PERSVEILIG

Checklist digitale veiligheid

Deze handout van PersVeilig bevat praktische tips, checklists en andere nuttige informatie om je dagelijkse werk als journalist veiliger te maken.

Contact met PersVeilig

Op de website persveilig.nl vind je allerlei informatie over veiligheid. Voel je daarnaast helemaal vrij om contact op te nemen als je wilt praten over veiligheidszaken. Het is een plezier om je te helpen of advies te geven.

E-mail: info@persveilig.nl

Volg PersVeilig ook op Twitter, LinkedIn en YouTube voor informatie, nieuws en tips.

Veilig en verantwoord online

Online ben je kwetsbaarder dan je denkt. Journalisten zijn soms geneigd de digitale gevaren te onderschatten. Of ze denken hun persoonlijke gegevens goed te hebben afgeschermd, terwijl dit niet het geval is. Hoe dan ook is de tijd definitief voorbij dat journalisten worden aangespoord zichzelf online zoveel mogelijk te profileren en op alle social media aanwezig te zijn. **Natuurlijk kun je online actief zijn, maar doe dit dan wel veilig en verantwoord.** Deze tips kunnen je hierbij helpen. Houd hierbij altijd in je achterhoofd dat de mens de zwakke schakel is als het om digitale veiligheid gaat.

Algemeen

- Check regelmatig wat er over jou online te vinden is. Google jezelf en check jezelf op social media. Vergeet ook zoekmachines als Bing en Yahoo niet.
- Denk altijd twee keer na voordat je een post plaatst.
- Let op dat je geen software downloadt bij openbare wifi-punten. Deze software kan malware bevatten. Let sowieso op bij het gebruiken van openbare wifi-punten omdat de beveiliging niet te garanderen is en je internetverkeer zichtbaar kan zijn voor derden.
- Laat apparatuur als telefoons en laptops niet zomaar rondslingeren in ruimtes waar je zelf niet bent. Dit geldt met name in hotels in het buitenland.
- Zorg dat de software altijd up to date is. Dit maakt de kans kleiner dat je slachtoffer wordt van online criminaliteit. Denk aan ransomware, waarbij je computer op afstand geblokkeerd wordt.
- Gebruik veilige wachtwoorden (*bijvoorbeeld via een password manager*) en maak waar mogelijk gebruik van tweetrapsverificatie.
- Communiceer zoveel mogelijk via een versleutelde berichtenservice, zoals Signal.

Social media

- Check periodiek of je privé-gegevens goed zijn afgeschermd op social media. Neem hier rustig de tijd voor, want het is niet altijd gemakkelijk om de privacy-instellingen van de verschillende platforms te doorgronden. Zorg vooral dat je telefoonnummer, informatie over naasten en woonadres niet openbaar zijn. Pas op met vrienden die jou taggen – waardoor het gevaar bestaat dat privéinformatie zichtbaar wordt voor derden.
- Onthoud: iedereen kan slachtoffer worden in het digitale domein. Als het jou overkomt, probeer het dan niet persoonlijk te maken – hoe moeilijk dit misschien ook is.
- Houd je mentale gezondheid in de gaten. Lees zo min mogelijk reacties onder een post die je geplaatst hebt. Maak sociale media niet belangrijker dan ze zijn en besteed er niet té veel tijd aan.

Tips voor werknemers en freelancers

- Scherm je social media-accounts goed af. Check regelmatig de privacy-instellingen.
- Bewaar alle bedreigende of haatdragende berichten. Maak screenshots en bewaar deze in een aparte map waar je ze niet elke dag tegen hoeft te komen. Constante confrontatie met die berichten moet je vermijden. Als bepaalde uitingen niet strafbaar zijn, kan een opeenstapeling van berichten van bepaalde personen wel leiden tot strafvervolging op basis van stalking of belaging.
- Blokkeer mensen die haatdragende berichten sturen. Let wel op! Als je iemand blokkeert of een bericht rapporteert voordat je het gedocumenteerd hebt dan is het weg - en blijft het weg. Dan heb je dus ook geen bewijs! Goede volgorde is cruciaal.
- Meld online dreigingen bij je werkgever en bij PersVeilig.
- Het verzamelen van al het materiaal kan na deze traumatische ervaring extra confronterend zijn. Vraag anderen dat te doen (*via de werkgever of vrienden*) als je het zelf niet aankunt.
- Let goed op je mentale gesteldheid. Online dreiging kan grote gevolgen hebben. Wees je daarvan bewust en zoek hulp als het je wordt aangeboden of als je merkt dat je hulp nodig hebt. verminderen, mocht je dit wensen.
- Als laatste, praat erover! Met familie, vrienden, werk- of opdrachtgever, collega's of slachtofferhulp. Je staat er niet alleen voor.

