

Digitale beveiligingschecklist

Voor eindgebruikers en thuiswerkers

Loop de zes categorieën na en vink een punt pas af wanneer je de instelling hebt gecontroleerd of de actie hebt uitgevoerd. Kies bij twijfel de veilige standaard of vraag je organisatie om hulp. Per categorie staan zes punten; samen zijn dat exact 36 actiepunten.

-
- | | | | |
|-----------|--|-----------|--|
| 01 | Zo gebruik je de checklist | 02 | 1. Wachtwoorden & Authenticatie — 6 punten |
| 03 | 2. Software & Patchbeheer — 6 punten | 04 | 3. Back-ups & Herstel — 6 punten |
| 05 | 4. Netwerk & Draadloze Verbindingen — 6 punten | 06 | 5. Phishing- & Social-Engineeringherkenning — 6 punten |
| 07 | 6. Apparaat- & Endpointbeveiliging — 6 punten | 08 | Telling en afronding |

Zo gebruik je de checklist

Deze checklist helpt je de digitale beveiliging van je eigen accounts, apparaten en thuiswerkplek praktisch na te lopen. Jij voert de controles uit; de gebruiker van het apparaat of account bevestigt wat al is geregeld. Pas zakelijke instellingen niet zelfstandig aan als je organisatie daarvoor een beheerprocedure heeft.

- Vink een punt af nadat je het hebt gecontroleerd of uitgevoerd.
- Essentieel = basismaatregel om direct na te lopen; Aanbevolen = nuttige versterking; Geavanceerd = extra maatregel wanneer die beschikbaar en passend is.
- Elk onderdeel telt één keer mee. De nummering loopt door van 1 tot en met 36.

Veilig uitvoeren

Gebruik officiële instellingen en bekende contactkanalen. Deel nooit wachtwoorden, herstelcodes of eenmalige verificatiecodes met iemand die erom vraagt.

☒ 1. Wachtwoorden & Authenticatie — 6 punten

Bescherm accounts met unieke aanmeldgegevens en een tweede verificatiestap waar mogelijk. Een wachtwoordmanager bewaart wachtwoorden versleuteld en kan helpen sterke, unieke wachtwoorden te gebruiken.

- ☐ 1. Essentieel — Gebruik voor ieder belangrijk account een uniek wachtwoord. Hergebruik maakt het risico groter wanneer een andere dienst wordt getroffen.
- ☐ 2. Aanbevolen — Bewaar wachtwoorden in een betrouwbare wachtwoordmanager in plaats van in een onbeveiligde notitie of spreadsheet.
- ☐ 3. Essentieel — Beveilig je e-mailaccount, wachtwoordmanager en andere belangrijke accounts met MFA (meervoudige verificatie), als de dienst dit aanbiedt.
- ☐ 4. Aanbevolen — Kies bij MFA bij voorkeur een passkey of verificatie-app wanneer beschikbaar; sms-codes kunnen een alternatief zijn, maar zijn niet voor elke situatie de sterkste optie.
- ☐ 5. Essentieel — Deel nooit je wachtwoord, herstelcode of eenmalige verificatiecode, ook niet met iemand die zich voordoeft als medewerker van een dienst.
- ☐ 6. Geavanceerd — Bewaar herstelcodes van MFA op een veilige plek die niet afhankelijk is van hetzelfde apparaat of account.

Best practice

Een passkey gebruikt cryptografische sleutels in plaats van een gedeeld geheim dat je intypt. Gebruik deze optie als zowel de dienst als je apparaat haar ondersteunen; beschikbaarheid verschilt per dienst.



2. Software & Patchbeheer — 6 punten

Beveiligingsupdates verhelpen bekende kwetsbaarheden. Schakel automatische updates in waar dat kan en controleer ook apparaten die je minder vaak gebruikt, zoals routers en printers.

