HACKHELPDESK

Eerste hulp bij cybercrime voor ondernemers

HACKHELPDESK.NL

VISHING

Wat is vishing?

Bij vishing of 'voice phishing' creëert de fraudeur een automatisch systeem van spraakberichten om via telefoontjes naar de persoonlijke gegevens van telefoongebruikers te vragen.

Wat is het doel?

Het doel is hetzelfde als bij e-mail phishing of sms phishing (smishing). Het spraakbericht creëert bij de gebruiker een gevoel van urgentie om actie te ondernemen en bijgevolg informatie te verstrekken.

Verschaf nooit enige informatie aan een automatisch spraakbericht. Bemerk ook dat de bedrieger gemakkelijk een vals telefoonnummer kan aanmaken om zich uit te geven voor iemand anders. Geef nooit enige informatie door indien je niet zelf het telefoongesprek hebt gestart.

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

Stel waar mogelijk een tweestapsverificatie in via instellingen → beveiliging.

Stap 6

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

Stap 7

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

HACKHELPDESK

Eerste hulp bij cybercrime voor ondernemers

HACKHELPDESK.NL

Stap 8

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

Stap 9

Meld het nepbericht op fraudehelpdesk.nl

PREVENTIE

Tip 1

Open geen spraakberichten en andere audiobestanden die binnenkomen via e-mail van mensen die je niet kent. Klik ook niet op links in dit soort e-mails.

Tip 2

Geef nooit zomaar je gegevens over de telefoon, ook niet als de beller betrouwbaar lijkt. Deel dus nooit gevoelige informatie, zeker niet op het verzoek van iemand die zich plotseling via e-mail of telefonisch bij je meldt.

Tip 3

Word je gebeld door iemand met een onbekend nummer die claimt een hoge managementfunctie te hebben? Bel dan ter controle eerst terug naar een bekend telefoonnummer van die persoon.

Tip 4

Wees je ervan bewust dat een stem tegenwoordig na te bootsen is. Het feit dat je een stem herkent, zegt niets over de betrouwbaarheid.

Tip 5

Stel jezelf altijd de vraag: is dit een normaal verzoek? Laat je niet onder druk zetten om mee te werken als je het niet helemaal vertrouwt.