigingen. In windows zit standaard de antivirusprogramma Defender en hij scoort best hoog als virusscanner. Het mist sommige geavanceerde functies zoals een VPN, uitgebreide phishingbescherming of privacytools die je bij betaalde antiviruspakketten vindt. Bij Apple is geen virusscanner aanwezig. Door zijn gesloten structuur, strenge app store controle is een virusscanner niet echt nodig. Een virusscanner zal ook maar beperkt werken door het gesloten structuur van Apple. Toch zal men ook bij Apple alert moeten zijn voor Phising en wachtwoorden fraude. Ook bij Linux is standard geen virusscanner aanwezig. Door zijn gebruikersrechtenstructuur, pakkettenbeheer en open-source transparantie ook niet echt nodig. Bij uitwisselen met oa Windows-bestanden, e-mails en/of gevoelige data is een virusscanner voor Linux wel aan te raden. Ook bij Android is standard geen virusscanner aanwezig. Er zijn voldoende virusscanner voor Android beschikbaar. Een betrouwbare antivirus/anti-malware oplossingen zoals Malwarebytes Premium voor windows kan je digitale veiligheid verbeteren. Zorg dat op je laptop, computer én smartphone een antivirusprogramma staat. Een antivirusprogramma spoort schadelijke bestanden op je computer op en verwijdert deze. De populairste antivirusprogramma's voor windows zijn Bitdefender, Antivirus Plus, Total

Security, MalwareBytes Premium, Sophos Home Premium, Avira Internet Security, Avast Free Antivirus, McAfee Internet Security en Norton 360 Deluxe. Ze bieden allen een uitstekende bescherming tegen malware en andere online bedreigingen. Onderling kunnen ze verschillen in sterke malwaredetectie, uitgebreide beveiligingsfuncties, breed scala aan beveiligingsopties, ouderlijk toezicht, bescherming tegen identiteitsdiefstal, voor meerdere apparaten, biedt een solide firewall en/of zowel een gratis als betaalde versie beschikbaar. Ook bieden veel internetaanbieders (zoals KPN) een virusscanner aan. Soms is deze inbegrepen in het maandbedrag, soms moet je er apart voor betalen. Maak ook af en toe een totale scan van al jou partities op jou computer door de virusscanner. Wil je weten welke virusscanner voor jou geschikt is? Bij de Consumentenbond vind je hier meer informatie over.

8. Gebruik naast een virusscanner op je laptop of PC ook een firewall. Bij Android is geen firewall beschikbaar. Het in en uitgaande verkeer wordt bij Android geregeld bij het instaleren van de verschillende appjes. Windows, Linux en iOS bevatten wel een ingebouwde firewall. Bij IOS en Linux moet je hem na het installeren van het besturingssysteem nog wel aanzetten en instellen. Bij Windows staat de firewall van Defender na het instaleren van Windows al aan. Indien nodig kan je de instellingen wijzigen, aanpassen of voor een andere firewall vervangen. Deze standaard firewalls volstaat voor de gemiddelde gebruiker van Windows, Linux en IOS. Een firewall is een beveiligingssysteem dat netwerkverkeer filtert en controleert op basis van vooraf ingestelde regels. Het fungeert als een digitale barrière tussen jouw apparaat en het internet, waardoor ongewenste