Check makkelijk en snel hoe jij cybercriminelen buiten houdt!

Vink aan waar je aan voldoet.
Op de achterkant van deze flap staat de toelichting.

**Alles aangevinkt?**
Goed bezig! Jij bent alert op online gevaar. Maar blijf goed opletten, een digitale misstap is nog altijd snel gemaakt.

**Mis je een vinkje?**
Je bent al goed bezig met je online veiligheid. Mogelijk is het interessant om eens stil te staan bij het gemiste vinkje. Op breda.nl/cyberambassadeurs vind je meer informatie en de gratis e-learning.

**Mis je meerdere vinkjes?**
Ga naar breda.nl/cyberambassadeurs of fraudehelpdesk.nl voor meer tips en adviezen. Of neem contact met ons op via het contactformulier op de website.

**Tenslotte... gebruik je gezond verstand!**
Als iets te mooi lijkt om waar te zijn, dan is het dat meestal ook. Wees online alert en sceptisch als je iets niet vertrouwt of kent.

**Cyber Ambassadeurs Breda**
Neem contact op via het contactformulier op de site: www.breda.nl/cyberambassadeurs
of via: cyberambassadeurs@breda.nl

# 10 TIPS TEGEN CYBERCRIME

## CHECK MAKKELIJK EN SNEL HOE JIJ CYBERCRIMINELEN BUITEN HOUDT!

CYBER AMBASSADEURS

GEMEENTE BREDA

| Stelling | Toelichting |
|---|---|
| **1 Installeer een antivirusprogramma** | Gebruik een antivirusprogramma om je apparaat te beschermen en schakel automatisch updates in. Laat het antivirusprogramma daarnaast geregeld je apparaat scannen op infecties. Schakel een eventueel meegeleverde firewall altijd in, zodat deze verbindingen tussen het apparaat en het internet in de gaten kan houden. |
| **2 Gebruik wachtwoord zinnen** | Het gebruik van lange wachtwoorden is belangrijk, vooral bij cruciale systemen zoals DigiD of jouw wifi netwerk. Gebruik bij voorkeur 12 tekens of meer, het aantal tekens bepaald namelijk hoe lastig het wachtwoord te kraken is. Gebruik daarnaast voor elke dienst een uniek wachtwoord, hiervoor kun je gebruik maken van een wachtwoordmanager die unieke wachtwoorden kan genereren en opslaan. |
| **3 Gebruik twee-staps-verificatie waar mogelijk** | Door het instellen van twee-staps-verificatie voeg je een tweede beveiliging toe aan je account. Deze tweede stap zorgt ervoor dat men niet met enkel het wachtwoord binnen kan komen in je account. Instellen van twee-staps-verificatie kan bij alle belangrijke accounts, zoals je mail of WhatsApp, via instellingen. |
| **4 Installeer altijd de software updates** | Producenten van besturingssystemen, browsers en andere programma's brengen geregeld updates uit om beveiligingslekken te verhelpen. Maak waar mogelijk gebruik van automatische updates. Controleer in andere gevallen minimaal maandelijks of updates beschikbaar zijn en installeer deze. Door techniek die up-to-date is verklein jij de kans dat je gehackt wordt, stel deze updates dus niet uit. |
| **5 Maak alleen verbinding met vertrouwde wifi-netwerken** | Bij openbare en onbeveiligde wifi netwerken kunnen andere meekijken. Verstuur dus geen gevoelige gegevens (e-mail of internetbankieren) over netwerken die je niet kent of gebruik een virtual private netwerk (VPN). |
| **6 Open geen berichten en onbekende bestanden die je niet verwacht of vertrouwt** | Ontvang je onverwacht een bericht met bijlagen, (ingekorte) link of verzoek om in te loggen? Dit wordt ook wel phising genoemd, waarbij criminelen hengelen naar jouw gegevens. Gebruik je gezond verstand en ga hier niet op in, zelfs niet wanneer je de afzender kent. Accepteer het bericht alleen als je zeker weet dat het echt is en je het verwacht te krijgen. |
| **7 Installeer alleen apps via officiële applicatiewinkels** | Ook apps voor je mobiele telefoon of tablet kunnen malware bevatten. Installeer apps daarom alleen via de officiële applicatiewinkels en gebruik geen illegale kopieën. Kijk ook goed naar de toegangsrechten van de app. Bekijk ervaringen van medegebruikers om een beeld te vormen van de betrouwbaarheid van de app. |
| **8 Controleer het adres van websites** | Controleer het webadres (URL) in de bovenste balk van je browser om vast te stellen dat je geen nagemaakte website bezoekt. Ken je de website nog niet? Controleer via zoekmachines wat er te vinden is over de site. Vertrouw je het niet volledig? Vul dan geen (gevoelige) gegevens in op deze website. |
| **9 Ongevraagd helpdesk advies: verbreek de verbinding** | Oplichters die zich voordoen als medewerkers van bedrijven zoals Microsoft of je bank proberen je wijs te maken dat je een probleem hebt, maar dat daar tegen een vergoeding iets aan te doen is. Vervolgens vraagt de oplichter om hem mee te laten kijken in je computer. Krijg je zo'n telefoontje, ga dan niet met deze mensen in gesprek. |
| **10 Maak regelmatig back-ups** | Door regelmatig back-ups te maken van je computer en van je bestanden of foto's op je telefoon of tablet, kun je schade van bijvoorbeeld gijzelsoftware of virussen beperken. Indien je een back-up hebt liggen, kun je toch nog bij een kopie van je gegevens. Back-ups maak je op een externe, losgekoppelde harde schijf die je op een andere locatie bewaart. Ook kun je gebruik maken van een online-opslagdienst. |