The Trusted Third Party

De 10 gouden regels voor cyberveiligheid

10 GOUDEN REGELS VOOR CYBERVEILIGHEID

<table>
<tr><td>  </td><td>1. Bescherm je accounts met sterke authenticatie

Gebruik steeds waar mogelijk multifactor-authenticatie (MFA)

• Lange wachtwoorden zijn efficiënter omdat ze voor cybercriminelen moeilijker te kraken zijn, gezien de vele mogelijkheden dat het aantal tekens biedt.
• Sterke wachtwoorden zijn minstens 14 tekens lang, zijn niet gemakkelijk te achterhalen en bevatten: hoofdletters, kleine letters, numerieke tekens, speciale tekens (&, $, %, !, =, +…)</td></tr>
<tr><td>  </td><td>2. Gebruik verschillende wachtwoorden voor professionele en persoonlijke accounts.</td></tr>
<tr><td>  </td><td>3. Sla al je gegevens op in een systeem waar regelmatig en centraal back-ups worden gemaakt.</td></tr>
<tr><td>  </td><td>4. Voer beveiligingsupdates uit op al je apparaten zodra ze beschikbaar zijn.</td></tr>
<tr><td>  </td><td>5. Laat nooit fysieke informatie (bijvoorbeeld papieren) of apparaten onbeheerd achter op je bureau.</td></tr>
<tr><td>  </td><td>6. Vermijd openbare Wi-Fi en gebruik het Virtual Private Network (VPN) van de organisatie.</td></tr>
<tr><td>  </td><td>7. Vermijd phishing door jezelf de volgende vragen te stellen:

• Is de verzender iemand die ik ken?
• Verwachtte ik een bericht over het vermeldde onderwerp?
• Vraagt het bericht om informatie zoals een gebruikersnaam, een wachtwoord of een bankrekeningnummer?
• Is het dringend?
• Waarheen leidt de link? (Ga er alleen met je muis over, niet klikken)
• Bevat het bericht een QR-code?
• Word ik persoonlijk aangesproken?
• Staan er taalfouten in het bericht?
• Zit het bericht in de map Spam / Junkmail?
• Probeert iemand mij nieuwsgierig te maken?
• Wordt er om een betaling gevraagd?

Hoe reageer je op een phishing e-mail?

• Antwoord er niet op, open geen enkele bijlage en klik niet op de links.
• Deel nooit bankgegevens waar via sms of e-mail om wordt gevraagd.
• Meld de poging tot phishing aan het meldpunt [de IT-afdeling/provider] en verwijder de e-mail/tekst.</td></tr>
</table>

	8. Neem de volgende maatregelen in acht bij de behandeling van interne of vertrouwelijke informatie: • Vergrendel je computer als je hem onbeheerd achterlaat. • Laat geen computers of papieren onbeheer achter op bureaus buiten de werkuren. • Laat geen papieren onbeheerd achter in printers. • Let altijd op je omgeving wanneer je vertrouwelijke informatie raadpleegt of bespreekt in openbare ruimtes. Probeer je waar mogelijk af te zonderen om te voorkomen dat iemand een gesprek afluistert.
	9. Gebruik alleen officiële websites en platforms om applicaties en software te downloaden. Het downloaden van software moet vermeden worden. Software wordt geïnstalleerd door de **IT-afdeling/provider**.
	10. Meld alle informatiebeveiligingsincidenten aan je IT-afdeling/provider Neem altijd contact op met het meldpunt **[de IT-afdeling/provider]** wanneer: • je vragen of opmerkingen hebt over dit document; • je iets opmerkt dat in strijd is met dit document; • er zich een vermoedelijk of bevestigd incident voordoet.

Blijf altijd op de hoogte

Op de hoogte blijven van het actuele nieuws rondom cybersecurity? Meld je dan aan voor onze nieuwsbrief of word lid van onze LinkedIn-pagina. Hier vind je regelmatig relevante artikelen, nieuws en praktische inzichten over cybersecurity.

Wat kun je verwachten?

- Actuele updates en nieuws
- Duiding van complexe wet- en regelgeving
- Interessante praktijk

Meld je aan en blijf altijd één stap voor