toegang en schadelijke activiteiten worden geblokkeerd. Een firewall analyseert inkomend en uitgaand verkeer en bepaalt welke gegevens worden doorgelaten en welke worden geblokkeerd. Dit gebeurt op basis van verschillende criteria oa Verkeer van verdachte of onbekende bronnen kan worden geweigerd, Specifieke poorten kunnen worden gesloten om bepaalde soorten verkeer te blokkeren, of Alleen veilige protocollen worden toegestaan. Er zijn verschillende soorten firewalls zoals de Packet-filtering firewall (deze controleert individuele datapakketten en blokkeert ongewenst verkeer.), Stateful firewall (deze houdt de status van actieve verbindingen bij en maakt beslissingen op basis van eerdere communicatie.) en de application-level firewall (deze werkt op applicatieniveau en kan specifieke programma's of protocollen blokkeren.). De populairste firewalls voor Windows zijn Norton 360, Bitdefender, McAfee, Palo Alto Networks VM-Series & Sophos Firewall en VMWare vDefend Distributed Firewall. Onderling kunnen ze in detail van elkaar verschillen. De gratis firewalls voor Windows zijn Comodo Free Firewall, ZoneAlarm Free Firewall, GlassWire, TinyWall Free Firewall, Sophos XG Firewall Home Edition, Evorim Free Firewall, Lulu en Windows Firewall Control. Als je een firewall gebruikt update deze programma’s ook regelmatig. Daarnaast zijn Next-Generation Firewalls (NGFW's) steeds populairder, omdat ze gebruik maken van AI en machine learning om zero-day bedreigingen te detecteren en blokkeren.
9. Let op phishing. Klik niet zomaar op links in e-mails of berichten van onbekende afzenders. Controleer altijd de afzender en de URL.
10. Bij het downloaden van bestanden en apps kunnen deze bestanden en apps ook virussen en malware bevatten. Gebruik daarom bij downloaden zoveel mogelijk of alleen officiële bronnen zoals officiële website van het programma of via vertrouwde platforms zoals Microsoft Store, Apple App Store of Google Play Store. Let op neplinks en URL’s die misleidend of net echt lijken. Lees reviews: Als een app veel negatieve recensies krijgt of amper gedownload is, wees voorzichtig. Laat je antivirus de nieuwe bestanden automatisch scannen alvorens te installatie. Als je twijfelt, kun je de programma’s eerst in een virtuele omgeving testen voordat je ze op je hoofdapparaat installeert.
11. Bij twijfel neem zelf contact met de bewuste instantie (bank of belastingdienst) of personen om te verifiëren dat de informatie wel klopt.
12. Maak regelmatig back-ups – Bewaar belangrijke bestanden op een externe harde schijf of in de cloud, zodat je ze niet verliest bij een aanval.
13. Wees waakzaam voor QR codes. Het gevaar bij QR-codes is dat ze vaak officieel en vertrouwd lijken, maar net als bij phishing kan het linkje in een QR-code ook nep zijn. Gebruik hier je gezonde verstand. Krijg je een menukaart van een restaurant met een QR code, dan is deze waarschijnlijk wel veilig. Maar scan niet zo maar in het wilde weg alle QR-codes die je tegenkomt. Het is niet altijd duidelijk of de qr code die je scant officieel is. De FBI waarschuwt bijvoorbeeld

