Checklist

Hieronder vind je algemene privacy-tips welke je gemakkelijk in je dagelijkse leven kunt toepassen. Deze privacy tips bespreken we ook uitgebreid in de Pro Privacy Podcast. We verwijzen met regelmaat naar handleidingen op ons Pro Privacy Platform. Heb je bij ons een Pro Privacy Phone of een Pro Privacy Laptop gekocht? Dan heb je onbeperkt toegang tot deze handleidingen.

Huishouden

❒ **Zorg voor zo min mogelijk SMART-apparatuur**. Sommige apparaten (zoals TV's) zijn enkel nog in SMART-variant te verkrijgen. Zorg er in dat geval voor dat je ze niet (of zo min mogelijk) verbindt met je netwerk.

❒ **Vermijd de 'slimme' meter waar mogelijk.** Deze meter weet exact welk apparaat op welk moment ingeschakeld staat. Dit kan veel over een mensenleven vertellen. Op basis van deze data kan in de toekomst mogelijk gestuurd gaan worden op je gedrag (nudging). De beste optie is een 'domme' digitale meter. Dit is een digitale meter zonder zendmodule. Heb je een digitale meter met zendmodule? Zorg dan dat je de zendmodule laat verwijderen. Kan dit niet? Zorg dan dat je het uitlezen op afstand uit laat schakelen bij je netbeheerder.
Dit kan bijvoorbeeld hier bij netbeheerder Stedin:
https://www.stedin.net/slimme-meter/slimme-meter-uitlezen

❒ Is de 'domme' digitale meter geen optie en heb je al een slimme meter? **Zorg er dan minstens voor dat je de het uitlezen op afstand uit laat schakelen** bij je netbeheerder (zie hierboven).

❒ **Neem een internetverbinding van een provider die je digitale privacy en veiligheid respecteert.** Een goed voorbeeld hiervan is freedom.nl. Hier hebben wij verder geen samenwerking mee.

Berichten-apps

❒ **Gebruik zoveel mogelijk open source end-to-end-encrypted (versleutelde) berichtenapps zoals Signal en Session, ook als het grootste deel van je familie en vrienden dit niet doet.** Het begint bij jezelf. Ook als je maar met 1 iemand communiceert via deze apps, ben je al goed bezig. Zowel Signal als Session hebben zeer uitgebreide handleidingen op ons Pro Privacy Platform.

❒ **Mocht je Signal gebruiken, stel dan een gebruikersnaam in en verberg je telefoonnummer.** Door dit te doen, kunnen mensen je niet meer vinden in Signal door te zoeken naar je telefoonnummer. In plaats daarvan moeten ze je gebruikersnaam kennen. Mocht je het dan toch niet vertrouwen, wijzig dan (na het doorgeven) direct je gebruikersnaam. Geen last meer dus van Arabische prinsen of mooie vrouwen die geld nodig hebben voor de operatie van oma. Onze klanten vinden een zeer uitgebreide Signal-handleiding op ons Pro Privacy Platform.

❒ **Schakel indien mogelijk Verdwijnende Berichten in bij je huidige berichten apps.** Verdwijnende Berichten is een functie waarbij berichten na een bepaalde tijd automatisch worden verwijderd. Wij raden dit aan, omdat je gespreksgeschiedenis een belangrijke informatiebron is met allerlei gegevens die je door de jaren heen hebt gedeeld met anderen.

❒ **Verhuis je gespreksgeschiedenis NOOIT mee naar een nieuwe telefoon.** Het is goed om met een schone lei te beginnen. Mocht je toch de gespreksgeschiedenis willen bewaren, sla de gesprekken dan op op je PC. Dit proces verschilt per app.

E-mail

❒ **Schakel over naar alternatieve encrypted (versleutelde) e-maildiensten als Tuta Mail en Proton Mail.** Zowel Tuta Mail als Proton Mail hebben zeer uitgebreide handleidingen op ons Pro Privacy Platform.

❒ **Deel je persoonlijke e-mailadres zo min mogelijk**. Maak in plaats daarvan gebruik van een e-mailaliasdienst als addy.io. Addy.io heeft een zeer uitgebreide handleiding op ons Pro Privacy Platform.

❒ **Gebruik je e-mail zo min mogelijk voor persoonlijke communicatie.** Gebruik in plaats daarvan een berichten app als Signal en/of Session.

