MEMO

PHISHING

1/4

Wa's da?

Phishing is een frauduleuze techniek waarbij een oplichter je probeert wijs te maken dat hij een persoon of instelling is die je kent en vertrouwt – een bank, een administratie, een persoonlijk contact... – om zo private of professionele informatie van je los te weken.

Zijn doel?

- De hand leggen op persoonlijke informatie zoals inloggegevens, wachtwoorden, creditcardnummers
- Toegang krijgen tot gevoelige gegevens binnen de Stad
- Ertoe komen dat er geld wordt overgemaakt

Comment ?

Hij belt je, stuurt je een e-mail of een bericht met de volgende inhoud:

- Een geïnfecteerde bijlage die een virus op je apparaat installeert
- Een link die doorverwijst naar een kwaadaardige website
- Een vals betalingssysteem

MEMO

PHISHING

2/4

Zorg ervoor dat je een phishingmail herkent

Wees waakzaam. Bepaalde elementen moeten een belletje bij jou doen rinkelen:

- Er is geen enkele reden waarom je dit bericht ontvangt.
- Het onderwerp van de e-mail is vaag. Je herkent de context niet.
- Hij kwam in je spamfolder terecht.
- Er is sprake van een mogelijke beloning of sanctie.
- De toon is alarmistisch of intrigerend en speelt in op de noodzaak van een dringende reactie

MEMO

PHISHING

3/4

Leer de juiste reflexen aan tegen phishing

- Beantwoord de e-mail niet
- Controleer de conformiteit van het afzenderadres door er met de muiscursor op te gaan staan, zonder te klikken
- Klik niet op de links. Ga er met de muis overheen om er zeker van te zijn dat het om een officieel websiteadres van de organisatie gaat
- Open geen bijlagen, bestanden of afbeeldingen
- Voer geen transacties uit via een onbekend systeem
- Beveilig je gegevens en maak back-ups
- Bespreek het met je collega's
- Stuur de e-mail door naar **ITSecurity@brucity.be**

MEMO

PHISHING

4/4

Onderneem actie als je denkt dat je het slachtoffer bent van een phishingaanval

In het kader van je beroepsactiviteit:

- Stuur onmiddellijk een e-mail naar **ITSecurity@brucity.be**
- Breng je verantwoordelijke en je collega's op de hoogte

In het kader van je privéleven:

- Neem via een ander kanaal contact op met de persoon of organisatie waarvan de identiteit wordt gebruikt
- Wijzig je wachtwoorden
- Als je gegevens met betrekking tot je betaalmiddelen hebt doorgegeven, neem dan onmiddellijk contact op met je bankinstelling
- Scan je computer met je antivirussoftware
- Neem contact op met het Centrum voor Cybersecurity België (CCB) **https://www.safeonweb.be**