voor criminelen die qr codes op parkeerautomaten vervalsen en zo jouw betaling innen. Gebruik dus altijd je gezonde verstand. Enkele tips om QR-code-fraude te voorkomen: Als het om een app gaat download deze dan via de app/play store. Controleer altijd het webadres net als bij (phishing)berichtjes met linkjes. Check het webadres het liefst bij het scannen, voordat je doorklikt. Laat je niet misleiden door officieel uitziende documenten. Bijvoorbeeld een brief van je bank, met daarin een QR-code. Een verkorte link (zoals bit.ly) in een QR-code is extra verdacht. Er is immers ruimte genoeg voor een volledig webadres.

14. Openbare opladers? Liever niet Lege telefoon op het vliegveld of in de bus? Pas op met het gebruiken van openbare usb-poorten en oplaadkluisjes. Deze kunnen gebruikt worden om jouw gegevens uit te lezen en malware te installeren. In het Engels heet het 'juice jacking'. En ook al is het (nog) geen grootschalig probleem, het is zeker mogelijk. Gebruik dus liever een stopcontact of zet je telefoon uit tijdens het laden.
15. Gebruik verschillende mailadressen. Phishing is het stelen van je gegevens via nepberichten. Via linkjes in e-mail, sms of social media kom je terecht op nagemaakte websites van banken, overheid of bedrijven. Herken phishing door verschillende mailadressen voor verschillende activiteiten te gebruiken. Door bijvoorbeeld een ander emailadres te gebruiken voor online aankopen & nieuwsbrieven dan voor je bank of de overheid kun je spam of nepmails makkelijker (onder)scheiden van je belangrijke mail.
16. Voorzichtigheid en een gezond verstand spelen vaak nog een belangrijkere rol. Laat nooit je telefoon toestel onbeheerd achter en wees voorzichtig met het afgeven van je paspoort.
17. De ANWB Cyberhulp kan je helpen online veiliger te maken. Hulp bij het instellen van FMA op je apparaten, hulp bij (mogelijke) incidenten en een verzekering voor als er toch iets gebeurt.
18. Beheer je instellingen voor social media. Zorg dat je persoonlijke en privégegevens achter slot en grendel zitten. Cybercriminelen die social engineering gebruiken, kunnen je persoonlijke informatie vaak aan de hand van een paar gegevens achterhalen. Hoe minder je dus openbaar deelt, hoe beter. Als je bijvoorbeeld de naam van je huisdier of de meisjesnaam van je moeder noemt, kun je de antwoorden op twee algemene beveiligingsvragen onthullen.
19. Maak je thuisnetwerk sterker. Het is een goed idee om te beginnen met een sterk versleutelingswachtwoord en een virtueel privénetwerk. Een VPN versleutelt al het verkeer dat je apparaten verlaat totdat het op de bestemming aankomt. Als cybercriminelen erin slagen je communicatielijn te hacken, onderscheppen ze alleen maar versleutelde gegevens. Het is verstandig om een VPN te gebruiken wanneer je met een openbaar wifinetwerk verbinding maakt, of het nu in een bibliotheek, café, hotel of luchthaven is.
20. Als extra kan je ook bestanden met gevoelige informatie in Word, Excel, pdf, rar en zip voorzien van een wachtwoord alvorens je ze kan openen.
21. Praat met je kinderen over internet. Je kunt je kinderen leren over aanvaardbaar internetgebruik en daarbij alle communicatiekanalen openlaten. Zorg dat ze weten dat ze altijd naar je toe kunnen komen als ze online worden lastiggevallen, gestalkt of gepest. Ook als oppas opa en oma is het niet verkeerd om er met de klein kinderen er over te praten en bij ongeregeldheden jou kinderen hierover te informeren.
22. Neem maatregelen om jezelf tegen identiteitsdiefstal te beschermen. Identiteitsdiefstal vindt plaats wanneer iemand je persoonlijke gegevens via fraude of misleiding verkrijgt, meestal voor economisch gewin. Hoe doen ze dit? Je kunt worden misleid en je persoonlijke gegevens via internet onthullen, of een dief kan je e-mail stelen om toegang te krijgen tot accountinformatie. Daarom is het belangrijk om je persoonlijke gegevens te bewaken. Een VPN (kort voor virtueel privénetwerk) kan je ook helpen de gegevens die je online verzendt en ontvangt te beschermen, vooral wanneer je via openbare wifi op internet gaat.
23. Wees je ervan bewust dat identiteitsdiefstal overal kan gebeuren. Het is verstandig te weten hoe je je identiteit kunt beschermen, zelfs wanneer je op reis bent. Je kunt een heleboel dingen doen om te voorkomen dat criminelen je privégegevens in handen krijgen wanneer je onderweg bent. Zet je reisplannen bijvoorbeeld niet op social media en gebruik een VPN wanneer je in je hotel via het wifinetwerk op internet gaat.
24. Houd een oogje op de kinderen. Net zoals je met je kinderen over internet wilt praten, wil je ze ook beschermen tegen identiteitsdiefstal. Identiteitsdieven richten zich vaak op kinderen omdat hun Burgerservicenummer en kredietgeschiedenis een schone lei betekenen. Je kunt hen beschermen tegen identiteitsdiefstal door voorzichtig te zijn in

het delen van de persoonlijke gegevens van je kind. Het is ook slim om te weten waar je op moet letten om te zien of de identiteit van je kind is misbruikt.

25. Door te begrijpen en identificeren van de verschillende vormen van phishing aanvallen kan je passende maatregelen nemen om jou identiteit gegevens en bank gegeven te beveiligen.

Waar kan je Cybersecurity melden.

Weet wat je moet doen als je slachtoffer wordt. Als je denkt dat je het slachtoffer bent geworden van een cybermisdaad, moet je dit melden bij de lokale politie 0900-8844 en in sommige gevallen de FBI en de Federal Trade Commission. Dit is belangrijk, zelfs als de overtreding niet zo ernstig lijkt. Jouw melding kan de autoriteiten helpen bij hun onderzoek of voorkomen dat criminelen in de toekomst misbruik maken van anderen.
Als je denkt dat cybercriminelen je identiteit hebben gestolen. Dit zijn enkele stappen die je moet nemen. Neem contact op met de bedrijven en banken waarvan je weet dat daar fraude heeft plaatsgevonden.