❒ **Stel NOOIT een Forward in van bijvoorbeeld je Gmail naar Tuta Mail.** Een Forward zorgt ervoor dat e-mailberichten naar een e-mailadres worden doorgestuurd naar een ander e-mailadres.

❒ **Maak ALTIJD een back-up e-mailadres voor Tuta Mail en/of Proton Mail.**

❒ **Stel een herstel e-mailadres in.** De meeste e-maildiensten stellen je in staat om een zogenaamd Herstel e-mailadres toe te voegen aan je e-mailaccount. Dit herstel e-mailadres wordt in de meeste gevallen gebruikt om het wachtwoord te wijzigen. Wij adviseren niet alleen om gebruik te maken van deze functie, maar ook om exclusief gebruik te maken van een e-mailadres van Tuta Mail en/of Proton Mail als Herstel e-mailadres. Koppel dus NIET je Gmail aan je Tuta Mail.

❒ Mocht een e-maildienst het aanbieden, **gebruik dan ALTIJD een wachtwoord bij het versturen van een e-mail naar iemand die je goed kent**. Tuta Mail en Proton Mail bieden beide deze functie aan. Wij adviseren om dit vooral te gebruiken wanneer je met deze 2 diensten een e-mail stuurt naar een andere e-maildienst zoals Gmail, Hotmail, Live, Outlook, Yahoo en alle andere diensten.

Bellen en SMSen

❒ **Vul NOOIT meer in dan nodig is bij het toevoegen van een contact aan je telefoon.** De voornaam van de desbetreffende persoon en het telefoonnummer zijn voldoende. Mocht je meerdere contacten hebben met dezelfde voornaam/achternaam, gebruik dan initialen of andere gegevens waaraan jij je contacten kunt herkennen. Vraag aan je familie en vrienden of ze dit ook bij jou contactinformatie willen doen.

❒ **Bij het geven van je contactinformatie aan iemand geef je alleen de basisinformatie door.**

❒ **Sla NOOIT je contacten op in de cloud**, bijvoorbeeld door het synchroniseren met iCloud.

❒ **Klik NOOIT op links die in sms'jes worden getoond** als je hier niet om hebt gevraagd. Voorbeelden hiervan zijn het bekijken van een bestelstatus en het betalen van facturen.

❒ **Neem een nieuw telefoonnummer bij het aanschaffen van een nieuwe telefoon.**

❒ **Maak géén gebruik van een simkaart indien mogelijk.** Het is mogelijk om anonieme mobiele data te verkrijgen met een eSIM (zie onze Anonieme eSIM-handleiding op het Pro Privacy Platform). Bellen doe je dan standaard via een end-to-end-encrypted-berichten-app als Signal of Session. Dit is ook nog eens vele malen beter voor je privacy. In GrapheneOS is het mogelijk om handmatig je simkaart uit te schakelen. Deze kan je dan zo nu en dan inschakelen wanneer je hem echt nodig hebt.

❒ **Maak indien mogelijk ALLEEN gebruik van prepaid simkaarten** als je afhankelijk bent van een simkaart.

❒ **Bekijk alle contacten die je in je telefoon hebt staan en verwijder contacten waar je niet mee communiceert** en eventuele dubbele contacten.

❒ **Stel ALTIJD een pincode in voor je simkaart.** Vraag na bij je telecomprovider hoe je dit kunt doen. Ga indien mogelijk voor een eSIM, deze is niet fysiek te verwijderen.

❒ **Verwijder sms'jes die je niet meer nodig hebt**, bijvoorbeeld voor het inloggen op een website/dienst.

❒ **Neem ALLEEN telefoontjes aan waarbij het telefoonnummer zichtbaar is**, tenzij je een telefoontje verwacht van bijvoorbeeld het ziekenhuis. Mocht een instantie aangeven dat ze je gaan bellen, vraag dan altijd voor de zekerheid of dat met een privénummer wordt gedaan, zodat je hier rekening mee kunt houden.

❒ **Schakel de simkaart UIT als je deze even niet wilt gebruiken**. Eigenaren van een Pro Privacy Phone kunnen dit doen binnen GrapheneOS.

❒ **Spreek af met je familie en vrienden dat ze ALLEEN je contactinformatie aan iemand door mogen geven met jouw toestemming.**

Financiele zaken

❒ **Betaal waar mogelijk altijd contant.**

❒ **Mocht contant betalen niet mogelijk zijn, koop dan cadeaubonnen met contant geld** (of privacycrypto). Zo kan je alsnog privacyvriendelijk winkelen. Webwinkels als Bol.com geven je ook de mogelijkheid om met cadeaubonnen te betalen, maar ook om ze op te waarderen. Hierdoor kun je tegoed toevoegen aan je Bol.com, waarna je de cadeaubonnen kunt weggooien.

