Tips om veilig te bankieren

We maken deze periode van de Corona crisis nog meer gebruik van e-mail, WhatsApp, Internet Banking, Mobile Banking app, ATM- en POS-apparaten en Social Media.
Internet criminelen, ook wel bekend als cybercriminelen, proberen mensen op allerlei manieren te misleiden. Dit doen ze vooral met technieken die 'Phishing' en 'Ransomware' worden genoemd.

Wees daarom voorzichtig met het openmaken van bijlagen in e-mails vooral als die er vreemd en verdacht uitzien, dit kan een phishing email zijn, waarbij de bijlage ransomware bevat.

Wat is phishing?
Een 'phising mail' lijkt erg op een normale mail van DSB en heeft als doel uw persoonlijke gegevens te achterhalen om zo toegang te krijgen tot uw rekeningen en hier geld van af te halen.

Wat is ransomware?
Dit is malafide software die internet criminelen trachten te installeren op uw computer en die vervolgens documenten en informatie op uw computer onleesbaar en dus onbruikbaar maakt.

Enkele tips:

- Open geen e-mails en bijlagen van onbekenden, verwijder de e-mail direct;
- Klik niet zomaar op bijlagen en/of de weblinks/URLs;
- Betaal online alleen via beveiligde websites (gesloten hangslot in de URL);
- Deel of stuur nooit uw pincode en/of wachtwoord via een e-mail, smsje, appje of Facebook;
- Benader DSB Internet Banking via de beveiligde website https://www.dsb.sr

Alhoewel een 'phishing-mail' op een 'normale e-mail' lijkt, kan deze toch worden onderscheiden door te letten op:

1. Afzender:
a. Controleer het adres van de afzender;
b. Controleer de domeinnaam waarvan u de e-mail hebt ontvangen;
c. Controleer of het e-mailadres ook echt overeenkomt met het websiteadres.

2. Aanhef; in de meeste gevallen weten deze cybercriminelen niet wie de ontvanger is; een meneer of een mevrouw. Als een instantie een e-mail naar u verstuurt en zo ook DSB als zij een algemene e-mail verstuurt, gebruikt ze meestal uw achternaam. Cybercriminelen gebruiken algemene termen, zoals 'Geachte heer/mevrouw' of 'Beste klant'

3. Er wordt gevraagd naar persoons- of gevoelige gegevens. In de meeste gevallen wordt er gevraagd naar persoonlijke gegevens. DSB vraagt nooit naar persoonlijke of gevoelige gegevens per e-mail. Dat geldt ook voor overige instanties, z.a. banken, verzekeringsmaatschappijen enz.

4. Spoed of laatste waarschuwingen; In veel valse e-mails probeert men u onder druk te zetten door gebruik te maken van laatste waarschuwingen of spoedmeldingen.

5. Links of bijlagen; In de meeste phishing e-mails is er een link of een bijlage aanwezig waarin u gevraagd wordt om erop te klikken.

6. Controleer de e-mail en de domeinnaam op taalfouten, spellingsfouten.

7. Vaak wordt ingegaan op iets dat speelt en de aandacht heeft, bijv. Corona-virus.

8. De indruk wordt gewekt dat het van *een betrouwbare instantie afkomstig* is (check dus goed de domeinnaam).

9. Er wordt iets *gratis* aangeboden.

10. Er wordt aangegeven dat er *een probleem* is met uw account en dat die instantie het zal oplossen.

Heeft u een 'phising-mail' van DSB gehad? Stuur deze door naar contactcenter@dsb.sr.
Laten wij samen cybercrime tegengaan!