Tips voor werkgevers en leidinggevenden

Preventie en veiligheidsbeleid

- Zorg ervoor dat (nieuwe) werknemers getraind worden in (digitale) weerbaarheid en in het (veilig) gebruik van social media.
- Voer een zero tolerance-beleid als het gaat om online dreiging en intimidatie van de eigen werknemers.
- Monitor reacties op social media en haal dreigende en intimiderende reacties onmiddellijk weg.
- Freelancers voelen zich extra kwetsbaar en zijn mogelijk bang de dreiging te melden. Zorg voor een veilige werkomgeving waarin dit melden wél mogelijk is.
- Spreek met de social media afdeling af, dat werknemers en freelancers niet getagd worden in berichten van de werk- of opdrachtgever als zij dit liever niet hebben.

Als een journalist slachtoffer is geworden van online dreiging, intimidatie of haat:

- Begrijp de ernst van de situatie voor de betrokken werknemer wanneer deze is getroffen door online bedreigingen of agressie. Vraag jezelf af of (*andere*) leidinggevenden de urgentie van het probleem erkennen. Vraag jezelf af of leidinggevenden hiervoor getraind moeten worden. Een werknemer die getroffen wordt door online aanvallen, heeft behoefte aan erkenning. Bied die.
- Zorg ervoor dat werknemers alle steun krijgen, inclusief psychosociale hulp. Neem online dreiging serieus. De gevolgen voor de werknemers kunnen groot zijn. Online dreiging is géén part of the job.
- Vraag waar de werknemer behoefte aan heeft. Elke werknemer die te maken heeft gehad met (*massale*) online dreiging, voelt zich eenzaam en verlaten.
- Soms bieden collega's aan de social media-accounts te monitoren of om belastend materiaal te verzamelen. Dit kan de getroffen journalist enorm helpen.
- Veel journalisten die te maken hebben gehad met online dreiging, vragen zich af of de beledigingen en dreigingen zijn veroorzaakt door hun eigen schuld. Verzeker de medewerker dat hij of zij niets fout heeft gedaan.
- Indien nodig is een publieke steunbetuiging van de werknemer te overwegen – zeker als het gaat om een massale aanval.
- Neem naar buiten toe onherroepelijk stelling tegen racisme. Diversiteit in de media draait niet alleen om het binnenhalen van mensen, maar hen ook houden en rugdekking geven wanneer zij om hun uiterlijk of achtergrond worden aangevallen.
- Bied de getroffen werknemer aan al het materiaal te (*laten*) verzamelen.

Nuttige websites

- Op http://geosocialfootprint.com/ kun je de locaties zien van Twitter-accounts (van jezelf en van anderen).
- De website https://webmii.com/ geeft een overzicht van jouw aanwezigheid op verschillende social media.
- https://veiliginternetten.nl/ en https://laatjeniethackmaken.nl/ zijn websites met tips en trucs over online veiligheid.
- Facebook biedt mogelijkheden om jezelf te registreren als journalist. Geregistreerde journalisten worden beter beschermd dan reguliere gebruikers. Ook andere social media hebben dit soort veiligheidsopties.
- Wachtwoordmanager https://1password.com/for-journalism/ biedt speciale mogelijkheden voor journalisten.
- Op https://cltc.berkeley.edu/ vind je een online security guide for journalists.
- Dit is een veiligheidsplanner: https://securityplanner.consumerreports.org/.
- Neem contact op met Google als er privégegevens in de zoekmachine staan. Ga naar de Google Beschermingspagina: https://landing.google.com/advancedprotection/

***Tip:** op PersVeilig.nl is de interactieve training 'Eerste hulp bij online bedreigingen' te vinden.*

Over PersVeilig

PersVeilig wil de positie van journalisten versterken tegen geweld en agressie op straat, op social media en tegen juridische claims.

NVJ

Nederlands Genootschap van Hoofdredacteuren

POLITIE

OPENBAAR MINISTERIE