

Beveilig mobiele toestellen

Een goede beveiliging van smartphone, tablet en laptop is nodig om cybercriminelen of andere indringers buiten te houden. Als een toestel in verkeerde handen terecht komt, kan dat veel schade berokkenen. Deze tips helpen je op weg.

Toegang en applicaties

- Gebruik enkel veilige applicaties en programma's. Installeer alleen applicaties uit een officiële app store (Google Play, App Store) of van een officiële verkoper (bv. LG, Samsung, SONY, Amazon, enz.). Installeer nooit een app van een bron die je niet kent. Google en Apple doen veel moeite om ervoor te zorgen dat de apps die zij aanbieden geen malware bevatten. Zelfs als iemand erin slaagt een kwaadaardige applicatie in een van deze winkels aan te bieden, zullen Google of Apple dit snel ontdekken en hun fout herstellen. Het probleem met andere aanbieders is dat ze niet dezelfde veiligheidsgarantie bieden.
- Beperk de toegang van je applicaties tot het strikt noodzakelijke. Een rekenmachine-app heeft bv. geen toegang nodig tot je locatie of contacten.
- Activeer de toegang van wifi, Bluetooth, Near Field Communication (NFC), data, geolocatie etc. alleen als je ze nodig hebt. Kies niet voor automatische activeringsfuncties (bv. voor wifi).
- Verwijder regelmatig applicaties die je niet gebruikt en controleer regelmatig de gegevens die door je applicaties worden gebruikt om ongepast verkeer op te sporen.

Hou je toestellen in goede gezondheid

- Activeer het automatisch updaten van hardware en software. Dit zorgt ervoor dat zodra er een kwetsbaarheid wordt gedetecteerd, je toestel beter beschermd is.
- Sluit je toestellen dagelijks af. Bij het opstarten worden updates immers meestal automatisch uitgevoerd.
- Gebruik een [virusscanner](#).

Beveilig je toestellen met een sterk wachtwoord of code

- Kies een goede pincode voor je simkaart. Als je een nieuwe simkaart ontvangt, kies je een geschikte pincode die niet direct aan jou gelinkt is. Pincodes zoals: 0000, 1111 of 1234 zijn te vermijden, net zoals je geboortedatum of de PIN-code van je eID of bankkaart.
- Kies een wachtwoord of cijfercode en geen patroon. Een patroon blijft soms zichtbaar op het scherm.
- Activeer de automatische vergrendeling van je smartphone of tablet wanneer deze inactief is (maximaal 1 minuut).
- Indien mogelijk, stel dan een tijdslot na een aantal mislukte pogingen op je smartphone of tablet in en stel het automatisch wissen van gegevens na te veel toegangspogingen in. Zorg uiteraard wel dat goede back-ups voorhanden zijn.

Behoud de controle

- Laat je toestellen niet onbeheerd achter.
- Zorg dat anderen geen toegang hebben tot je toestellen.
- Hou je toegangscode en wachtwoorden geheim.
- Gevoelige gesprekken voer je in een privéruimte of goed beveiligde zone