

Checklist phishing

By Checklist Wizard

- Check https
 - Controleer of het webadres begint met https://, waar de s staat voor secured: beveiligd
Dat betekent dat de verbinding is versleuteld en kan daardoor niet worden afgeluisterd.
 - Maar vraag ook het certificaat van echtheid op
Zo zie je of het gebruikte SSL-certificaat (Secure Socket Layer) wel hoort bij de bank of webwinkel die men zegt te zijn.
 - Dat doe je in Internet Explorer door op het gouden slotje te klikken rechts naast na de adresbalk.
 - Klik in Firefox in de adresbalk op de naam van de website op een blauwe of groene achtergrond.
- Klik niet zomaar op linkjes
 - Phishers gebruiken vaak links in e-mailberichten die bij een hele andere website uitkomen.
 - Je kunt in webmail of in je mailpakket de werkelijke bestemming eenvoudig checken door boven het linkje te zweven met je muiscursor
Dan toont de browser of mailssoftware het werkelijke webadres.
 - Je kunt ook in je mailprogramma even instellen op tekstweergave om te zien waar de link heen leidt.
 - Sluit altijd de browser als je op een inlogpagina terechtkomt.
 - Log altijd in door zelf het adres van de bank in de browser in te voeren.
- Tik zelf webadressen in
 - Tik zelf het adres van uw banksite, webmail of sociale netwerksite in de adresbalk van uw browser in, om in te loggen.
- Verstrek geen inloggegevens
 - Veel phishingmails vragen om persoonlijke informatie of gegevens die al bij de officiële instantie bekend zijn, zoals inloggegevens en transactiecodes.
 - Verstrek nooit zulke persoonlijke informatie via e-mail - en uiteraard ook niet via de telefoon.
- Let op taalfouten
 - Veel phishingmails en phishingsites zijn automatisch vertaald uit het Engels naar het Nederlands en bevatten daardoor slecht Nederlands.
 - Een aanhef 'Lieve klant' (de robotvertaling van Dear customer) maakt duidelijk dat het om een phishingmail gaat.
 - Het omgekeerde geldt echter niet: er zijn steeds meer phishingmails en phishingsites die wel in goed Nederlands zijn geschreven.
- Werk de browser bij
 - Oude en niet-bijgewerkte browsers bevatten nogal eens beveiligingslekken en kwetsbaarheden waardoor phishers de weergave van SSL-certificaten en webadressen in de adresbalk kunnen manipuleren.
 - Nieuwe browsers zijn hier beter tegen beschermd.
 - Daarnaast hebben de meest recente browsers een phishingfilter, die je waarschuwen als je naar een phishingsite surft die op de zwarte lijst staat.
 - Check in je browser of het filter aanstaat.
 - In Internet Explorer heet het phishingfilter SmartScreen
 - In Firefox vind je phishingfilter via Opties - Beveiliging.
- Controleer regelmatig je afschriften
 - Zelfs als alles er normaal uitziet, en er een geldig SSL-certificaat wordt getoond, kan het mis zijn.
 - Er is kwaadaardige software in omloop waarmee cybercriminelen alle informatie op het beeldscherm kunnen manipuleren.

- Daarom blijft het belangrijk om regelmatig je rekeningoverzicht op onbekende transacties te controleren.
- Banken stellen dit in hun voorwaarden ook als eis om uit te keren bij schade.
- Meld phishing direct
 - Neem direct contact op met je bank (liefst telefonisch) als je fraude met je geld vermoedt.
 - Hierdoor kun je voorkomen dat de schade nog groter wordt.
 - Neem bij twijfel over een e-mailbericht contact op met de bank.
 - Gebruik hiervoor het telefoonnummer dat op de originele banksite of het briefpapier van je bank staat.