INTERNETVEILIGHEID BEGINT BIJ UZELF

Hoe beschermt u uzelf tegen cybercriminaliteit?

U heeft het ongetwijfeld in uw omgeving al meegemaakt, dat iemand is opgelicht via de telefoon of de computer. En dat is niet omdat die mensen dom zijn. Want criminelen worden steeds slimmer en daardoor kan cybercriminaliteit ons allemaal overkomen. Senioren blijken extra kwetsbaar te zijn voor digitale oplichting. U dus ook! Hoog tijd om er zoveel mogelijk over te weten te komen en maatregelen te nemen om deze ellende te voorkomen.

In deze folder staan belangrijke tips om uzelf te beschermen tegen cybercriminaliteit.

Wat is cybercriminaliteit?

Cybercriminaliteit is een veelkoppig monster. Sommige misdrijven zijn vooral een bedreiging voor bedrijven. U kunt bijvoorbeeld denken aan een website die onbereikbaar wordt of allerlei vormen van kwaadaardige software zoals virussen en gijzelsoftware.
Andere misdrijven treffen u persoonlijk. Zo vindt 'ouderwetse oplichting' steeds meer digitaal plaats zoals aankoopfraude. Dit is een vorm van fraude waarbij u online een aankoop doet en betaalt, maar het product nooit ontvangt.

Ook whatsappfraude komt nog steeds voor. Criminelen doen zich voor als een familielid of andere bekende en benaderen u met een probleem waarvoor zij hulp nodig hebben. Het woordgebruik van de crimineel is vaak lastig van echt te onderscheiden. Het is dan ook niet gek als u per ongeluk geld overmaakt naar aanleiding van zo'n bericht.
Ook geven criminelen zich uit als medewerkers van bijvoorbeeld een bank en vertellen hun slachtoffers dat ze snel in actie moeten komen om geen geld kwijt te raken en te doen wat ze zeggen.

Dit overkomt mij niet!

Veel mensen denken "Cybercriminaliteit overkomt mij niet!" Maar niets is minder waar. Iedereen kan slachtoffer worden van de trucs die cybercriminelen gebruiken. Bent u nog niet overtuigd? Kijk dan eens goed naar de volgende cijfers:

• 12% van alle senioren wordt elk jaar slachtoffer van cybercriminaliteit. Dit zijn er ruim 400.000 per jaar.
• Per jaar worden ruim 26.500 van de 65 senioren wordt financieel getroffen door cybercriminaliteit.

• Als senioren het slachtoffer worden, leidt dit vaak tot ernstigere psychologische en sociale gevolgen dan bij jonge mensen.
Als u het idee hebt dat u geen interessant doelwit bent voor cybercriminelen, dan zit u ernaast. Iedereen die online is, is een interessant en potentieel slachtoffer voor criminelen. Dit is dus bijna iedereen, want we kopen allemaal weleens iets online of we plaatsen wat informatie over onszelf op social media of we regelen onze bankzaken online. Sommige criminelen zijn uit op uw geld, maar soms azen ze ook op uw persoonsgegevens waarmee ze bijvoorbeeld identiteitsfraude kunnen plegen of informatie over u en uw familie of interesses om u erin te kunnen luizen.

Hoe bescherm ik mijzelf?

Cybercriminaliteit is een paraplu waaronder heel veel verschillende digitale delicten vallen. Er is dus ook niet één manier om uzelf te beschermen tegen al deze delicten. Voor sommige delicten is het bijvoorbeeld belangrijk om technische beveiliging te gebruiken, terwijl bij andere delicten het heel erg belangrijk is om zelf heel kritisch en alert te zijn. Eerst vijf tips over uw eigen gedrag.

1. Wees gezond wantrouwend
Lees berichten kritisch voordat u overgaat tot actie: gebruikt de verzender ineens andere woorden dan u gewend bent of is iets te mooi om waar te zijn? Dan is het vaak foute boel. Ga hier dus niet op in. Voordat u een online aankoop doet kan u ervaringen van anderen opzoeken. Zo komt u er gauw genoeg achter of u te maken heeft met een betrouwbare partij.

2. Reageer nooit onder tijdsdruk
Een bekende en helaas goed werkende methode van criminelen is om u onder druk te zetten. In de haast of stress die u dan voelt, denkt

u niet helder meer na. Dat is precies hun bedoeling! Trap er niet in. Als u dus wordt benaderd door iemand (of misschien wel een voor u bekende organisatie) die aangeeft dat er iets mis is of dat ze iets van u nodig hebben en dat er haast bij is, haal dan uw gezonde wantrouwen uit de kast. En ga door naar tip 3 hieronder.

3. Vraag hulp en praat erover
Vraag mensen in uw omgeving of ze even meekijken wanneer u een bericht ontvangt waarbij u twijfelt over de echtheid. Ziet u een koopje op marktplaats? Of twijfelt over een bericht van bijvoorbeeld de Belastingdienst. Is die wel echt? Wacht dan eerst op andermans oordeel, voordat u verdere stappen zet. Juist als u snel wil handelen is vertragen verstandig!

Maar ook als er nog geen directe aanleiding is, kan het geen kwaad om met vrienden en bekenden zo nu en dan over cybercriminaliteit te praten. U kunt elkaar tips geven en alert houden om niet in de digitale valstrikken van criminelen te trappen.

4. Deel niet zomaar persoonlijke informatie
Met persoonsinformatie kan iemand identiteitsfraude plegen. Geef daarom nooit zomaar belangrijke informatie zoals BSN-nummer of foto's van belangrijke documenten (diploma, ID-kaart of paspoort). Met deze informatie kan een crimineel in uw naam een lening aanvragen of zich voordoen als u om vrienden en familie te misleiden.

