Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Kennen ze jou ergens van?

Betalen met de mobiele telefoon. Virtueel door uw droomhuis wandelen. Eindelijk weer contact met een oude schoolvriend. Online solliciteren. De voorbeelden van het gemak van digitalisering zijn eindeloos. Maar met alle kansen, nemen ook de risico's toe. Phishing mails en aanvallen met ransomware door cybercriminelen zijn inmiddels bekende problemen. Ook landen zetten digitale middelen in voor eigen gewin: van het verspreiden van desinformatie tot aan spionage en sabotage. En die activiteiten treffen niet alleen bedrijven en overheidsorganisaties; er zijn ook zogenoemde statelijke actoren die op grote schaal persoonsgegevens verzamelen. Met deze infosheet informeren we u over deze werkwijze en wat u en uw naasten ertegen kunnen doen.

Weet wat er gebeurt

De afgelopen jaren hebben de Nederlandse inlichtingen- en veiligheidsdiensten meerdere keren gezien dat statelijke actoren gegevens verzamelen die andere personen, organisaties of landen kunnen schaden. Persoonsgegevens die vervolgens kúnnen worden gebruikt voor digitale aanvallen of spionageactiviteiten richting personen die om politieke of economische redenen relevant zijn. Politici bijvoorbeeld, maar ook ambtenaren, wetenschappers, topfunctionarissen, journalisten of de instanties waarvoor zij werkzaam zijn. Ook familieleden en vrienden rondom deze personen kunnen interessant zijn, als een soort 'opstap' naar de persoon om wie het echt draait: degene met toegang tot vertrouwelijke informatie.

Voor het verzamelen van gegevens wordt onder andere 'scraping software' gebruikt. Dit zijn computerprogramma's die automatisch gegevens verzamelen van open bronnen, met name van sociale media. Facebook, Instagram, LinkedIn – dit soort platforms zijn alomtegenwoordig in het leven van veel mensen. Persoonlijke gegevens zoals een geboortedatum, woonadres, loopbaan en persoonlijke interesses zijn er relatief eenvoudig en goedkoop te achterhalen. Deze informatie kan vervolgens worden gebruikt om contact te maken. Zo zijn in de Verenigde Staten diverse gevallen bekend waarbij misbruik werd gemaakt van LinkedIn. Personen deden zich bijvoorbeeld voor als headhunter om in contact te komen met een oud-CIA-medewerker. En bij nep-sollicitatieprocedures werden documenten verstuurd die bij opening malware installeerden op de pc van de nietsvermoedende sollicitant.

Word weerbaar

Het verzamelen van openbare informatie is op zichzelf niet verboden, maar het is uiteraard onwenselijk als deze informatie wordt gebruikt voor heimelijke of ondermijnende doeleinden. Weerbaarheid tegen statelijke dreigingen is daarom van groot belang. Nederland neemt veel verschillende maatregelen om statelijke dreigingen tegen te gaan. Mensen bewust maken van de risico's is daar essentieel onderdeel van. Wat kunt u doen om uw (persoons)gegevens zo goed mogelijk te beschermen?

Bescherm uw online privacy

- Wees op social media terughoudend met het verstrekken van contactgegevens en informatie over de exacte invulling van uw werkzaamheden.
- Stel de privacy-instellingen van uw socialmedia-accounts in. Deel informatie, foto's en video's alleen met (bekende) vrienden.
- Wees u bewust met wie u online bevriend of verbonden bent. Kies uw digitale netwerk met zorg en wees kritisch op wie u toevoegt aan uw netwerk.
- Wees u ervan bewust welke gegevens u online invult en achterlaat, bij bijvoorbeeld buitenlandse webwinkels.
- Gebruik de incognitomodus van uw browser. Beheer en verwijder cookies.
- Ga veilig om met uw wachtwoorden. Lange en ingewikkelde wachtwoorden zijn sterker dan korte, eenvoudige wachtwoorden.
- Gebruik waar mogelijk twee-staps-verificatie: een manier om online accounts extra te beveiligen met een code die naar uw telefoon wordt gestuurd.

Bescherm uw apparatuur

- Voorzie uw wifi-netwerk thuis van een sterke vorm van authenticatie.
- Kies bewust waar u een app toestemming toe geeft; houd controle over wat een app van u weet. Kijk ook op ConsuWijzer.nl.
- Klik niet zomaar op bijlagen of links in e-mails. Leer valse e-mails te herkennen. Op de site van Fraudehelpdesk is veel informatie te vinden.
- Gebruik niet zomaar openbare wifi. Hoe handig ook, openbare wifi is niet veilig. Veiliger is om gebruik te maken van uw databundel (3G of 4G verbinding).
- Maak regelmatig back-ups van uw computer, foto's en bestanden op uw telefoon en tablet. Zo beperkt u de schade als bijvoorbeeld door ransomware bestanden gegijzeld worden.
- Draai updates van uw software. Zo voorkomt u dat virussen gebruikmaken van kwetsbaarheden in oude versies van programma's. Het helpt om hiervoor automatisch updaten in te stellen.

Informatie voor ouders

- Verdiep uzelf in de virtuele wereld van Facebook, Instagram, Snapchat, TikTok en Twitter. Ga erover in gesprek, bijvoorbeeld door samen de Ouder & Kind Quiz te doen op www.mediawijsheid.nl/ouderkindquiz.
- Wijs uw kind op het belang van privacy. Maak duidelijk dat je nooit persoonlijke informatie, zoals e-mailadressen, huisadressen of telefoonnummers, online moet plaatsen. Gebruik het online privacy stappenplan van Mijn Kind Online en help uw kind in 6 stappen naar het bewaken van zijn/haar eigen online identiteit.
- Maak gebruik van de functie 'ouderlijk toezicht'. Veel verschillende platforms bieden deze mogelijkheid, waarmee u het type medium kan filteren/blokkeren/beperken/controleren. Let wel op: dit is een hulpmiddel, begeleiding van kinderen bij het gebruik van (online) media blijft belangrijk. Kijk op Kijkwijzer.nl voor meer informatie over 'ouderlijk toezicht'.

Wees alert op vreemde activiteiten

- Wees altijd kritisch. Is de webwinkel te vertrouwen? Waar gaat de link naar toe? Wie vraagt om persoonlijke informatie? Is het echt nodig een kopie van uw identiteitsbewijs te sturen?
- Realiseer u dat informatie over uw werk en netwerk zeer waardevol kan zijn voor anderen. Bedenk daarom goed met wie u deze informatie deelt.
- Krijgt u een raar gevoel bij mensen of instanties die contact met u leggen? Wordt u online benaderd door vreemde accounts? Dan is het altijd raadzaam om u terughoudend op te stellen en dit te melden bij de afdeling veiligheid van uw werkgever.

Waar kunt u terecht?

Kijk voor meer tips over het beschermen van uw online privacy op veiliginternetten.nl. Heeft u twijfels over de oprechtheid van een (online) contact? Meld dit dan bij uw werkgever.

Waarom deze infosheet van de NCTV?

Veiligheid is allereerst een eigen verantwoordelijkheid van personen en organisaties. De overheid, vaak bij monde van de politie, geeft hiervoor advies. De NCTV identificeert en duidt dreigingen en risico's. Als adviseur nationale veiligheid helpen we de weerbaarheid van onder andere burgers en bedrijven te verhogen. Het is vanuit die verantwoordelijkheid dat de NCTV deze infosheet heeft opgesteld.