HACKHELPDESK

Eerste hulp bij cybercrime voor ondernemers

HACKHELPDESK.NL

PHISHING

Wat is phishing?

Phishing is het vissen (hengelen) naar inlog- en persoonsgegevens van gebruikers.

Waar gebeurt het?

Phishing gebeurt via (massaal verzonden) e-mails, online handelsplaatsen of berichten op social media. Verder kan phishing ook telefonisch (vishing) of via sms (smishing) worden uitgevoerd.

Hoe gebeurt het?

In het geval van e-mails, online handelsplaatsen of social media wordt er gevraagd om in te loggen op een website die sprekend lijkt op die van bijvoorbeeld een bank of een andere bekende instantie. Als je inlogt worden je inloggegevens meteen doorgestuurd naar de crimineel.

Als phishing telefonisch of via sms wordt uitgevoerd nemen criminelen contact met je op en doen zij alsof ze bij jouw bank werken. Vaak wordt gezegd dat er sprake is van een veiligheidsprobleem. Ze vragen naar de inloggegevens of je krijgt het verzoek naar een valse website te gaan en je gegevens in te vullen.

Wat is het doel?

Phishing heeft als doel om met de gegevens die het slachtoffer invult de bankrekening te plunderen.

REPRESSIE

Wat je vooral wel moet doen.

Stap 1

Verander zo snel mogelijk je wachtwoorden. Begin bij de belangrijkste accounts, zoals je mail of bankrekening.

Stap 2

Is er een wachtwoord gelekt dat je op meerdere plekken gebruikt? Verander dan ook daar direct je wachtwoord. Kies voor ieder account een uniek wachtwoord van tenminste 12 tekens.

Stap 3

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

Stap 4

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

Stap 5

Is er schade? Bewaar zoveel mogelijk screenshots of foto's en doe aangifte bij de politie.

Stap 6

Stel waar mogelijk tweestapsverificatie in via instellingen > beveiliging.

HACKHELPDESK

Eerste hulp bij cybercrime voor ondernemers

HACKHELPDESK.NL

Stap 7

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

Stap 8

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

Stap 9

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

Stap 10

Meld het phishing bericht via fraudehelpdesk.nl om anderen te helpen waarschuwen.

PREVENTIE

Beveilig jezelf

Een goede virusscanner en een spamfolder helpen je om extra alert te zijn bij e-mails die niet in je Postvak IN terecht komen. Ook helpt het om bewust na te denken waar je je gegevens achter laat.

Check de afzender

Krijg je een e-mail van een bedrijf? Kijk dan niet alleen naar de naam van de afzender, maar ook naar het e-mailadres. Kijk ook altijd naar de afzender, hoe word je aangesproken?

Geef niet zomaar gegevens door

Als je wordt aangemoedigd om op een link te klikken om wat voor reden dan ook, dan moeten alle alarmbellen afgaan. Ook wordt er soms aan je gevraagd om een bijlage te downloaden. Als je iets niet vertrouwt, doe het dan niet.

Check de link

Voordat je op een link in een e-mail klikt, controleer dan ALTIJD eerst de link. In de tekst lijkt de link naar sites van bijvoorbeeld de NS of de Mediamarkt te gaan, maar in werkelijkheid stuurt de link je naar een malafide site. Ze lijken op elkaar, maar ze zijn toch anders.

Bij twijfel nooit oversteken

Bedrijven mailen je nooit, maar dan ook echt NOOIT om je persoonlijke gegevens te verifiëren. Wordt het toch gevraagd? Geef dan geen gegevens door. Twijfel je? Neem dan zelf contact op met het bedrijf. Een extra controle kan nooit kwaad.