B1.2.1 Pas op! Zo voorkom je phishing

Uwaga! Tak zapobiegasz phishingowi

Phishingmails lijken steeds echter, *omdat* criminelen bijna geen spelfouten meer maken. Ze gebruiken vaak dwingende taal, zodat u snel op een **link** klikt en te veel informatie geeft. Controleer daarom altijd de **afzender** en de domeinnaam, en ga liever zelf naar de **officiële website**. Scan ook nooit een **QR-code** in een e-mail voor betalingen of om in te loggen. Een bank vraagt nooit om **persoonlijke gegevens** via e-mail.

*E-maile phishingowe wyglądają coraz bardziej wiarygodnie, ponieważ przestępcy prawie nie robią już błędów ortograficznych. Często używają języka wywierającego presję, abyś szybko kliknął/kliknęła **link** i podał/podała zbyt dużo informacji. Dlatego zawsze sprawdzaj **nadawcę** i nazwę domeny, a najlepiej wejdź sam(a) na **oficjalną stronę internetową**. Nigdy też nie skanuj **kodu QR** w e-mailu do płatności lub logowania. Bank nigdy nie prosi o **dane osobowe** przez e-mail.\/p>*

1. Waarom gebruiken criminelen vaak dwingende taal in een e-mail?
   a. Omdat ze willen dat u snel klikt zonder na te denken.
   b. Omdat ze willen dat u altijd op 'afmelden' klikt.
   c. Omdat ze willen dat u rustig de mail bewaart.
   d. Omdat ze willen dat u het bericht doorstuurt naar de bank.
2. Wat is een veilige manier om te controleren of een link betrouwbaar is?
   a. De link direct openen en meteen inloggen.
   b. De link doorsturen naar vrienden voor advies.
   c. De QR-code in de mail scannen om sneller te betalen.
   d. Met de muis over de link zweven om de domeinnaam te controleren.

1-a 2-d