❒ **Maak géén gebruik van iDeal/Wero-profielen**. Gewoon lekker (ouderwets) de velden blijven invullen. We hebben het gevaar van iDeal/Wero-profielen uitgebreid besproken in Pro Privacy Podcast #03.

❒ **Gebruik NOOIT apps of bonuskaarten om ergens korting op te krijgen.** Bij de Albert Heijn kun je om de bonuskaart van de medewerker vragen. Bij de Lidl kan je vragen of de kassamedewerker zijn/haar telefoonnummer in wil voeren in het systeem.

❒ **Vermijd supermarkten waar geen kassa's meer staan met een (echt) persoon.**

❒ **Als je in een supermarkt bent waar slechts een enkele echte kassa staat, gebruik deze dan.** Ook als er een lange rij staat! Laat de locatie-eigenaar zien dat kassa's met echte mensen nodig zijn. Het is niet zielig voor de kassamedewerker. Sterker nog, de medewerker kan op die manier makkelijker zijn/haar baan blijven behouden.

❒ **Betaal in een winkel NOOIT met je telefoon, maar in plaats daarvan contant.** Als dat niet kan, betaal dan met de pinpas. Bij betaling via je telefoon komt je data direct bij Big Tech terecht. We hebben dit uitgebreid besproken in Pro Privacy Podcast #10.

❒ **Betaal NOOIT contactloos met je pinpas.** Lekker (ouderwets) de pinpas in het pinapparaat doen en de code invullen. Scherm dit natuurlijk goed af.

❒ **Maak ALLEEN gebruik van bank-apps op GrapheneOS.** Het liefst in een apart gebruikersprofiel. Dit is het meest veilige en privacyvriendelijke mobiele besturingssysteem van dit moment, dat we installeren op de Pro Privacy Phone.

❒ **Gebruik GEEN Tikkie bij digitale betalingen.** Stuur alleen directe betaalverzoeken met de bank-app die je gebruikt. Hiermee zorg je ervoor dat er geen gebruik wordt gemaakt van nog een derde partij.

❒ B**ekijk financiële zaken NOOIT in het openbaar.** Voorbeeld: bank-apps en crypto wallets NOOIT openen als je je in een publieke ruimte bevindt.

❒ **Mocht je gebruikmaken van betaalpasjes, houd deze dan ALTIJD in een pashouder welke straling blokkeert.** Op deze manier kunnen kwaadwillenden je pasjes niet scannen. Houd er dan wel rekening mee dat je de pasjes uit de houder moet halen om ze te kunnen gebruiken.

❒ **Gebruik privacycrypto bij online webwinkels waar dit direct geaccepteerd word**t (zie ook onze Pro Privacy Crypto Cursus).

❒ **Koop cadeaubonnen met privacycrypto** en geef deze uit in online webwinkels waar betalen met privacycrypto niet mogelijk is (zie ook onze Pro Privacy Crypto Cursus).

❒ **Gebruik ALLEEN pinautomaten die in een binnenruimte staan.** Mocht dit niet mogelijk zijn, scherm het geld dat je uit een pinautomaat haalt dan goed af.

❒ **Laat een bestelling indien mogelijk NOOIT afleveren op je huisadres.** Gebruik in plaats daarvan een PostNL- of ander soort afhaalpunt waar je het pakketje kunt ophalen.

❒ **Vermijd 'buy now, pay later'-diensten:** Diensten als Klarna, AfterPay of in3 verzamelen extreem gedetailleerde data over je koopgedrag en financiële situatie. Betaal liever direct of met een cadeaubon om deze surveillance-economie te omzeilen.

Veilig internetten

❒ **Gebruik ALTIJD een goede privacy-vriendelijke VPN-dienst** waarbij je géén account hoeft aan te maken. Onze favoriete VPN-diensten zijn Mullvad VPN en NymVPN. Zowel Mullvad VPN als NymVPN hebben een uitgebreide handleiding op ons Pro Privacy Platform.

❒ **Maak NOOIT gebruik van publieke WiFi-netwerken**. Mocht dit onvermijdelijk zijn, gebruik dan ALTIJD een goede VPN, bijvoorbeeld Mullvad VPN of NymVPN.

