



Digitale weerbaarheid:

Neem de regie over je online veiligheid

Fijn dat je hebt deelgenomen aan de voordracht CyberAttack! Onze digitale wereld biedt ontzettend veel kansen, gemak en mogelijkheden om in verbinding te blijven. Om hier optimaal van te genieten, is het belangrijk om te weten waar de valkuilen liggen en hoe je deze slim kunt ontwijken. Kennis en een goede voorbereiding zijn daarin je beste bescherming. Met de juiste maatregelen houd je online criminelen eenvoudig buiten de deur en blijf je met een gerust gevoel digitaal actief.

In deze brochure vind je de tips en de belangrijkste aandachtspunten uit de voorstelling. Ik behandel de belangrijkste preventieve stappen, de meest voorkomende digitale fenomenen en hoe je kordaat handelt als er toch iets fout dreigt te gaan.

Wil je na het lezen nog meer achtergrondinformatie, surf dan zeker naar www.cyberpreventie.be.



Het belang van kennis en voorzorgsmaatregelen



Cybercriminelen gebruiken geavanceerde technieken om persoonlijke gegevens te stelen, gericht op menselijk gedrag en vertrouwen in plaats van complexe systemen. Door bewustzijn en proactieve voorzorgsmaatregelen te nemen, kun je jezelf en je dierbaren beschermen.



Preventie begint bij alertheid en goede gewoontes. Wees altijd oplettend bij onverwachte berichten of e-mails en deel nooit zomaar persoonlijke of financiële informatie zonder dat je honderd procent zeker bent van de betrouwbaarheid van de bron.



Veelvoorkomende fenomenen

Phishing voorkomen en herkennen

Phishing is een van de meest verspreide vormen van digitale oplichting. Criminelen doen zich via e-mail, sms, WhatsApp of telefoon voor als een betrouwbare instantie – zoals je bank, de overheid of een koeriersdienst – met als doel je inloggegevens of bankcodes te ontfutselen.



Phishing voorkomen en herkennen



Controleer de afzender:

Wees voorzichtig met berichten van onbekende afzenders. Controleer het e-mailadres goed; het moet exact overeenkomen met de officiële domeinnaam van de organisatie, zoals @banknaam.be voor je bank.



Klik niet zomaar op verdachte links:

Phishingberichten bevatten vrijwel altijd een link die leidt naar een valse, nagemaakte website. Beweeg je computermuis over de link (of houd deze op je smartphone ingedrukt) om het werkelijke webadres te bekijken. Ziet het adres vreemd of afwijking uit? Klik dan niet.



Wees voorzichtig met bijlagen:

Open nooit zomaar bijlagen van afzenders die je niet verwacht/kent. Deze bestanden kunnen schadelijke software (malware) bevatten die je toestel kan infecteren en je gegevens kan stelen.



Hoe lees je een url:

Zoek de derde slash en lees de echte domeinnaam voor de extensie. Iedereen wil een eenvoudige domeinnaam die je goed kan onthouden.
`https://www.DOMEINNAAM.ext/pagina`

Phishing voorkomen en herkennen



Rapporteer verdachte berichten:

Ontvang je een verdacht bericht? Stuur het meteen door naar verdacht@safeonweb.be. Hiermee help je niet alleen jezelf, maar waarschijnlijk ook meteen anderen. Denk eraan, **is een bericht onverwacht, maakt het je boos of blij en moet je snel handelen,....** dan is het waarschijnlijk een phishingmail.



Geef N00T codes door:

Geef nooit je persoonlijke codes, pincodes of **responscodes** van je kaartlezer door. Echte banken, de politie of overheidsinstanties zullen nooit om deze informatie vragen via telefoon, e-mail of berichten.



Dubbelcheck bij twijfel:

Heb je een dringende hulpvraag ontvangen via WhatsApp van een bekende met een nieuw nummer? Neem altijd eerst contact op via het oude, vertrouwde telefoonnummer om de situatie te verifiëren.



Veilig online shoppen en (ver)koopsfraude

Online winkelen en het kopen of verkopen via tweedehandsplatforms is handig, maar vereist oplettendheid om fraude en valse webshops te voorkomen.



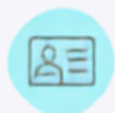
Controleer het webadres (URL):

Legitieme webwinkels hebben doorgaans een duidelijke domeinnaam en maken gebruik van een beveiligde verbinding, herkenbaar aan https://. Let op spelfouten, ongebruikelijke leestekens of afwijkende extensies in de domeinnaam.



Kijk kritisch naar de opbouw:

Oplichtingssites hebben vaak kenmerken zoals vreemde vertalingen, spelfouten en afbeeldingen van lage kwaliteit. Controleer de betrouwbaarheid van een website met hulpmiddelen zoals ScamAdviser.com.



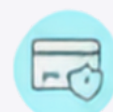
Zoek naar contactgegevens en voorwaarden:

Controleer of de webshop duidelijke contactinformatie heeft, zoals een fysiek adres, telefoonnummer en BTW-nummer. Bekijk ook het privacy- en retourbeleid. Zijn deze gegevens niet aanwezig? Google het adres dat op de site staat.



