HACKHELPDESK

Eerste hulp bij cybercrime voor ondernemers

HACKHELPDESK.NL

SMISHING

Wat is smishing?

Smishing staat voor 'SMS phishing'.

Hoe gebeurt er?

Zoals bij phishing, krijgt de gebruiker een berichtje dat op een urgente manier vraagt om actie te ondernemen. Bij smishing wordt een tekstbericht verzonden naar de telefoon van de gebruiker, in plaats van naar het e-mailaccount. Het bericht vraagt de gebruiker doorgaans om onmiddellijk actie te ondernemen door een telefoonnummer te bellen of zich naar een bepaalde website te begeven. Het telefoontje wordt vaak beantwoord door een automatisch antwoordsysteem. Aan de gebruiker wordt gevraagd om actie te ondernemen door persoonlijke informatie zoals wachtwoorden of creditcard informatie te verstrekken. Klik niet op dit soort links en bel niet naar het telefoonnummer.

Wat is het gevaar?

Smishing is vooral gevaarlijk omdat mensen vaak eerder geneigd zijn een sms te vertrouwen dan een e-mail.

REPRESSIE

Wat je vooral wel moet doen.

Stap 1

Verander zo snel mogelijk al je wachtwoorden. Kies voor ieder account een uniek wachtwoord van tenminste 12 tekens.

Stap 2

Bel de instantie waarvan het bericht zogenaamd afkomstig is (bijvoorbeeld je bank) en geef door wat er gebeurd is. Geef hierbij duidelijk aan welke (persoons)gegevens gelekt zijn.

Stap 3

Blokkeer direct je bankpas of creditcard als deze gegevens gelekt zijn.

Stap 4

Stel (mits van toepassing) je eigen organisatie op de hoogte van het incident.

Stap 5

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

Stap 6

Is er schade? Bewaar zoveel mogelijk bewijsmateriaal en doe aangifte bij de politie.

Stap 7

Waarschuw familie, vrienden en kennissen over deze vorm van oplichting.

Stap 8

Meld het nepbericht op fraudehelpdesk.nl

HACKHELPDESK

Eerste hulp bij cybercrime voor ondernemers

HACKHELPDESK.NL

PREVENTIE

Tip 1

Krijg je via een SMS bericht het verzoek om op een link te klikken, dan moeten alle alarmbellen gaan rinkelen. Wie vraagt dat en waarom? Soms kan het écht lijken alsof de afzender betrouwbaar is, bijvoorbeeld je bank of de overheid, maar betreft het toch een oplichter.

Tip 2

Klik nooit zomaar op links en geef ook nooit persoonlijke informatie via SMS of e-mailtjes. Wil je toch per se reageren op de SMS? Controleer dan eerst bij de bron (de afzender) of het klopt. Doe dit niet door te reageren op de sms, maar zoek zelf naar de officiële contactgegevens van de instantie.

Tip 3

Wees extra voorzichtig als je een SMS bericht van bijvoorbeeld een creditcard aanbieder, een bank of de overheid ontvangt. Deze organisaties vragen nooit om persoonlijke informatie via deze kanalen.

Tip 4

Als er een bericht binnenkomt waarvoor je moet inloggen, kun je beter zelf naar het juiste adres gaan in je browser. Dat is veel veiliger omdat je zo zelf de controle hebt over welk webadres je bezoekt. Op die manier minimaliseer je de kans dat je wordt opgelicht.