Laat u niet vangen!

Cybercrime

PHISHING

Middels phishing trachten criminelen via het internet naar uw persoonlijke informatie en bankcodes te hengelen.

U ontvangt een e-mail die ogenschijnlijk van uw bank uitgaat en u wordt met allerlei smoezen verzocht uw gegevens en codes in te geven.

Het kan zijn dat men u hierbij zelfs opbelt om u bij het login-proces te begeleiden.

Uiteindelijk zal u gevraagd worden om de code gegenereerd door uw kaartlezer of digipass in te geven.

Indien men telefonisch vraagt naar uw codes, beëindigt u best meteen het gesprek nadat u het oproepnummer genoteerd hebt. Geef uw codes ook niet door via chat, SMS, sociale media, etc.

Druk ook niet op (betaal)linken die u via WhatsApp, Facebook Messenger, etc. worden verstuurd.

Bedrijven zoals Microsoft gaan u zelf niet spontaan bellen bij PC problemen etc. Beëindig meteen dergelijk gesprek. Indien nodig neemt u zelf contact op met de klantendienst via de officiële website of e-mailadres.

Wees ook erg voorzichtig met kandidaat kopers die reageren op uw online zoekertjes. Klik geenszins op links, naar valse websites van banken, koeriersbedrijven, etc. die ze u versturen en hierbij om bankcodes vragen.

Meld verdachte e-mails, links en websites aan het Centrum voor Cybersecurity België via verdacht@safeonweb.be.

Phishing e-mails worden ook valselijk verzonden namens de politie of gerechtsdeurwaarders voor openstaande betalingen. Deze zijn vals.

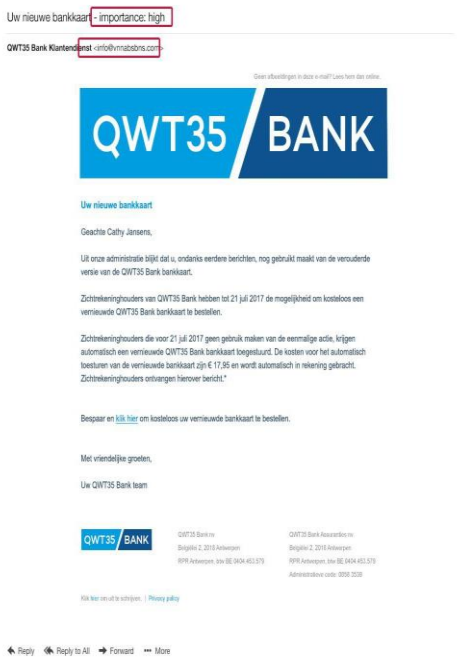
Door waakzaam te zijn, kan u vermijden het zoveelste slachtoffer te worden.

TIPS

1. Maak gebruik van een spamfilter om phishing mails te vermijden.
2. Open geen berichten die u verdacht vindt en download zeker geen bijlagen.
3. Klik niet op een link in een bericht van een onbekende afzender. U kan er wel met uw rechtermuisknop op drukken en selecteer “linkadres kopiëren” teneinde deze aan uw bank en de politie te melden.
4. Controleer het e-mailadres van de verzender. Gebruik de antwoordfunctie om zeker te zijn wat het e-mailadres is van de verzender.
5. Neem bij twijfel persoonlijk contact op met de bank.
6. Geef zelf de website en/of het telefoonnummer van uw bank in.

Hieronder vindt u een voorbeeld van een phishing e-mail. Hetgeen abnormaal is aan de e-mail is in het rood aangeduid.

Ten eerste zal de bank nooit een e-mail sturen met de vermelding “prioriteit: hoog”. Ten tweede is aan de domeinnaam van het e-mailadres te zien dat dit niet het domeinnaam van de bank betreft.


Uw nieuwe bankkaart - importance: high

QWT35 Bank Klantendienst <info@vnnabsbns.com>

QWT35 BANK

Uw nieuwe bankkaart

Geachte Cathy Jansens,

Uit onze administratie blijkt dat u, ondanks eerdere berichten, nog gebruikt maakt van de verouderde versie van de QWT35 Bank bankkaart.

Zichtrekeninghouders van QWT35 Bank hebben tot 21 juli 2017 de mogelijkheid om kosteloos een vernieuwde QWT35 Bank bankkaart te bestellen.

Zichtrekeninghouders die voor 21 juli 2017 geen gebruik maken van de eenmalige actie, krijgen automatisch een vernieuwde QWT35 Bank bankkaart toegestuurd. De kosten voor het automatisch toesturen van de vernieuwde bankkaart zijn € 17,95 en wordt automatisch in rekening gebracht. Zichtrekeninghouders ontvangen hierover bericht.*

Bespaar en klik hier om kosteloos uw vernieuwde bankkaart te bestellen.

Met vriendelijke groeten,

Uw QWT35 Bank team

QWT35 BANK

Reply Reply to All Forward More

WAT ALS HET TOCH MISGEGAAN IS?

1. Neem zo snel mogelijk contact op met uw bank. Vraag de transactie(s) tegen te houden.

2. Meld de feiten meteen aan de politie. Bezorg de politie de exacte data en tijdstippen; de gebruikte email- en internetadressen, namen van de betrokkene(n); afdrukken van chat- en mailberichten en schermafdrukken (via print screen of maak een foto).

openbaar ministerie

Parket Limburg

NUTTIGE LINKS:

- **www.safeonweb.be**
- **www.safeinternetbanking.be**
- **www.cybersimpel.be/nl**
- **www.ccb.belgium.be/nl/work**
- **www.febelfin.be/nl/consumenten/dossier/de-meest-gebruikte-fraudevormen-ontrafeld**