HACKHELPDESK

Eerste hulp bij cybercrime voor ondernemers

HACKHELPDESK.NL

TECHSUPPORT-SCAM

Wat is techsupport-scam?

Techsupport-scam is een vorm van cybercrime waarbij het slachtoffer wordt gebeld door iemand die zich voordoet als een medewerker van bijvoorbeeld Microsoft. Dit kan bijvoorbeeld een 'security-expert' of een 'technician' medewerker zijn.

Hoe gebeurt het?

In het gesprek wil de crimineel je doen geloven dat er problemen zijn ontdekt met de software van bijvoorbeeld Microsoft. De crimineel zal aandringen om snelle maatregelen toe te passen om het bestaande probleem te verhelpen en grotere problemen te voorkomen. Daarvoor zijn wel aanpassingen nodig op je computer. De beller is bereid om tegen betaling de zogenaamde problemen te verhelpen. Hier is sprake van oplichting/phishing.

Wat is het doel?

De crimineel is op je geld uit en wil je ertoe verleiden om tegen betaling onveilige software (een virus) op je pc te installeren. Hiermee krijgt de crimineel toegang tot je pc en bestanden. Daarnaast wordt bijna altijd het bedrag dat je voor de telefonische hulp moet betalen tijdens het betaalproces (ongemerkt) verhoogd. Hier kom je vaak pas later achter wanneer je onraad ruikt of je bankafschrift onder ogen krijgt.

REPRESSIE

Wat je vooral wel moet doen.

Stap 1

Verander zo snel mogelijk al je wachtwoorden, zeker op de belangrijkste plekken. Kies voor ieder account een uniek wachtwoord van tenminste 12 tekens.

Stap 2

Blokker je creditcard als je deze gegevens hebt verstrekt. Of neem contact op met je bank.

Stap 3

Scan je systeem met een malware scanner (bijvoorbeeld malwarebytes).

Stap 4

Heeft men toegang gehad tot je computer? Dan is het aan te raden om je harde schijf te wissen en het systeem opnieuw te installeren. Lukt je dit niet zelf? Neem dan contact op met een IT-specialist.

Stap 5

Zorg dat je virusscanner up-to-date is.

Stap 6

Doe aangifte zodat dit soort praktijken worden aangepakt. Dit kan nog niet online. Bel 0900-8844 voor een afspraak op een politiebureau.

HACKHELPDESK

Eerste hulp bij cybercrime voor ondernemers

HACKHELPDESK.NL

PREVENTIE

Om techsupport-scam te voorkomen is het vooral van belang dat het leert te herkennen en de werkwijze van de oplichters weet.

Leer het herkennen

Als je wordt bereikt ...

... doet de crimineel zich voor als een helpdeskmedewerker van bijvoorbeeld Microsoft of Windows en zegt dat je een computerprobleem hebt. Dit zou kunnen door zogenaamde fouten, een virus, dat je geen officiële/legale Windows zou hebben of dat je bent gehackt.

... spreekt de nepmedewerker Engels, vaak met een buitenlands (Indiaans) accent.

... wordt er gebeld vanaf een buitenlands of afgeschermd telefoonnummer.

Word je gebeld of herken je dit? Verbreek dan altijd de verbinding!

Werkwijze oplichters

Als je toch op het verhaal van de nepmedewerkers ingaat, volgen meestal de volgende stappen:

- Om je te kunnen "helpen" vragen de oplichters je een programma te downloaden, zodat ze op afstand je pc kunnen bedienen.
- Ze proberen je te overtuigen dat je een computerprobleem hebt door trucjes. Bijvoorbeeld door logboeken met foutmeldingen te tonen. Deze foutmeldingen komen echter op iedere pc voor, zijn niet ernstig en hoeven niet opgelost te worden. Of ze spelen in op actueel nieuws,
- Om de zogenaamde problemen op te lossen vragen ze om een betaling.
- Oplichters die een stapje verder gaan, laten je de betaling via internetbankieren uitvoeren en verhogen dan ongezien het bedrag of stelen je bank-creditcardgegevens.

Minder frequent, maar ook gemeld zijn:

- Het installeren van schadelijke software, zoals gijzelsoftware, die bijvoorbeeld al je bestanden blokkeert. Pas na betaling zou het probleem worden opgelost.
- Het stelen van privacygevoelige of persoonlijke gegevens, zoals wachtwoorden.
- Oplichters die zich voordoen als bankmedewerker en zeggen dat er iets mis is met je bank of creditcard om zo betaalgegevens af te troggelen. Ook helpdeskfraude uit naam van Google of Ziggo komt voor.