❒ **Heb je je wachtwoorden ergens genoteerd staan, sla dit dan op in een betrouwbare wachtwoordmanager als Bitwarden of KeePass en verbrand je notities.** Goede, veilige wachtwoordmanagers bieden je naast extra veiligheid ook

een hoop extra gemak. Het ene hoeft het andere niet in de weg te zitten. Onze klanten vinden een zeer uitgebreide Bitwarden-handleiding op ons Pro Privacy Platform.

❒ **Sla inloggegevens NOOIT op in een internetbrowser**, als daar naar wordt gevraagd.

❒ **Gebruik NOOIT dezelfde gebruikersnamen, e-mailadressen en wachtwoorden voor verschillende accounts.** Gebruik in plaats daarvan een Generator waarmee je willekeurige gegevens kunt genereren. Onder andere Bitwarden heeft een Generator die je hiervoor kunt gebruiken.

❒ **Als een website vraagt om cookies te accepteren, controleer dan ALTIJD of er een optie is om alléén essentiële cookies te gebruiken.**

❒ **Log ALTIJD uit bij het afsluiten van een website.**

❒ **Wis REGELMATIG je browsergeschiedenis van je internetbrowser.** Dit proces verschilt per browser.

❒ **Als een website je vraagt om persoonlijke gegevens op te slaan zodat je de volgende keer makkelijk een aankoop kunt doen, weiger dit dan ALTIJD.** Je kunt deze gegevens ook door bijvoorbeeld Bitwarden voor je laten invullen.

❒ **Als je je internetbrowser gebruikt voor meerdere doelen, bijvoorbeeld: privé en werk, maak dan gebruik van Browserprofielen.** Hiermee kun je je bezigheden van elkaar scheiden. Brave en Mullvad Browser ondersteunen onder andere deze functie.

❒ **Gebruik ALTIJD private-by-default-browsers die je standaard beschermen tegen cookies, trackers en fingerprinting.** Voor laptops zijn dat Brave Browser en Mullvad Browser. Voor GrapheneOS-telefoons en tablets zijn dat Vanadium en de Brave Browser. Zowel de Brave Browser, de Mullvad Browser als de Vanadium browser hebben uitgebreide handleidingen op ons Pro Privacy Platform.

❒ **Sla je meest gevoelige gegevens (zoals bijvoorbeeld foto's) niet op op de harde schijf van je PC/Mac.** Schaf in plaats daarvan een externe harde schijf/USB-stick aan en beveilig deze met sterke encryptie. Klanten met een Pro Privacy Laptop (of die gebruikgemaakt hebben van onze ombouwservice) vinden een uitgebreide VeraCrypt-handleiding op ons Pro Privacy Platform. Bewaar de harde schijf/USB-stick vervolgens op een plek waarvan alleen jij weet waar deze ligt.

❒ **Gebruik NOOIT de zoekmachine Google.** Gebruik in plaats daarvan Brave Search, of bijvoorbeeld SearX.

❒ **Probeer je YouTube gebruik te verminderen** en schakel over op een meer censuurresistentie en meer privacyvriendelijke optie als Odysee. Installeer de Watch On Odysee addon in je browser om te zien welke content-creators al op Odysee zitten.

❒ **Gebruik NOOIT meer WeTransfer, SendSpace of andere niet-privacyvriendelijke diensten waarmee je bestanden kunt sturen.** Gebruik in plaats daarvan een website als Wormhole.app of send.internxt.com, waarmee je dit wél op een privacyvriendelijke manier kunt doen. Onze klanten vinden een zeer uitgebreide Wormhole.app-handleiding op ons Pro Privacy Platform.

❒ **Klik NOOIT op links in verdacht uitziende e-mails.** Voorbeelden hiervan zijn het klikken op betaalverzoeken van een bank, een controle van gegevens door een bank, het klikken op een link zonder context, etc.

❒ **Let bij het delen van documenten, foto's en schermafbeeldingen op persoonlijke gegevens die hier mogelijk in kunnen staan.**

❒ **Verwijder accounts die je niet meer gebruikt**, zowel van een website als voor een app.

❒ **Deel je accountgegevens alleen met mensen die je ECHT vertrouwt.**

❒ **Print alleen iets wanneer je printer direct is aangesloten op het apparaat waarmee je iets wilt uitprinten.** Zo blijft alles lokaal.

❒ **Wijzig je WiFi-wachtwoord**, als je dit nog nooit gedaan hebt.