Plaats fraudewaarschuwingen en haal je kredietverslagen op.
Een fraudewaarschuwing is een gratis melding die u aan uw kredietrapport kunt toevoegen en waarbij u uw identiteit moet verifiëren voordat u een lening onder uw naam kunt afsluiten. Fraudewaarschuwingen fungeren als een tweede vorm van authenticatie om ervoor te zorgen dat u de enige bent die leningen kan afsluiten of kredietaccounts onder uw naam kunt openen.
De fraudewaarschuwing is voor maximaal één jaar geldig. Uitgebreide fraudewaarschuwing is zeven jaar geldig en is bedoeld voor slachtoffers van fraude.
Er zijn drie belangrijke situaties waarin je een fraudewaarschuwing moet plaatsen: als je denkt dat je het slachtoffer bent geworden van fraude, als je het slachtoffer bent geworden van identiteitsdiefstal of als je jou identiteit wilt beschermen tegen diefstal.
Je kredietverslag is een overzicht van je financiële geschiedenis, inclusief leningen, kredietkaarten en betalingsgedrag. In Nederland kun je dit opvragen via Stichting BKR. Dit is gratis, maar een gewaarmerkt overzicht kost €16,45.

Meld de identiteitsdiefstal.

Slachtofferhulp Nederland (0900-0101) biedt ondersteuning aan slachtoffers van Cybersecurity, zoals online fraude, identiteitsdiefstal en hacking.
Via hun website kan je gratis advies en tips krijgen.
Ze helpen je met emotionele steun, juridisch advies en/of praktische hulp.
Ze biedt gesprekken en begeleiding om je te helpen omgaan met de gevolgen.
Ze geven informatie over je rechten en helpen bij het doen van aangifte.
Ze geven advies over hoe je verdere schade kunt voorkomen en je digitale veiligheid kunt verbeteren.

Fraudehelpdesk (088-786 7372) helpt slachtoffers van Cybersecurity door waarschuwingen, advies en Meldpunt.
Ze informeren over actuele fraudepraktijken, zoals phishing, identiteitsdiefstal en online oplichting.
Ze geven tips over hoe je fraude kunt herkennen en voorkomen.
Je kunt verdachte situaties melden, zodat ze anderen kunnen waarschuwen en eventueel doorverwijzen naar de juiste instanties.

Centraal Meldpunt Identiteitsfraude (CMI) (088-900 1000) helpt slachtoffers van identiteitsfraude en biedt ondersteuning bij Cybersecurity-gerelateerde identiteitsdiefstal.
Ze kunnen je helpen bij het meldingen van identiteitsfraude bij andere instanties zoals de Belastingdienst en/of politie.
Ze geven advies, ondersteuning en tips om identiteitsfraude te voorkomen en helpen slachtoffers bij het herstellen van de gevolgen. Zij raden bijvoorbeeld het gebruik van de KopieID-app aan.
Voor bewustwording en preventie organiseren zij presentaties en workshops

Autoriteit Financiële Markten (AFM) (0800-540 0540) speelt een belangrijke rol in het bestrijden van financiële cybercriminaliteit. Ze richten zich vooral op toezicht op financiële instellingen, waarschuwingen, regelgeving, Onderzoek en handhaving.
Zij controleert of banken, beleggingsinstellingen en andere financiële partijen zich houden aan wetgeving tegen witwassen en fraude.
Ze waarschuwen consumenten en bedrijven voor risico’s zoals marktmanipulatie in de cryptosector, zoals ‘pump and dump’-praktijken, die vanaf eind 2024 verboden worden.

Ze legt boetes op aan bedrijven die zich niet aan de regels houden, zoals bij overtredingen van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft).

Autoriteit Consument en Markt (ACM) (088-070 7070) speelt een rol in het bestrijden van digitale fraude en Cybersecurity, vooral binnen de digitale economie en online consumentenbescherming.
Ze richten zich op toezicht op online platforms, bescherming tegen misleidende praktijken en concurrentie en marktwerking.
Zij controleert of digitale diensten voldoen aan de regels van de Digital Services Act (DSA), die sinds 2024 in werking is getreden.
Ze treden op tegen bedrijven die consumenten misleiden met valse aanbiedingen, verborgen kosten of oneerlijke handelspraktijken.
Ze voorkomt dat bedrijven de markt manipuleren, bijvoorbeeld door kartelvorming of misbruik van een economische machtspositie.

Daarnaast kan men gebruik maken van de ANWB Cyberhulp, consumentenbond en HCC.

Slot
Criminelen zullen steeds weer wat nieuws verzinnen om jou te proberen op te lichten.
Om je computer dicht te spijkeren tot een vesting zal ook niet echt nodig zijn.
Door alle beveiliging-software zou hij bijna niet meer vooruit te branden zijn.
Met je gezond verstand en een gezonde argwaan zal je al veel leed worden bespaard.
Mocht je toch slachtoffer van Cybersecurity worden weet dan wat je kan doen.