

# Phishing: *Het vissen naar uw bankgegevens*

Stel, u ontvangt een e-mail waarin wordt gevraagd om uw inloggegevens voor internetbankieren. Of waarin een link staat naar een andere inlogpagina dan u gewend bent. Wat doet u? U verwijdert de e-mail. De bank zou zo'n mail namelijk nooit sturen.

## Wat is phishing?

Phishing is het vissen naar uw gegevens door internetcriminelen. Meestal gebeurt dit via een e-mail die van uw bank afkomstig lijkt. Hierin wordt u gevraagd uw gegevens terug te sturen of in te voeren op een website. Bijvoorbeeld uw naam, adres, telefoonnummer, rekeningnummers en beveiligingscodes. Deze gegevens gebruiken de criminelen vervolgens om toegang te krijgen tot uw bankrekening.

## Wat is ertegen te doen?

De banken volgen de ontwikkelingen op het gebied van internetfraude nauwgezet en nemen maatregelen waar nodig. Daarnaast werken ze nauw samen met opsporingsinstanties om phishing sites op te sporen en uit de lucht te halen. En mocht u schade oplopen door phishing, dan wordt dit meestal vergoed.

Voor u wordt het steeds lastiger om nepmails en nepsites te herkennen. Criminelen worden namelijk steeds behendiger in het namaken. Eigenlijk kunt u maar een ding doen: onthoud dat uw bank **nóóit** ergens anders dan op de eigen inlogpagina om uw inloggegevens zal vragen.

VEILIG BANKIEREN 



## Nepmail: daar trapt u niet in!

- Verstrek nooit persoonlijke bankgegevens of inlogcodes
- Klik niet op links in een nepmail en verwijder de e-mail uit uw mailbox
- Kijk voor meer informatie op [www.veiligbankieren.nl](http://www.veiligbankieren.nl)



Nederlandse  
**Vereniging** van Banken