De Nederlandse banken hebben vijf principes voor veilig internetbankieren opgesteld. Lees ze door en volg ze op. Als er iets verdachts gebeurt:

HANG OP!
KLIK WEG!
BEL UW BANK!

1. Houd uw beveiligingscodes geheim.
2. Zorg ervoor dat uw betaalpas nooit door een ander gebruikt wordt.
3. Zorg voor een goede beveiliging van de apparatuur die u gebruikt voor uw bankzaken.
4. Controleer uw bankrekening.
5. Meld incidenten direct aan uw bank en volg aanwijzingen van de bank op.

www.veiligbankieren.nl

In opdracht van de gezamenlijke banken:

Nederlandse Vereniging van Banken

Betaalvereniging Nederland

BANKIERT U VEILIG?

Internetcriminelen verzinnen steeds nieuwe manieren om u uw betaalpas of uw persoonlijke codes te ontfutselen. Ze bellen op of sturen e-mails en zeggen dat ze van uw bank zijn. Blijf dus alert! Lees deze folder door, dan weet u precies waar u op moet letten.

De persoon die u belt klinkt misschien vriendelijk en vertrouwd, maar weet u zeker dat u uw bank aan de lijn hebt? Hang op als iemand uw pincode of inlogcodes voor online bankieren wil weten. Een echte bankmedewerker zal hier nooit om vragen.

Internetcriminelen doen veel moeite om een e-mail van uw bank na te maken. Wordt in een mail gevraagd op een link te klikken, gegevens in te vullen of uw betaalpas op te sturen? Doe het niet, klik weg! Meld valse e-mails bij uw bank. Op www.veiligbankieren.nl/meldnummers staan alle email-adressen.

Is uw smartphone of computer gestolen?
Bent u uw bankpas kwijt? Kreeg u een vreemd telefoontje van een bankmedewerker? Heeft u verdachte afschrijvingen ontdekt? Ziet de inlogpagina van internetbankieren er anders uit dan normaal?
Bel uw bank!

NEPMAIL, DAAR TRAPT U NIET IN

Internetcriminelen doen aan phishing: ze versturen nepmails en doen zich voor als uw bank of een andere vertrouwde organisatie. Met zo'n mailtje lokt de crimineel u naar een valse website, die bijvoorbeeld op die van uw bank lijkt.

Nietsvermoedend logt u in met uw persoonlijke gegevens. Zo komen uw gegevens in handen van de crimineel.

Als u weet waar u de meeste phishingmails aan kunt herkennen, verkleint u de kans dat u in de trucs van de internetcrimineel trapt.

De e-mail hieronder lijkt in eerste instantie van een bank te komen. **Maar pas op! De e-mail is nep.**

From: ABN AMRO Bank (klantenservice@abnanro.nl) — 1
Subject: Uw betaalpas moet vervangen worden

ABN·AMRO

Geachte relatie, — 2

Wij hebben u al meerdere malen er op geattendeerd dat uw betaalpas per 1 juni 2016 komt te vervallen. Desondanks heeft u geen contact met ons opgenomen. — 3

De vervanging van uw betaalpas is verplicht. Normaal brengen wij 17,95 in rekening voor een nieuwe betaalpas. Indien u vandaag een nieuwe betaalpas aanvraagd via ons online formulier, zijn de kosten volledig gratis en ontvangt u uw nieuwe betaalpas met nieuwe verplichte functies. — 3, 4

Klik hier om u aan te melden. Vul het online formulier in op uw internetbankieren (https://www.abnanro.nl/pasvervang/inlog) — 5

Uw betaalpas bevat persoonsgebonden informatie. Daarom dient u eerst uw betaalpas op te sturen voor een milieuvriendelijke recycling voordat u een nieuwe betaalpas ontvangt. — 6

ABN AMRO Bank
Wecycle Inleverpunt
Postbus 83073
1080 AB Amsterdam

WAAR KUNT U OP LETTEN?

1. **Controleer de afzender**
   Kijk niet alleen naar de afzender, maar ook naar het precieze afzendadres. Is dit een vaag adres, of een afgeleide versie van de echte naam van uw bank?

2. **De e-mail is niet aan u persoonlijk gericht**
   Begint een e-mail met "geachte heer / mevrouw", of een andere algemene aanspreekvorm? Pas dan goed op want mogelijk is het een phishingmail.

3. **Dwingend karakter**
   De e-mail speelt in op uw gevoel en er wordt direct actie van u verwacht. U zou bijvoorbeeld al meerdere malen gewaarschuwd zijn over het verlopen van de betaalpas. Als u vandaag nog reageert dan hoeft u volgens de e-mail niet te betalen voor een nieuwe betaalpas.

4. **Er staan fouten in de e-mail**
   Denk hierbij aan taalfouten, stijlfouten of vreemde woorden.

5. **In de e-mail staat een link naar de inlogpagina van internetbankieren**
   Uw bank zet zulke links nooit in een e-mail. Wilt u inloggen en internetbankieren? Typ dan zelf het webadres van uw bank in, of log in via de app van uw bank.

6. **Verstuur nooit uw betaalpas**