

B1.2.1 Pas op! Zo voorkom je phishing

Attention ! Voici comment éviter le phishing



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.



Les e-mails de hameçonnage semblent de plus en plus authentiques, parce que les criminels ne font presque plus de fautes d'orthographe. Ils utilisent souvent un langage pressant, afin que vous cliquiez rapidement sur un lien et que vous donniez trop d'informations. Vérifiez donc toujours l'expéditeur et le nom de domaine, et allez plutôt vous-même sur le site officiel. Ne scannez également jamais un code QR dans un e-mail pour des paiements ou pour vous connecter. Une banque ne demande jamais de données personnelles par e-mail.

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

1-c-2-b