

Tips ter voorkoming van Cybercrime

GEEF NOOIT JE PINCODE AAN IEMAND ANDERS.

Ook andere beveiligingscodes niet delen of je pincode ergens online invullen (anders dan de beveiligde Rabobank.nl-omgeving).

VERTROUW NIEMAND OP HET INTERNET.

Check de afzender van de e-mail, klik niet op de link in de e-mail maar login op uw bankrekening en bekijk of u daar een bericht heeft, bel desnoods het nummer van je bank.

WEES KRITISCH OP ALLE INFORMATIE DIE JE DEELT.

Alles wat je deelt op internet, blijft voor altijd vindbaar. Ook al lijkt het onschuldig, het kan nare gevolgen hebben.

GEBRUIK STERKE WACHTWOORDEN EN GEBRUIK VOOR ELK ACCOUNT EEN VERSCHILLENDE WACHTWOORD.

Schrijf ze niet op een blaadje maar gebruik een wachtwoordmanager app, hier kan je ook sterke wachtwoorden mee genereren!

Zet de twee-factor authenticatie aan voor jouw e-mail en al jouw social media accounts zodat niemand zich kan voordoen als jou. Deze feature kan je aanzetten voor bijna al jouw accounts en betekent dat je tijdens het inloggen op een tweede manier moet verifiëren dat het jouw account is!

Reageer nooit op berichten of telefoontjes van Rabobank waarin gevraagd wordt om in te loggen/je pas op te sturen/betalingen te doen et cetera. We zullen je dit nooit aan de telefoon, in een e-mail of via een SMS- of WhatsApp-bericht vragen.

Geef nooit gevolg aan een verzoek van 'de bank' om een overboeking te doen. Banken doen dergelijke verzoeken nooit.

Ga nooit direct mee in verzoeken van een 'bekende' die je snel vraagt om het doen van een betaling via WhatsApp, die je benadert met een 'nieuw telefoonnummer'. Controleer eerst of het wel echt die persoon is door bijvoorbeeld het nummer te bellen of face-to-face contact te zoeken.

Geef nooit je bankpas of codes af als er iemand namens 'de bank' langs de deur komt hiervoor.

Stuur nooit je bankpas op. Dit vraagt Rabobank nooit.

Nooit een kleurcode inscannen die je hebt ontvangen van iemand anders.

Bewaar je pincode nooit bij je bankpas.

Extra tips voor ondernemers

GEBRUIK ALLEEN BEVEILIGDE APPARATUUR EN OFFICIËLE SOFTWARE

ZORG VOOR EEN FIREWALL & ANTIVIRUS-SYSTEEM

Een firewall is een must voor iedere onderneming. Zo houdt u de meeste hackers, virussen, spyware en ransomware tegen.

VOER SOFTWARE-UPDATES DIRECT UIT

Een software-update is in feite een gratis bescherming tegen alle beveiligingsproblemen die tot dan toe bekend zijn. Voer software-updates daarom direct uit.

ZORG VOOR BEWUSTWORDING BIJ UW MEDEWERKERS

Bespreek cyberrisico's met uw medewerkers en spreek heldere spelregels af. Bijvoorbeeld over het gebruik van wachtwoorden:

- Zorg voor sterke wachtwoorden van minimaal 8 tekens, maar liever meer.
- Gebruik zoveel mogelijk verschillende tekens en symbolen.
- Wissel wachtwoorden regelmatig.

MAAK DAGELIJKS EEN BACK-UP

Maak dagelijks een back-up en sla die gegevens op in een veilige omgeving. Het liefst in een clouddienst én op een fysiek extern medium, koppel dit externe medium altijd los van de computer. Zo voorkomt u besmetting.

ZORG VOOR EEN NOODPLAN

Cybercriminelen zijn slim. En dus gaat het soms toch mis. Wees hierop voorbereid. Bedenk vooraf hoe u ervoor zorgt dat u uw gegevens terugkrijgt. En hoe u uw klanten weer kunt bedienen.

Kijk voor meer informatie op:

www.rabobank.nl/particulieren/veiligbankieren

www.rabobank.nl/bedrijven/veiligbankieren

www.cybernetwerkzhe.nl

