Online criminaliteit

Hoe te voorkomen?

Iedereen loopt risico slachtoffer te worden van online criminaliteit. Het is belangrijk om uw risico op slachtofferschap en de gevolgen daarvan klein te houden. In dit informatieblad leest u hoe u zich eenvoudig kunt beschermen.

Controleer de link voordat u klikt

Criminelen kunnen persoonlijke gegevens achterhalen, geld stelen, kwaadaardige software of virussen op apparaten plaatsen als u op een verkeerde link klikt.

- Een veilig webadres (URL) begint met https//: en heeft een hangslotje;
- Kijk goed naar de afzender, de aanhef, het taalgebruik en de vormgeving van het bericht;
- Blijf ook oplettend als u de persoon of organisatie kent. Soms ziet het er echt uit maar is het toch nep;
- Vertrouwt u het niet? Neem eerst telefonisch contact op met de persoon, het bedrijf of de organisatie.

Maak nooit zomaar geld over

Let op wanneer u ongevraagd helpdeskadvies krijgt of een bekende dringend financiële hulp nodig heeft. Met een onverwachtse en zeer dringende boodschap hopen criminelen u te overtuigen geld, vertrouwelijke gegevens of toegang tot apparaten te geven.

- Criminelen kunnen misbruik maken van een bekend telefoonnummer. Enkel het telefoonnummer controleren is daarom niet voldoende;
- Verbreek het contact en (video)bel ter controle het nummer van de persoon, het bedrijf of de organisatie die bij u bekend is;
- Maak geen geld over, deel geen persoonlijke gegevens en geef nooit iemand zomaar toegang tot uw apparaten;
- Houd uw pincodes en inlog- of beveiligingscodes altijd geheim en sta nooit uw bankpas, creditcard of inlogapparaatje af.

Bedenk goed wat u met wie deelt op het internet

Criminelen kunnen uw persoonlijke gegevens gebruiken om u of mensen uit uw omgeving op te lichten.

- Blijf bewust van wat u deelt. Zo makkelijk als het is om iets op internet te plaatsen, zo moeilijk is het om dit er weer af te krijgen;
- Laat u uw gegevens ergens achter, ga na wie toegang krijgt tot deze gegevens en hoe lang deze gegevens te zien zijn;
- Geef niet meer gegevens dan noodzakelijk.

Versie April 2023

Maak alleen verbinding met vertrouwde en beveiligde wifinetwerken

Wanneer u gebruik maakt van openbare of onbeveiligde wifinetwerken, kunnen anderen mogelijk zien wat u op het internet doet en welke gegevens u verstuurt.

- Verstuur geen gevoelige gegevens (e-mail, internetbankieren) over wifinetwerken die u niet kent of niet vertrouwt;
- Zorg dat de wifinetwerken die u (onder andere thuis) gebruikt beveiligd zijn met een gegevensversleuteling;
- Wilt u toch gebruik maken van openbare wifi-netwerken? Gebruik dan een versleutelde verbinding (VPN).

Installeer alleen apps via de officiële applicatiewinkel

Criminelen kunnen via apps kwaadaardige software of virussen op uw apparaten plaatsen. Zij kunnen dan meekijken op uw apparaat, bestanden beschadigen of verwijderen en (door middel van chantage) u geld afhandig maken.

- Installeer apps altijd alleen via de officiële applicatiewinkels, zoals de Windows store, de App store en Google Play;
- Controleer tot welke gegevens de app toegang krijgt;
- Bekijk de beoordelingen van medegebruikers om een beeld te vormen van de betrouwbaarheid van de app.

Zorg voor sterke en unieke wachtwoorden

Met zwakke wachtwoorden kan een crimineel aan uw persoonlijke gegevens komen, zoals uw bankgegevens.

- Kies geen veelgebruikte of voor de hand liggende wachtwoorden, zoals uw geboortedatum of telefoonnummer;
- Gebruik een wachtwoord(zin) van minimaal 12 tekens, waaronder speciale tekens als cijfers en leestekens;
- Controleer of uw wachtwoord(zin) sterk genoeg is met de wachtwoordkraaktest op veiliginternetten.nl;
- Het is belangrijk dat u verschillende wachtwoorden gebruikt voor uw apparaten en accounts. In een wachtwoordmanager kunt u de wachtwoorden opslaan;
- Maak gebruik van tweestapsinlog. Naast gebruikersnaam en wachtwoord, moet u dan ook uw identiteit bevestigen met een toegangscode of vingerafdruk.

Doe direct uw updates

Het is belangrijk dat u uw apparaten en apps beveiligd door regelmatig updates uit te voeren. Wanneer u dit niet tijdig doet kan gemakkelijk ingebroken worden op uw apparaten.

- Krijgt u een melding om een update te doen? Stel dit niet uit en doe dit direct;
- Breng in kaart welke apparaten u in huis heeft die verbonden zijn met internet. Ga naar de instellingen van uw apparaten en stel 'automatisch updaten' in;
- Mocht het niet mogelijk zijn om het apparaat automatisch te laten updaten, zet dan een herinnering in uw agenda om zelf de updates uit te voeren.

Gebruik een virusscanner

Een virusscanner kan u beschermen tegen veelvoorkomende kwaadaardige programma's.

- Welk antivirusprogramma het beste bij u past, is afhankelijk van uw computeractiviteiten en de manier waarop de virusscanner infecties opspoort en bestrijdt;
- Let op dat u geen 'nep-antivirus' download, waarmee u uw apparaat infecteert met een virus;
- Laat de antivirusscanner regelmatig uw apparaten scannen.

Maak regelmatig back-ups

Wanneer een crimineel uw apparaat toch heeft kunnen besmetten met een virus of andere kwaadaardige software, dan kunnen zij uw bestanden vergrendelen of beschadigen.

- Maak dagelijks een back-up van uw waardevolle bestanden;
- Zorg ervoor dat de back-up losgekoppeld is van uw apparaat.

Toch slachtoffer geworden? Wat nu?

- Melding of aangifte helpt bij het tegengaan van digitale criminaliteit, ook als u geen schade heeft. U kunt terecht bij Aangifte of melding doen | politie.nl (0900-8844), Home - Fraudehelpdesk (088-7867372) en/of Meld Misdaad Anoniem (0800-7000).
- Heeft u behoefte aan meer ondersteuning of advies, neem dan contact op met Slachtofferhulp Nederland (0900-0101).
- Is u geld afhandig gemaakt, heeft u het vermoeden dat iemand uw beveiligingscodes heeft of is uw bankpas kwijt, bel dan direct uw bank via het bij u bekende telefoonnummer.
- Wijzig direct uw gebruikersnamen en beveiligings- en inlogcodes. Doe dit vanaf een apparaat dat niet besmet is met schadelijke software.

Voor meer algemene informatie, ga naar www.rotterdam.nl/cyber of bel de gemeente Rotterdam via 14010 (kies voor optie 9, overige vragen).