Raadpleeg beoordelingen van anderen:

Zoek online ervaringen en reviews. Veel klachten over niet-geleverde producten kunnen een waarschuwing zijn om voorzichtig te zijn.



Gebruik Veilige Betaalmethoden :

Het is aan te raden om veilige betaalmethoden te gebruiken, zoals creditcards of erkende betaaldiensten die aankoopbescherming bieden. Een nog betere optie is om te kiezen voor achteraf betalen. Laat je niet leiden naar een betaallink, maar betaal met je eigen bankapp.

Wees bovendien zeer voorzichtig met aanbiedingen die te mooi lijken om waar te zijn; extreem lage prijzen worden vaak als lokmiddel ingezet.

Vriendschapsfraude herkennen



Bij vriendschaps- of romancefraude bouwt een oplichter via sociale media of datingapps weken of maandenlang een hechte vertrouwensband op met het slachtoffer. Vaak zijn de slachtoffers op dat moment emotioneel zwak.

Zodra er een emotionele afhankelijkheid is ontstaan, begint de dader financiële hulp te vragen voor een 'onvoorzien noodgeval', een 'vliegticket' of een 'medische ingreep'.

Blijf altijd kritisch wanneer iemand die je nog nooit in het echt hebt ontmoet om geld vraagt.



Wat als een vriend het slachtoffer is?



Een nieuwe online vriend

Probeer je vriend te overtuigen om die nieuwe bekende te onderzoeken voordat hij betaalt. Zoek de persoon op via Google en maak gebruik van Google Lens.



Schakel professionele hulp in

Als jouw vriend sterk overtuigd is van de nieuwe vriendschap, informeer dan discreet de familie. Overweeg daarnaast om professionele hulp in te schakelen, zoals de huisarts.

Goede internet-hygiëne: je dagelijkse beveiliging

Een digitale beveiliging rust op een paar eenvoudige basishandelingen.

Door deze toe te papsen in je dagelijks leven verklein je de kans op digitale incidenten drastisch:



Gebruik TwEEfactorauthenticatie (2FA):

TwEEfactorauthenticatie voegt een cruciale extra beveiligingslaag toe. Zelfs als een crimineel je wachtwoord achterhaalt, heeft hij nog steeds de tweede stap nodig om in te loggen.

Download een authenticator-app op je smartphone (zoals Google Authenticator of Microsoft Authenticator) en koppel deze aan al je belangrijke accounts, zoals e-mail, sociale media en online bankieren.



Houd al je toestellen en software up-to-date:

Installeer updates voor je smartphone, computer en apps zodra deze beschikbaar zijn. Beveiligingsupdates dichten bekende lekken en kwetsbaarheden die anders door hackers uitgebuit kunnen worden.



Bescherm je privacy:

Wees terughoudend met het delen van persoonlijke gegevens op het internet en denk na voordat je gevoelige informatie deelt op openbare platforms.



Goede internet-hygiëne: je dagelijkse beveiliging



Gebruik een wachtwoordkluis:

Het hergebruiken van hetzelfde wachtwoord voor meerdere websites is een groot risico. Een wachtwoordkluis helpt je om voor elke dienst een uniek, ijzersterk wachtwoord te genereren en veilig te bewaren.



Check regelmatig op virusussen:

Gebruik betrouwbare beveiligingssoftware en controleer je apparaten regelmatig op schadelijke bestanden.



Noodnummers bij je contacten

Zorg ervoor dat je het telefoonnummer van je bank en cardstop toevoegt aan je contacten. Op deze manier hoef je deze in geval van nood niet te zoeken.



Goede internet-hygiëne: je dagelijkse beveiliging

Maak een shoppingadres:



Maak een shoppingadres aan, en hou een ander emailadres uitsluitend voor officiële instanties.

Laat niemand software op jouw toestel zetten



Laat niemand zonder jouw toestemming software op je apparaat installeren. Alleen als je zelf om de installatie vraagt, kan het gebeuren.

Lees belangrijke berichten op een groot scherm



Lees berichten waarin je geld ontvangt of moet betalen op een zo groot mogelijk scherm. Dit geeft je de kans om alles duidelijk en nauwkeurig te controleren.



Toch fout gelopen

Geen tijd te verliezen



Financiële schade of zijn je bankgegevens gedeeld? Neem dan onmiddellijk contact op met je bank of Card Stop om je rekeningen te laten bevriezen en je kaarten te blokkeren. Voor het blokkeren van bankkaarten kun je direct bellen naar Card Stop op 050 170 170.



Meld het incident zo snel mogelijk bij de lokale politie. Je aangifte is essentieel voor het onderzoek en helpt om fraudeurs tegen te houden.



Maak gebruik van gepersonaliseerde organisaties die ondersteuning en advies bieden, zoals Safeonweb of de Federale Ombudsdienst.



Pas onmiddellijk je wachtwoorden aan op een veilig apparaat en log je overal uit als je vermoedt dat een account is gehackt.