❒ **Deel je WiFi-wachtwoord NOOIT digitaal met iemand.**

❒ **Maak gebruik van apps die GEEN metadata opslaan van je foto's.** Metadata bestaat uit data waarmee de locatie van de foto kan worden bepaald, de tijd waarop de foto is gemaakt en andere gevoelige gegevens. Gebruik dit uiteraard NIET om te frauderen bij je verzekering of andere instanties.

❒ **Deel je locatie NOOIT via de app**, tenzij het een noodgeval betreft.

❒ **Deel ALLEEN je scherm met mensen die je vertrouwt.**

Openbare communicatie

❒ **Gebruik NOOIT Zoom, Google Meet en Microsoft Teams** om online vergaderingen mee te voeren. Gebruik in plaats daarvan Signal, Session, Brave Talk of Nextcloud Talk.

❒ **Voer NOOIT persoonlijke gesprekken in het openbaar.** Mensen luisteren (bewust of onbewust) mee en anders luistert hun telefoon mee of andere afluisterapparatuur.

❒ **Alleen familie en vrienden mogen je contactgegevens aan iemand anders doorgeven met jouw toestemming.**

❒ **Gebruik NOOIT smartspeakers als Google Nest.** Het apparaat moet kunnen horen dat je 'Hey Google' zegt om opdrachten uit te kunnen voeren.

❒ **Wees bewust van je afval:** Vernietig fysieke documenten met persoonlijke gegevens (bankafschriften, medische rapporten, oude contracten) met een papierversnipperaar voordat je ze weggooit. Dit voorkomt 'dumpster diving'.

Apps

❒ **Gebruik NOOIT de DigiD-app om in te loggen op een website**. Gebruik in plaats daarvan de sms-controlefunctie waarmee je aan de hand van een smsje kan inloggen met je DigiD. Dit kun je instellen op www.digid.nl.

❒ **Beveilig indien mogelijk apps ALTIJD met een pincode.**

❒ **Vermijd zoveel mogelijk Big Tech-applicaties** van de Big Six: Amazon, Facebook, Apple, Microsoft, Google en Twitter/X.

❒ **Probeer niet te afhankelijk te worden van 1 dienst.** Daarmee bedoelen we dat je niet per se alle apps van een dienst hoeft te gebruiken. Voorbeeld: Proton biedt de apps Proton Mail, Proton Drive, Proton Pass, Proton Calendar, Proton Pass en Proton VPN aan. Als de Proton-dienst uitvalt of wordt gehackt, kan het invloed hebben op alle diensten.

❒ **Bekijk ALLE apps op je telefoon en ga na of je ze allemaal gebruikt.** Zo ja, hoe vaak gebruik je ze? Heb je ze echt nodig? Is er een webversie van de app(s)? Zijn er alternatieven? Voorbeeld: de IKEA-app geeft je gratis koffie bij het bezoeken van een filiaal. Dat is het dus niet waard om de IKEA-app te installeren. Gratis koffie bestaat niet!

❒ **Is er ook een webversie van de app? Voorbeeld: Marktplaats. Je kunt ook gewoon de website gebruiken in plaats van de app.** Je kunt zelfs een snelkoppeling maken van de website, welke vervolgens als app functioneert. Dit wordt ook een

Progressieve Web App genoemd. Dit kun je bijvoorbeeld met Brave Browser instellen. We hebben een zeer uitgebreide handleiding van Brave Browser op ons Pro Privacy Platform.

❒ **Gebruik indien mogelijk ALTIJD een authenticatorapp om je accounts extra te beveiligen.** Een authenticator-app zorgt ervoor dat je na het invoeren van je inloggegevens een extra handeling moet doen op je telefoon, zoals het invoeren van een 6-cijferige code. Aegis Authenticator voldoet aan onze kernwaarden en kan hiervoor worden gebruikt. Aegis Authenticator heeft een uitgebreide handleiding op ons Pro Privacy Platform.

❒ **Controleer REGELMATIG op updates van je apps.** Dit kan via de app-store(s) die je gebruikt op je apparaat.

❒ **Wees voorzichtig met gezondheidsapps:** Apps voor menstruatiecyclus, slaaptracking, fitness of meditatie verzamelen vaak zeer gevoelige gegevens. Lees de privacyverklaring zorgvuldig en kies voor diensten die end-to-end encryptie aanbieden en een duidelijk privacybeleid hebben.

