

Oplichters nemen controle van op afstand over mijn toestel (Remote Access Scam)

Hoe kan ik dit voorkomen en herstellen?

1. Hoe herken je deze vorm van oplichting?

Om te helpen met technische problemen maken IT-professionals gebruik van software die van op afstand verbinding maakt met de computers van hun klanten of medewerkers. Hiervoor gebruiken ze **Remote Desktop Software**, zoals bijvoorbeeld AnyDesk of TeamViewer. Jammer genoeg gebruiken ook hackers en oplichters deze software om verbinding te maken met de computer van hun slachtoffers. Deze vorm van hacking of oplichting heet **Remote Access Scam**. Hoe gaat dat in z'n werk?

1. **Oplichters benaderen je met één of andere smoes.**
 - Ze beweren dat je een beveiligingsprobleem hebt, dat er vanuit jouw computer errorberichten naar hen worden verstuurd of dat je een computervirus hebt.
 - Soms verzinnen ze andere verhalen: je bent zagezegd opgelicht en zij zullen helpen om je geld terug te krijgen, je maakt kans op een goede investering of je wordt genoemd in een gerechtelijk onderzoek.
 - Of je krijgt een virusmelding op je computer en je wordt uitgenodigd om contact op te nemen via een telefoonnummer (vaak een buitenlands of betalend nummer).
2. **Daarna vragen ze je een programma te downloaden** waarmee ze je verder kunnen helpen. Je krijgt instructies om het programma te installeren en acties uit te voeren. Het gaat om programma's waarbij jij de toestemming geeft om mee te kijken en handelingen uit te voeren op jouw toestel.
3. **Nu heeft de oplichter de volledige controle over je toestel.** Daardoor kan die onder meer je online bank account beheren, virussen installeren of je wachtwoorden en andere gegevens stelen of veranderen. Op die manier kan de hacker op een later tijdstip zelfs terug keren naar je toestel.
4. Het gebeurt dat je op het einde van de interventie **een bedrag moet overmaken voor de geleverde dienst**. Soms betaal je op de koop toe voor de oproep omdat je naar een **betaalnummer** belde.

2. Hoe voorkomen dat je slachtoffer wordt van de Remote Access Scam?

1. Geef een onbekende nooit toegang tot je toestellen

Download nooit programma's waarbij je iemand de toestemming geeft om 'mee te kijken' in je toestel, tenzij je deze persoon vertrouwt (familie of de ICT-dienst van je werkgever of leverancier) en je ook helemaal zeker bent dat je deze persoon aan de lijn hebt en niet iemand die zich voordoeft als een bekende.

2. Vertrouw nooit online hulp die je ongevraagd wordt aangeboden voor een probleem dat je niet zelf opgemerkt hebt

Wees altijd op je hoede als een onbekende je onverwacht wil helpen en vraagt om programma's te downloaden en een aantal acties uit te voeren. Microsoft, Apple, de politie, de overheid of je bank zullen je nooit ongevraagd contacteren en vragen om Remote Desktop Software zoals TeamViewer of Anydesk te installeren.

3. Reageer niet op beveiligingsberichten die op je computer verschijnen en je vragen om naar een nummer te bellen voor hulp of ondersteuning

Als er een beveiligingsbericht op je toestel verschijnt, moet je daar enkel op reageren als je zeker bent dat het van je eigen antivirus afkomstig is. Een onverwacht bericht of pop-up waarin je gevraagd wordt om een telefoonnummer te gebruiken is zeer verdacht.

Wat moet je doen als je een programma installeerde?

Wat moet je doen als de oplichter toegang had tot je online bank account?

- Zie aparte info WAT TE DOEN IN GEVAL VAN.....