Herken digitale criminaliteit en handel juist

Het per mail hengelen naar informatie is de snelst groeiende tak van digitale criminaliteit. Het is een vorm van oplichting. Maar hoe herkent u oplichting en wat kunt u er aan doen om uzelf te beschermen? De Unie KBO helpt u om preventieve maatregelen te nemen.
Via de mail, maar ook via de telefoon, lijken betrouwbare instanties zoals een bank of creditcard-maatschappij te vragen om bijvoorbeeld uw inloggegevens, creditcardinformatie, pincode of andere persoonlijke informatie. In werkelijkheid zijn het fraudeurs die achter uw gegevens proberen te komen. Phishing heet deze vorm van internetfraude.

Met een phishing email willen fraudeurs u naar een valse (bank)website lokken dat een kopie van de echte website is. Hier wordt u vervolgens verzocht om uw inlognaam en wachtwoord in te voeren. Op deze manier krijgt de fraudeur de beschikking over uw gegevens. Met alle gevolgen van dien.

Een andere bekende vorm van oplichting zijn emailberichten waarin u wordt verzocht iemand of een bekende te helpen. In deze email, waarin de gebruikte Nederlandse taal direct vragen op zal roepen, doet de internetcrimineel zich voor als een voor u bekend persoon die direct geld nodig heeft omdat hij/zij ergens onderweg is gestrand, zieke familie heeft, enz.. Soms heeft de email een hoog geloofwaardigheidsgehalte doordat deze is ondertekend met de naam van de bekende. In een dergelijk geval is vaak het emailaccount van de bekende gehackt. Soms is de e-mail in het Engels gesteld.

Herkennen

Het is vaak moeilijk een phishing e-mail te onderscheiden van een echte betrouwbare e-mail. Toch zijn er belangrijke kenmerken te noemen waaraan u een phishing e-mail kunt herkennen:

- Banken, creditcardmaatschappijen en andere legitieme bedrijven vragen nooit (bank)gegevens.
- Het taalgebruik en zinsopbouw zijn vaak van slechte kwaliteit.
- Een phishing e-mail is meestal onpersoonlijk.
- Er wordt vaak om een snelle reactie of handeling gevraagd.
- Phishing e-mails spelen vaak in op uw angst om opgelicht te worden.
- In de e-mail wordt gesproken over problemen die urgent zijn of over fraude en oplichting.
- In de e-mail staat vaak een link naar de ‘website’ van een bank. Dit is vaak een valse website.

Wat kunt u doen als u een 'verdachte' e-mail ontvangt?

Lijkt de e-mail te komen van een bekende onderneming? Bijvoorbeeld van een postorderbedrijf, een bank of creditcardmaatschappij?

- Reageer nooit op e-mails waarin om persoonlijke gegevens wordt gevraagd.
- Controleer het digitale ‘certificaat’ van uw bank.
- Zorg dat de beveiliging op uw computer actueel is.
- Wees zelf altijd kritisch op email en verdachte telefoongesprekken.
- Stuur het valse bericht door via Valse e-mail aan uw bank of creditcardmaatschap. Het juiste e-mailadres is te vinden op de site van de bank.

(Bron: Nieuwsbrief 5 Unie KBO)