- ☐ 7. Essentieel — Schakel automatische beveiligingsupdates voor het besturingssysteem in, als die optie beschikbaar is.
- ☐ 8. Essentieel — Installeer aangeboden beveiligingsupdates voor telefoon, tablet en computer tijdig; stel ze niet steeds uit zonder reden.
- ☐ 9. Aanbevolen — Schakel automatische updates voor je browser in en verwijder browsers die je niet meer gebruikt.
- ☐ 10. Aanbevolen — Controleer via de officiële instellingen of leverancier of er firmware-updates zijn voor router en andere netwerkapparatuur.
- ☐ 11. Aanbevolen — Werk veelgebruikte apps bij via de officiële appwinkel of website van de leverancier; vermijd installatiebestanden uit onbekende bronnen.
- ☐ 12. Geavanceerd — Verwijder software en browseruitbreidingen die je niet meer nodig hebt, zodat je minder ongebruikte onderdelen hoeft te onderhouden.

Best practice

Controleer bij een update dat je in de instellingen van het apparaat of op de officiële website van de leverancier bent. Klik niet op onverwachte update-links in berichten.

☒ 3. Back-ups & Herstel — 6 punten

Een back-up is een aparte kopie waarmee je gegevens kunt terugzetten na verlies, schade of een incident. Synchronisatie alleen is geen betrouwbare vervanging: verwijderingen of wijzigingen kunnen ook worden gesynchroniseerd.

- ☐ 13. Essentieel — Maak back-ups van belangrijke bestanden, zoals documenten, foto's en werkbestanden.
- ☐ 14. Aanbevolen — Gebruik de 3-2-1-regel als richtlijn: drie kopieën van gegevens, op twee soorten opslagmedia, met één kopie buiten de primaire locatie.
- ☐ 15. Essentieel — Houd ten minste één back-up gescheiden van het apparaat dat je dagelijks gebruikt; een offline of anderszins afgeschermd kopie kan helpen tegen verspreiding van schade.
- ☐ 16. Aanbevolen — Beperk toegang tot back-ups en gebruik versleuteling waar die beschikbaar is, vooral voor draagbare opslag en cloudback-ups.
- ☐ 17. Essentieel — Controleer of back-ups daadwerkelijk worden voltooid en kijk of de verwachte bestanden aanwezig zijn.
- ☐ 18. Aanbevolen — Test periodiek het terugzetten van een onbelangrijk testbestand, zodat je weet hoe herstel werkt voordat je het nodig hebt.

Best practice

Bewaar een kopie op een andere locatie dan je primaire apparaat. Een tweede map die alleen synchroniseert met hetzelfde account is niet automatisch een onafhankelijke back-up.



4. Netwerk & Draadloze Verbindingen — 6 punten

Beveilig je wifi via de routerinstellingen. Routernamen en menu's verschillen per model; volg de documentatie van de leverancier of de beheerprocedure van je organisatie.

- ☐ 19. Essentieel — Gebruik WPA3 voor wifi als router en apparaten dit ondersteunen; anders kies je WPA2 met AES, indien beschikbaar.
- ☐ 20. Aanbevolen — Gebruik WPA2-Enterprise alleen op een netwerk dat door je organisatie wordt beheerd en waarvoor je geldige organisatie-inloggegevens hebt.
- ☐ 21. Essentieel — Vervang het standaardbeheerderswachtwoord van de router door een uniek wachtwoord en bewaar dit veilig.
- ☐ 22. Aanbevolen — Installeer routerfirmware-updates via de officiële beheerinterface of instructies van de leverancier.
- ☐ 23. Aanbevolen — Gebruik een gastnetwerk voor bezoekers of slimme apparaten wanneer je router dit ondersteunt; deel niet je hoofdnetworkwachtwoord als dat niet nodig is.
- ☐ 24. Geavanceerd — Gebruik op een openbaar of anderszins onbetrouwbaar netwerk een VPN van een betrouwbare aanbieder of je organisatie als dat passend is; blijf ook dan updates en veilige aanmeldgewoonten gebruiken.

Goed om te weten

Een VPN versleutelt verkeer tussen je apparaat en de VPN-dienst, maar maakt een onbetrouwbare website niet veilig en vervangt geen updates, MFA of zorgvuldig klikgedrag.

