

Digitaal veilig op reis in het buitenland

Van trainingsstages tot de Spelen

De wereld wordt steeds digitaler, ook de topsport. Kijk maar eens naar jouw trainingen en wedstrijden: kun je eigenlijk nog wel zónder data?

Digitale innovaties brengen ons veel, maar vormen ook een risico. Want wat gebeurt er als jouw gegevens in verkeerde handen komen? Of als trainings- en wedstrijddata op straat liggen? Dat moeten we met elkaar voorkomen. Niet alleen in Nederland, waar digitale veiligheid over het algemeen goed geregeld is, maar ook in het buitenland. Bijvoorbeeld als je op trainingsstage gaat of deelneemt aan een EK, WK of de Spelen.

Met deze checklist ga je altijd veilig op reis in het buitenland.



1. Vergrendel je apparaten

- Laat je je telefoon of laptop achter? Vergrendel die altijd. Je telefoon vergrendel je misschien vaak al wel onbewust, maar je laptop mogelijk minder snel.
- Een Windows-laptop vergrendel je snel met de toetsencombinatie Windows (⊞) + L.
 - Een Apple-laptop vergrendel je snel met de toetsencombinatie Control + Command (⌘) + Q

Tip: Gebruik als beveiliging je vingerafdruk of gezichtsherkenning om te ontgrendelen.



2. Gebruik geen openbare wifi-netwerken

- Het is verleidelijk: gebruikmaken van een openbaar wifi-netwerk dat geen wachtwoord vereist. Maar dit is absoluut niet veilig. Vanaf het moment dat je verbinding maakt met zo'n wifi-netwerk is je telefoon of laptop toegankelijk voor hackers.
- Wil je toch online op je laptop? Gebruik dan de wifi-hotspot via je eigen telefoon.
 - Kun je geen gebruikmaken van je eigen mobiele databundel in het land waar je bent? Overweeg dan om een databundel aan te schaffen van een lokale (maar bekende) provider en maak buiten de EU gebruik van een virtueel privénetwerk (VPN). Roamen met je eigen simkaart is een (duurder) alternatief.

Tip: Gebruik een VPN. Een VPN verbergt jouw identiteit, versleutelt jouw dataverkeer en vergroot dus jouw digitale veiligheid. Goede VPN's zijn overigens niet gratis.



3. Blijf alert op valse communicatie

98% van de hackaanvallen gebeurt via *social engineering*, zoals phishing of spoofing. Dit zijn vormen van oplichting waarbij neplinks worden gedeeld of berichten echt lijken, maar vals zijn. Vaak wordt gevraagd naar persoonlijke gegevens.

Wees voorzichtig: reageer nooit op verzoeken via telefoon of e-mail om inloggegevens te delen.

Tip: Blijf op reis extra alert. Juist in het buitenland komen vaak verzoeken binnen die moeilijker te herkennen zijn.



4. Installeer updates direct

Voer updates voor je apparatuur zo snel mogelijk uit. Vaak maken veiligheidsverbeteringen deel uit van een update, dus hoe eerder je een update installeert, hoe beter.

Tip: Zet je laptop uit net voordat je op reis gaat en herstart die bij aankomst met een veilige en snelle internetverbinding. Dan worden updates vaak automatisch geïnstalleerd.



5. Let op welke apps je installeert

Installeer niet zomaar een applicatie op je telefoon of laptop. Installeer applicaties alleen vanuit de officiële appstores. Apps die buiten de appstores om worden aangeboden, zijn over het algemeen niet gecontroleerd op schadelijke software.

In sommige landen is het installeren van applicaties minder veilig. Sommige regimes gebruiken apps om hun bevolking in de gaten te houden. Wees daarom terughoudend in het installeren van lokale apps.

Tip: Zorg dat je ook van applicaties zo snel mogelijk (of zelfs automatisch) de laatste updates installeert.



6. Verbind niet zomaar met externe apparaten

Een USB-stick, externe harde schijven, draadloze apparaten en zelfs USB-oplaadpoorten kunnen besmet zijn met virussen. Sluit je apparaten daarom niet zomaar aan op communicatiepoorten of andere apparaten waarvan je de eigenaar niet bent of niet goed kent.

Laad je apparaten op in het stopcontact, met de originele lader en de juiste reisstekker. Wil je toch een USB-oplaadpoort gebruiken? Gebruik dan een USB-dataprotector.

Tip: Sla in elk geval geen persoonsgegevens op een USB-stick. Niet alleen omdat een USB-stick vatbaar is voor virussen, ook omdat je die makkelijk kwijtraakt.



7. Maak back-ups van je gegevens

Weinig is vervelender dan het kwijtraken van je gegevens, of het nou door verlies, diefstal of beschadiging van je apparatuur is. Zorg er daarom voor dat je back-ups maakt, waar je ook bent.

Tip: Op veel apparaten kun je automatisch back-ups laten maken.



8. Houd je reisgegevens voor jezelf

Denk goed na over het delen van jouw reisplannen of verblijfslocaties op bijvoorbeeld social media. Als deze informatie in verkeerde handen valt, kunnen kwaadwillenden je bewegingen volgen en aanvallen plannen.

Tip: Wees terughoudend met het delen van locatiegegevens op online kanalen.



9. Neem zo min mogelijk data mee op reis

Data die je niet bij je hebt, kan ook niet gestolen worden. Zorg er daarom voor dat je alleen gegevens op je apparaten hebt staan die je tijdens je reis ook écht nodig hebt.

Staat er gevoelige informatie op je apparaten die je niet meer nodig hebt? Verwijder of archiveer deze dan. Zo beperk je de risico's.

Tip: Zorg ervoor dat je je apparaten opgeruimd houdt, ook als je niet op reis bent of gaat.

