Wijs&vanOostveen

BOUWEN AAN VERMOGEN SINDS 1987

BEVEILIGD INTERNETTEN

BELANGRIJKE TIPS AANGAANDE CYBERCRIMINALITEIT EN BEVEILIGINGSASPECTEN

Internet heeft een hoge vlucht genomen in onze wereld. Dit zorgt onder anderen voor een steeds sneller verkeer van producten en diensten via het internet. Helaas zijn er, net zoals in het gewone maatschappelijke verkeer, ook criminelen actief op internet. Ondanks alle voorzorgsmaatregelen neemt de criminaliteit op internet, de 'cybercriminaliteit', de laatste jaren steeds meer toe.

Onder deze soort van criminaliteit wordt onder anderen verstaan:

- Identiteitsfraude. Hierbij maakt iemand misbruik van uw persoonlijke gegevens. Onder uw naam worden er producten of diensten besteld, uitkeringen of creditcards aangevraagd, betalingen gedaan of bankrekeningen geopend.
- Hacking. Hierbij wordt ingebroken in een computersysteem of netwerk. Inbrekers kunnen hiervoor onder andere gebruikmaken van virussen, spyware, phishing en poortscans.
- Internetoplichting, zoals phishing, scam, marktplaatsfraude en malafide ticketsites.

Hierna volgt een uitleg van enkele van de hiervoor genoemde vormen van cybercriminaliteit:

- Spyware is de naam voor computerprogramma's (of delen daarvan) die gevoelige informatie van computergebruikers verzamelen zoals bankgegevens en deze doorsturen naar een externe partij.
- Phishing ("vissen"), is een verzamelnaam voor digitale activiteiten die tot doel hebben persoonlijke informatie aan mensen te ontfutselen. Deze persoonlijke informatie kan direct worden misbruikt voor het doen van bijvoorbeeld grote uitgaven (in het geval van creditcardnummers) of voor wat in het Engels "identity theft" wordt genoemd, het stelen van een identiteit. In dit geval zijn bijvoorbeeld gegevens als sofi-nummers, adressen en geboortedata nodig. Phishing is een vorm van internetfraude waarbij u valse e-mails ontvangt die u naar een nagebootste website proberen te lokken. Klik nooit op links in een phishing e-mail. Waarschuw ook altijd de organisatie uit wiens naam u de mail krijgt.
- Poortscans. Voordat inbrekers overgaan tot een inbraak verkennen zij meestal hun terrein. Zij zoeken dan vooral naar zwakke plekken in de beveiliging van uw computer(netwerk). Poortscannen is een van de manieren om via internet een onbeveiligde ingang op een computer te vinden.

Door Wijs & van Oostveen, inclusief de depotbanken waarmee wordt samengewerkt, wordt er veel aandacht besteed om de systemen zo veilig mogelijk te maken en criminaliteit te vermijden dan wel zoveel mogelijk te beperken. Ook de Belegger, als gebruiker van de Website, kan zelf bijdragen aan deze veiligheid door de hierna genoemde zaken in acht te nemen.

De Belegger wordt ten strengste geadviseerd om de volgende beveiligingsmaatregelen te nemen:

- Gebruik altijd de nieuwste versies van uw internet browsers, aangezien browsers vaak aangepast worden met meer en betere beveiligingstechnieken;
- Voer regelmatig software updates uit op uw computer waaronder het installeren van recente updates van antivirus programma's en/of firewalls. Hierdoor worden eventuele gevonden beveiligingslekken verholpen;
- Controleer of gecodeerde pagina's niet op de harde schijf worden opgeslagen. Gecodeerde pagina's worden standaard niet op de harde schijf opgeslagen om te voorkomen dat andere gebruikers op dezelfde PC deze achteraf kunnen raadplegen;

- Bescherm identificatie-/authenticatiegegevens en geef deze gegevens nooit vrij aan anderen, ook niet aan medewerkers van Wijs & van Oostveen en/of een depotbank;
- Geef uw wachtwoord nooit door aan anderen, ook niet aan medewerkers van Wijs & van Oostveen en/of een depotbank;
- Laat uw computer nooit onbewaakt achter, in het bijzonder niet in het geval u zich bevindt op een pagina waarvoor een wachtwoord vereist is en waar u bent ingelogd;
- Sluit de door u bezochte internetsite op een juiste wijze af (log correct uit);
- Gebruik alleen een veilig wachtwoord om oneigenlijk gebruik door anderen te vermijden of zoveel mogelijk te beperken; en
- Vervang regelmatig uw wachtwoord en zorg dat anderen deze niet kunnen inzien of vinden.

Wijs & van Oostveen kan nooit geld of financiële instrumenten van de Quant Notes-rekening overboeken zonder een opdracht van de Belegger. Onttrekkingen van uw Quant Notes-rekening wordt alleen ten gunste van de door de Belegger opgegeven vaste tegenrekening uitgevoerd, welke op de naam van de Belegger is gesteld. Mocht de Belegger ondanks alle voorzorgmaatregelen toch merken dat er misbruik van de Quant Notes-rekening plaatsvindt of als de Belegger het vermoeden heeft dat dit mogelijk gaat plaatsvinden, meld dit dan direct aan Wijs & van Oostveen. Wij zullen dan zo snel mogelijk maatregelen nemen om de schade te vermijden of te beperken. Ondanks alle beveiligingsmaatregelen kan de Belegger slachtoffer worden van cybercriminaliteit, waarbij de daaruit voortvloeiende schade altijd voor rekening van de Belegger komt.