5. Phishing- & Social-Engineeringherkenning — 6 punten

Phishing probeert je te verleiden gegevens te delen, geld over te maken of schadelijke inhoud te openen. Het kan binnenkomen via e-mail, berichtenapps, telefoongesprekken of andere kanalen.

- ☐ 25. Essentieel — Controleer bij een link het volledige domein en de spelling; vertrouw niet alleen op de zichtbare linktekst of de naam van de afzender.
- ☐ 26. Essentieel — Ga bij een onverwacht verzoek om in te loggen zelf naar de bekende website of app, in plaats van via de meegestuurde link.
- ☐ 27. Essentieel — Open onverwachte bijlagen niet voordat je de afzender en de reden van verzending via een bekend kanaal hebt gecontroleerd.
- ☐ 28. Aanbevolen — Wees extra alert op onverwachte urgentie, verzoeken om geheimhouding, betaalverzoeken en vragen naar wachtwoorden of verificatiecodes.
- ☐ 29. Geavanceerd — Bekijk bij twijfel de volledige berichtgegevens of e-mailheaders als je weet hoe je die veilig interpreteert; headers kunnen informatie over afzender en doorgifte tonen, maar bewijzen op zichzelf niet dat een bericht legitiem is.
- ☐ 30. Essentieel — Meld verdachte berichten via het afgesproken meldkanaal van je organisatie of de betreffende dienst; verwijder of rapporteer ze volgens die procedure.

Voorbeeld

Een bericht zegt dat je account binnen enkele minuten wordt geblokkeerd en vraagt om je code. Klik niet en deel de code niet. Open zelf de bekende app of website en meld het bericht via het officiële kanaal.

☒ 6. Apparaat- & Endpointbeveiliging — 6 punten

Een endpoint is een apparaat dat toegang heeft tot accounts of netwerken, zoals een laptop, telefoon of tablet. Beperk de schade bij verlies of onbevoegde toegang door vergrendeling, versleuteling en zorgvuldig fysiek gebruik.

- ☐ 31. Essentieel — Stel een sterk ontgrendelmechanisme in, zoals een lange toegangscode of een passend wachtwoord; vermijd voorspelbare codes.
- ☐ 32. Essentieel — Schakel automatische schermvergrendeling in en vergrendel je scherm wanneer je wegloopt.
- ☐ 33. Aanbevolen — Controleer of volledige-schijfversleuteling is ingeschakeld: BitLocker is beschikbaar op ondersteunde Windows-edities en FileVault op macOS.
- ☐ 34. Aanbevolen — Bewaar herstelinformatie voor schijfversleuteling veilig en apart van het apparaat; verlies van die informatie kan toegang tot gegevens bemoeilijken.
- ☐ 35. Essentieel — Laat een laptop of telefoon niet onbeheerd achter op een openbare plek; neem het apparaat mee of berg het veilig op.
- ☐ 36. Geavanceerd — Controleer of de functies voor apparaatlocatie en wissen op afstand zijn ingesteld en begrijp hoe je ze via de officiële accountinstellingen gebruikt.

Let op

Beschikbaarheid en beheer van BitLocker verschillen per Windows-editie en organisatie-instelling. Controleer de officiële instellingen of vraag je IT-beheerder voordat je wijzigingen aanbrengt.

Telling en afronding

Gebruik de telling om te controleren of alle onderdelen zijn nagegaan. Een vakje blijft leeg als je de instelling niet hebt gecontroleerd, de functie niet beschikbaar is of je nog hulp nodig hebt.

- Wachtwoorden & Authenticatie: 6 punten (1–6).
- Software & Patchbeheer: 6 punten (7–12).
- Back-ups & Herstel: 6 punten (13–18).
- Netwerk & Draadloze Verbindingen: 6 punten (19–24).
- Phishing- & Social-Engineeringherkenning: 6 punten (25–30).
- Apparaat- & Endpointbeveiliging: 6 punten (31–36).
- Totaal: exact 36 genummerde actiepunten in 6 categorieën.

Vervolg

Noteer voor jezelf welk punt nog openstaat en controleer het later via de juiste instellingen of met hulp van je organisatie. Deel geen gevoelige gegevens in notities bij deze checklist.