Apparaatbeveiliging

❒ **Controleer REGELMATIG op updates van je apparaat** en voer ze uit. Als het apparaat na een update om een herstart vraagt, doe dit dan zo snel mogelijk. Stel dit dus NIET uit!

❒ **Stel ALTIJD een pincode (ontgrendelingscode) in op je telefoon en tablet en een wachtwoord op je computer.** Dit is een essentiële veiligheidsmaatregel die ervoor zorgt dat bij diefstal de kwaadwillende niet zomaar in je apparaat kan komen.

❒ **Maak ALTIJD gebruik van een vingerafdruk als je je op openbare plekken bevindt, zoals een winkelcentrum, station, etc.** Hiermee voorkom je dat mensen en camera's over je schouder kunnen kijken en kunnen zien wat je pincode/wachtwoord is.

❒ **Gebruik een privacy-screenprojector voor zowel je telefoon, tablet en laptop.** Dit zorgt ervoor dat je alleen kunt zien wat er zich op het scherm bevindt als je er recht voor zit. Dit is vooral handig in het OV. Ga er maar vanuit dat er iemand (bewust of onbewust) op je scherm kijkt.

❒ **Gebruik NOOIT Face ID** (gezichtsscans) om je apparaat te ontgrendelen.

❒ **Plaats je telefoon in een Faraday-hoesje als je deze niet gebruikt**. Als je alleen woont, hoef je dit niet te doen, tenzij je een alternatief hebt voor noodgevallen.

❒ **Sluit NOOIT zomaar een USB-stick aan op je laptop** als die niet van jou is.

❒ **Gebruik een schuifje voor de camera van je laptop.**

Reizen

❒ **Gebruik NOOIT parkeerapps, zelfs niet voor het gemak.** Parkeerautomaten verplichten je nooit om een app te gebruiken. Als een automaat géén cash accepteert, gebruik dan je pinpas. Dit is altijd beter dan het gebruik van een app.

❒ **Gebruik NOOIT Flitsmeister of andere soortgelijke apps.** Flitsmeister verkoopt je metadata (zoals je locatie, hoe lang je in de auto zit, wanneer de auto rijdt, etc.) door aan derde partijen.

❒ **Als je met het openbaar vervoer reist, koop een kaartje waar mogelijk.** Bij de grote stations kun je ook een Ov-kaart kopen met cash geld.

❒ **Indien het kopen van een kaartje niet mogelijk is, gebruik dan alleen een OV-chipkaart om in te checken** en niet een telefoon, pinpas, creditcard en de OVpay-app.

❒ **Sluit je apparaten NOOIT aan op een USB-poort die je tegenwoordig in het OV kunt vinden.** Pro Privacy Phones en -tablets hebben hier een interne beveiliging voor, maar ook dan is het af te raden.

❒ **Gebruik tijdens het reizen met het OV ALLEEN apps die niet kunnen zien waar je bent.** Mocht dit niet mogelijk zijn, beperk dan de locatiefunctionaliteit van de app en zoek handmatig de haltes op waar je meer informatie over wilt weten.

Sociale en Psychologische Privacy

❒ **Leer 'social engineering' herkennen:** Veel privacybreuken beginnen niet met een hack, maar met een telefoontje of e-mail van iemand die zich voordoet als iemand anders. Wees altijd sceptisch en verifieer de identiteit van degene die om informatie vraagt via een ander, bekend kanaal.

❒ **Beheer je 'privacy-expectancy':** Wees je ervan bewust dat privacy een trade-off is. Soms is een klein gemak (zoals een online bestelling) het verlies van een stukje privacy waard. Maak bewuste keuzes in plaats van alles standaard te accepteren.

❒ **Denk na over de privacy van anderen:** Deel geen foto's of informatie over vrienden, familie of collega's online zonder hun expliciete toestemming. Je bent mede verantwoordelijk voor hun privacy.

Werk en Onderwijs

❒ **Gebruik een apart apparaat voor werk:** Indien mogelijk, gebruik een door de werkgever verstrekte laptop of telefoon puur voor werkdoeleinden. Vermijd het installeren van privé-apps of het openen van privé-accounts op deze apparaten, omdat de werkgever hier vaak (wettelijk) toegang toe heeft.

❒ **Wees bewust van monitoringsoftware:** Werkgevers en scholen installeren vaak software om activiteit te monitoren. Ga er vanuit dat alles wat je doet op een apparaat van de zaak/school kan worden gezien.