Digitale fraude

Dagelijks worden we geconfronteerd met digitale fraude en wantoestanden op het internet. Hoe veilig internetbankieren? Hoe een valse website herkennen? Hoe een valse email herkennen? Hoe voorkomen dat iemand mijn pincode misbruikt? Hoe kan ik mijn computer beveiligen?

Geef hackers geen kans door de volgende beveiligingstips na te leven:

- Installeer software updates zodra deze beschikbaar zijn.
- Zorg ervoor dat je draadloos netwerk (wifi) beveiligd is.
- Installeer geen illegale of onbekende software.
- Vergrendel je computer wanneer je hem niet gebruikt. Zo voorkom je dat iemand eenvoudig toegang verkrijgt tot je persoonlijke gegevens en toepassingen.
- Log steeds uit van de bank-website bij het beëindigen van de transacties.
- Fraudeurs vragen steeds om dringend een actie te ondernemen om ergere problemen te voorkomen.
- Voer geen overschrijvingen uit op basis van een telefoongesprek. (bij twijfel kan je voorstellen om zelf terug te bellen)
- Gebruik tweestapsverificatie: gebruik naast een wachtwoord ook een extra beveiliging (bv. gezichtsherkenning én een code)

Hoe kan ik mijn smartphone of tablet beveiligen?

- Vergrendel je smartphone of tablet. Zo voorkom je dat iemand eenvoudig toegang verkrijgt tot je persoonlijke gegevens en toepassingen. Installeer alleen applicaties via de officiële appstores van Apple of Google.
- Gebruik altijd de meest recente versie van de mobiele bank-applicaties. Hetzelfde geldt voor het besturingssysteem van je toestel.

Hoe herken ik een valse e-mail?

- Er wordt vaak verwezen naar een **veiligheidsprobleem** met je bankkaart of je bankrekening.
- Je moet **dringend actie** ondernemen.
- Je moet dringend een **bijlage openen** of op een **link klikken**. De link brengt je naar een valse website waar je persoonlijke gegevens moet ingeven (je debetkaartnummer, de codes die je berekent met je kaartlezer, enz.…).

Hoe herken ik een valse website?

Oplichters gebruiken steeds vaker valse websites waarvan het webadres begint met https://. De ‘s’ in https staat voor “secure” en geeft aan dat de verbinding beveiligd is. Het biedt echter geen garantie dat de partij waarmee je communiceert te vertrouwen is.

Controleer het webadres in de adresbalk bovenaan in je browser.

Hoe kan ik voorkomen dat iemand mijn pincode voor mobiel bankieren misbruikt?

- Houd je pincode geheim. Schrijf ze nergens op en geef ze aan niemand door, ook niet telefonisch bij een dringend probleem.
- Kies geen voor de hand liggende pincode, zoals je geboortedatum of een oplopende cijfercombinaties (12345) zodat deze niet eenvoudig kan geraden worden.
- Kies geen pincode die je ook gebruikt voor een andere toepassing.
- Let op dat er niemand stiekem over je schouder meekijkt wanneer je je pincode invoert.
- Lees steeds de volledige berichten op de kaartlezer, stemt dit bericht overeen met de acties op uw computer. Of gebruik Itsme waar mogelijk.

Wat is quishing?

Een van deze nieuwe bedreigingen is Quishing, een vorm van phishing waarbij QR-codes worden gebruikt.

“Quishing”, een samentrekking van de termen "QR-code" en "phishing". Dit is een vorm van oplichting waarbij fraudeurs hun slachtoffers aanmoedigen om kwaadaardige QR-codes te scannen. Deze codes leiden de slachtoffers vervolgens door naar phishingwebsites of voeren kwaadaardige programma's uit.

Nuttige contactgegevens als er zich een probleem zou voordoen :

- KBC: Secure4u@kbc.be of 016/432 000 (24u/24 en 7d/7 bereikbaar)
- Belfius: phishing@belfius.be of 02/222 46 00 (24u/24 en 7d/7 bereikbaar)
- verdacht@safeonweb.be (is algemeen meldpunt van de overheid)

Interessante websites met informatie :

- https://www.kbc.be/secure4u
- https://www.belfius.be/webapps/nl/selfcare/belfius/fraude

- https://www.safeonweb.be
- Quishing: de nieuwe phishingtechniek | Drupal (safeonweb.be)