

Malware: Wat is het en hoe kan ik me ertegen beschermen?

De laatste fraudecijfers...

Fraudehelpdesk publiceerde kortgeleden een nieuwsbericht met de fraudecijfers van 2024. Het totaal aantal fraudemeldingen is met wel 10% toegenomen ten opzichte van 2023. Vooral het aantal meldingen van telefonische oplichting verdubbelde vorig jaar. Denk bijvoorbeeld aan fraudeurs die zich telefonisch voor doen als bankmedewerkers, en zo mensen proberen te overtuigen om hun geld over te maken naar een bankrekening waar het geld zogenaamd 'veilig' is.

Ook het aantal meldingen van valse e-mails is flink gestegen. In zo'n geval ontvangt u een e-mail die door een betrouwbare instelling lijkt te zijn gestuurd. Vaak vraagt zo'n e-mail u om op een bepaalde link te klikken. Als u dat doet, kan uw apparaat besmet raken met schadelijke software. Die software noemen we malware.

Wat is malware?

Malware is kwaadaardige software die door cybercriminelen op uw computer, smartphone of tablet kan worden geïnstalleerd via e-mails, apps, sms'jes en websites. Het doel? Uw persoonlijke gegevens in handen krijgen. Hiermee kunnen fraudeurs bijvoorbeeld toegang krijgen tot uw bankrekening om geld over te boeken en identiteitsfraude te plegen. Er zijn veel verschillende soorten malware. Een veelvoorkomende variant van malware, is spyware. Spyware bespioneert uw activiteiten zonder dat u het doorheeft. Het is alsof er een spion in uw apparaat zit die alles wat u doet registreert en naar een externe partij stuurt. De naam spyware komt van de Engelse woorden spion ('spy') en software ('ware'). Ook uw telefoon kan besmet raken met spyware. Dit gebeurt tegenwoordig vaak doordat mensen onbewust schadelijke apps op hun telefoon downloaden.

Het is een vervelend idee, maar gelukkig kunt u zich hiertegen beschermen. Onder andere door te begrijpen wat het is, en hoe u het kunt herkennen.

Hoe herkent u schadelijke apps?

Schadelijke apps en spyware bespioneren u en uw telefoon. Maar schadelijke apps werken net wat anders dan spyware. Deze apps gebruiken namelijk de ingebouwde functies van uw telefoon om informatie te verzamelen. Ze vragen vaak om allerlei toestemmingen die ze eigenlijk niet nodig hebben. Zoals een simpele zaklamp app die toegang vraagt tot uw camera, microfoon, locatie, contacten en agenda. Het is dus belangrijk om goed te kijken welke toestemmingen een app vraagt. En of deze toestemmingen eigenlijk wel nodig zijn om de app te kunnen gebruiken.

Spyware werkt stiekem op de achtergrond en steelt informatie. Een voorbeeld van spyware die op de achtergrond werkt, is een keylogger. Een keylogger is een spyware die elke toetsaanslag op uw apparaat vastlegt. U kunt een keylogger op uw apparaat krijgen door te klikken op een link in een e-mail, WhatsApp-bericht of sms van een cybercrimineel.

Malware: Wat is het en hoe kan ik me ertegen beschermen?

Soms is de kwaadaardige software verborgen in een doodgewone app in de App Store of Google Play Store. Gelukkig kunt u er op verschillende manieren achter komen of uw apparaat besmet is met spyware.

De signalen van spyware op uw apparaat

Stel dat u opeens merkt dat uw datagebruik zonder duidelijke reden omhoogschiet. Of dat u moeite heeft met inloggen op uw accounts. Dit kunnen tekenen zijn dat uw apparaat besmet is met spyware. Sommige spyware kan zelfs antivirus- en beveiligingssoftware uitschakelen, waardoor uw apparaat nog kwetsbaarder is. Daarnaast is het belangrijk om alert te zijn wanneer u signalen van fraude ontvangt. Zoals het ontvangen van berichten van uw bank dat uw betaallimiet opeens verhoogd is. Spyware kan hiervan de oorzaak zijn. Spyware kan namelijk verschillende soorten gegevens verzamelen om fraude te plegen, zoals:

- Inloggegevens (wachtwoorden en accountinformatie)
- Internetgebruik
- Biometrische gegevens (lichaamskenmerken) en webgebruik
- Vertrouwelijke gegevens zoals creditcardinformatie en burgerservicenummers

Wat te doen als u vermoedt dat uw telefoon of computer besmet is met spyware?

Als u denkt dat uw apparaat besmet is met spyware, dan kunt u enkele stappen nemen om uzelf te beschermen:

Zorg er eerst voor dat uw besturingssysteem up-to-date is. Updates kunnen problemen oplossen die hackers gebruiken voor hun aanvallen.

Download geen apps uit onbekende app-winkels, omdat deze mogelijk niet veilig zijn.

Controleer altijd de apps die u downloadt. Kijk naar de ontwikkelaar, het aantal downloads en de reviews. Let ook op spelfouten en slechte grammatica in de beschrijving en screenshots van de app, dit kan een teken zijn van een slechte app. Volg de aanbevelingen van betrouwbare bronnen zoals veiligbankieren.nl of veiliginternetten.nl.

Let op de toestemmingen die een app vraagt. Als een simpele rekenapp bijvoorbeeld om toegang tot uw camera of microfoon vraagt, kan dit een teken zijn dat de app eropuit is om informatie te verzamelen.

Verwijder oude, ongebruikte apps.

Zorg ervoor dat uw telefoon altijd vergrendeld is wanneer u hem niet gebruikt, en houd de telefoon in de gaten.

Installeer beveiligingssoftware om uw apparaat te beschermen en om uw privacy te waarborgen.

Malware: Wat is het en hoe kan ik me ertegen beschermen?

Hoe meldt u fraude?

Op een onbewaakt moment kan het toch gebeuren dat u het slachtoffer wordt van een fraude. Dit kan iedereen overkomen. Dan is het belangrijk dat u weet wat u moet doen, zodat u snel in actie kunt komen:

Neem zo snel mogelijk contact op met de bank waar uw tegenrekening loopt.

Zorg dat u de bank ook zo snel mogelijk belt. Doe altijd online aangifte bij de politie. Meld het ook als u géén schade heeft. Zo helpt u de politie beter zicht te krijgen op de fraudeurs.

Meld fraude bij de Fraudehelpdesk. De Fraudehelpdesk is de nationale helpdesk voor vragen en meldingen over fraude.

De Fraudehelpdesk gebruikt die meldingen voor advies aan slachtoffers van fraude en om anderen te waarschuwen.

Wilt u meer lezen over fraude en veilig bankieren?

Op het gezamenlijk voorlichtingsplatform van banken veiligbankieren.nl vindt u meer informatie over dit onderwerp. Op onze website leest u meer over de stappen die u kunt nemen om veilig bij ons te sparen.

Bron: Lloyds Bank