5. Social media accounts op privé
Zet al uw social media accounts standaard op 'privé' zodat alleen uw eigen contacten uw berichten kunnen zien. Neemt u alle uitnodigingen voor contacten op social media aan? Niet doen! Verbind alleen via sociale media met mensen die u persoonlijk kent of op een andere manier vertrouwt. Want hoe meer u prijsgeeft online, hoe makkelijker u slachtoffer wordt van cybercriminaliteit. Hoe meer ze over u weten, hoe beter criminelen u kunnen bespelen. Naast deze tips over uw eigen gedrag, is het ook belangrijk een paar technische zaken op orde te hebben. Misschien is het niet uw hobby om daarmee bezig te zijn, maar het is wel nodig om op die manier de toegang tot uw persoonlijke gegevens te beschermen. U zet uw fiets ten slotte ook op slot. Vraag gerust iemand uit uw omgeving om u hierbij te helpen!

1. Gebruik unieke en sterke wachtwoorden!
Toegegeven: het is best lastig om ingewikkelde en unieke wachtwoorden te gebruiken. We weten allemaal dat het belangrijk is, maar we doen het toch niet. Daar maken criminelen gebruik van om digitaal bij u in te breken. Veel mensen hebben namelijk hetzelfde wachtwoord voor verschillende websites en platformen. Vaak zijn deze wachtwoorden ook nog makkelijk te raden, omdat het wachtwoord bijvoorbeeld de naam van uw favoriete voetbalclub of uw kind bevat of uw geboortedatum. Gebruik dus wachtwoorden van minimaal 14 tekens en gebruik voor ieder account een ander wachtwoord. Overweeg hierbij de hulp van een digitale wachtwoord-kluis. Dat is een programma waar je tegen betaling al je sterke en unieke wachtwoorden in kan maken en opslaan.

2. Gebruik tweestapsverificatie
Bij veel applicaties heeft u de optie om tweestapsverificatie te gebruiken. Vaak wordt dit als omslachtig ervaren, omdat u een extra stap moet zetten voordat u kan inloggen. Het kost misschie
n wat extra moeite, maar deze extra verificatie zorgt ervoor dat bij het inloggen een wachtwoord alleen niet genoeg is. Naast het wachtwoord zal er via een extra stap een vingerafdruk of code worden

gevraagd als bevestiging. Mocht u niet precies weten hoe u tweestapsverificatie kunt instellen, is het niet gek om iemand te vragen met u mee te kijken!

3. Voer updates uit!
Een andere manier om uzelf te beschermen tegen cyberrisico's is het uitvoeren van updates. Door het installeren van updates op uw telefoon, computer en tablet worden zwakke plekken in apparaten en software hersteld. Zorg er dus voor dat updates automatisch worden geïnstalleerd. Zo kost het u geen tijd en draaien uw (beveiligings)software en apparaten voortaan altijd op de krachtigste versie.

Wat moet ik doen als ik toch slachtoffer word?

Mocht u toch slachtoffer worden van cybercriminaliteit, schaam u dan niet! Het kan namelijk iedereen overkomen.

1. Praat erover
Laat vooral aan anderen weten dat u slachtoffer bent geworden. Informeer bijvoorbeeld uw familie of vrienden zodat jullie samen kunnen kijken welke stappen er gezet moeten worden. Door met elkaar te praten over slachtofferschap van cybercriminaliteit worden we ons steeds bewuster van de methoden. Zo steken we een stok in de wielen van de cybercriminelen.

2. Meld het misdrijf
Afhankelijk van het misdrijf waarvan u slachtoffer bent geworden is het belangrijk om dit te melden bij de betrokken organisaties. Mochten cybercriminelen belangrijke bankgegevens hebben gestolen of bent uw grote geldbedragen kwijtgeraakt? Bel dan onmiddellijk de bank! Laat ze weten wat er gebeurd is. Zij hebben specialisten die u kunnen helpen om de juiste acties te ondernemen en de schade te beperken.

3. Doe aangifte bij de politie
Doe ook altijd aangifte bij de politie. Maak hiervoor een afspraak via 0900-8844. Nu denkt u misschien dat dit toch geen nut heeft, maar dat is wel het geval. De kans is misschien klein dat uw zaak meteen wordt opgelost, maar door zaken te bundelen wordt de kans groter dat criminelen worden gepakt. Ook helpt het de politie om inzicht te houden wat er precies speelt en op deze manier kunnen anderen gewaarschuwd worden.

4. Verander uw wachtwoorden
Als een account is gehackt of uw persoonlijke gegevens zijn gestolen, dan is het verstandig om uw wachtwoorden te veranderen. Zo voorkomt u dat criminelen bij andere accounts kunnen en beschermt u andere gegevens. Als u het lastig vindt om zoveel verschillende wachtwoorden te onthouden kunt u een wachtwoordkluis gebruiken. (zie ook de technische tip 1 hiervoor bij 'Hoe bescherm ik mijzelf?'

5. Check het lek
Als u denkt dat criminelen gegevens van u hebben buit gemaakt, kijk dan op www.haveibeenpwned.com. Hier kunt u heel gemakkelijk controleren of uw mailadres of telefoonnummer illegaal rondzwerft op het internet.

Meer info bij
- Fraudehelpdesk.nl
- Cybercrimeinfo.nl
- checkjelinkje.nl/appjelinkje
- www.seniorweb.nl

Deze flyer is ontwikkeld in eem samenwerking tussen het Veiligheidsnetwerk Oost-Nederland en het lectoraat Maatschappelijke Veiligheid van de Hogeschool Saxion, onder financiering van de Citydeal Lokale Weerbaarheid Cybercrime in samenwerking met het Centrum voor Criminaliteitspreventie en Veiligheid.