WWW.MINDYOURSTEP.INFO

Een Microsoft Scam

Wat is het? En hoe kun je het ontlopen?

De vraag

Je telefoon gaat, je neemt op en aan de andere kant van de telefoon hoor je iemand in (vaak) gebrekkig Engels: 'Hello sir/madam, You are speaking with one of the staff members of Microsoft. We have detected a serious vulnerability on your computer. Fortunately, we like to help you solve this!' OH NEE! Een beveiligingsprobleem op jouw computer maar goed dat een van de medewerkers van Microsoft jou wilt helpen met dit probleem.

STOP! NEE!

Zodra je een dergelijk telefoontje krijgt moeten bij jou direct alle alarmbellen gaan rinkelen en moet je ophangen. 'Huh? Hoezo?' denk je misschien...

De uitdaging

Bij een dergelijk telefoontje doet een beller zich namelijk voor als een medewerker van Microsoft. Dit wordt een Microsoft Scam genoemd. Dergelijke bellers doen zich niet alleen voor als medewerkers van Microsoft ook andere bedrijven worden gebruikt, de algemene term voor dergelijke telefoontjes is 'Tech Support Scam'.
Zoals de naam al zegt: oplichting door technische ondersteuning te bieden. Tech Support Scam is een vorm van social engineering, een van de meest voorkomende cyberaanvallen. Bij social engineering probeert een cybercrimineel toegang te krijgen tot jouw gegevens via persoonlijk contact met jou. Ook wordt social engineering bijvoorbeeld gebruikt om een (beveiligd) gebouw binnen te komen.
Via Tech Support Scam proberen oplichters toegang te krijgen tot jouw computer, jouw persoonlijke gegevens en daar waar ze in de meeste gevallen direct of indirect op uit zijn: jouw geld. Dit doen ze bijvoorbeeld door jou bepaalde software te laten downloaden, zodat ze vanaf een afstandje het 'probleem' kunnen oplossen. Aan het einde van het gesprek word je gevraagd om te betalen, via internetbankieren, iDeal, Western Union of in de vorm van iTunes cadeaukaarten, als dank voor de geboden 'hulp'. Vaak zorgt deze software er tevens voor dat ze jouw computer van een afstand kunnen overnemen, waardoor de oplichter bijvoorbeeld ongemerkt het bedrag dat jij betaalt kan verhogen. Wordt deze verhoging toch door jou opgemerkt? Dan is de kans groot dat de oplichter jouw computer blokkeert.

De oplossing

We geven je graag een aantal tips:

- De beste tip gaven we je al in de inleiding: het gesprek beëindigen! Laat je niet verleiden door gladde praatjes, maar hang direct op!
- Loopt een telefoontje niet geheel zoals hiernaast beschreven, maar vertrouw je het toch niet? Hang dan ook op. Bedrijven bellen je nooit zomaar op als het gaat om dit soort zaken.
- Installeer überhaupt nooit illegale software op je computer.
- Houd je software up-to-date.
- Maak gebruik van een anti-virusprogramma en een firewall.

Toch slachtoffer geworden van Tech Support Scam? We geven je een aantal tips:

- Informeer direct je bank.
- Pas jouw gebruikersnamen en wachtwoorden gelijk aan. En maak daarbij gebruik van een sterk wachtwoord.
- Verwijder de (mogelijk) kwaadaardige software van je computer. Schakel hiervoor, indien nodig, een specialist in.

Meer weten?

Bezoek onze website www.mindyourstep.info voor meer tips en tricks op privacy- en informatieveiligheidsvlak. Of neem direct contact op met Marijn Berndes via marijn@soulmade.nl of door te bellen naar 0162-430345.