SCHRIJVERS VEILIG

Checklist digitale veiligheid

Deze checklist bevat praktische tips en andere nuttige informatie om je dagelijkse werk als schrijver veiliger te maken.

Contact met SchrijversVeilig

Op de website schrijversveilig.nl kun je terecht voor het meldpunt, de helpdesk en informatie over de veiligheidstraining. Voel je daarnaast helemaal vrij om contact op te nemen als je wil praten over veiligheidszaken. Het is een plezier om je te helpen of advies te geven.

E-mail: info@persveilig.nl

Veilig en verantwoord online

Online ben je kwetsbaarder dan je denkt. We zijn soms geneigd de digitale gevaren te onderschatten. Of we denken onze persoonlijke gegevens goed te hebben afgeschermd, terwijl dit niet het geval is. Hoe dan ook is de tijd definitief voorbij dat schrijvers 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 überhaupt 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 tweestapsverificatie.
- 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 schrijvers

- Scherm je social media accounts goed af. Check regelmatig de privacy-instellingen.
- Bewaar bij bedreiging of intimidatie alle 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/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 wel. Dan heb je dus ook geen bewijs! Goede volgorde is cruciaal.
- Meld online dreigingen bij je uitgever en SchrijversVeilig.
- Het verzamelen van al het materiaal kan na deze traumatische ervaring extra confronterend zijn. Vraag anderen dat te doen (via de uitgever 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.

Internet Privacy Tool

Om de bewustwording te vergroten en onder andere schrijvers de kans te geven hun online zichtbaarheid te beperken, heeft PersVeilig in samenwerking met andere publieke beroepen de *Internet Privacy Tool* ontwikkeld. De tool laat je zien in welke gratis online registers jouw naam, achternaam in combinatie met jouw privé adres voorkomen. Het werkt heel eenvoudig. Klik op de link en maak een account aan op de Internet Privacy Tool.

Vervolgens begeleidt de tool je met concrete stappen om jouw online vindbaarheid te verminderen, mocht je dit wensen. De tool werkt uitsluitend op een laptop of desktop.

Registreer via: **inpri.nl**
Bij problemen met de registratie neem je contact op met support@inpri.nl

Nuttige websites

- Op **fixjeprivacy.nl** staan ook persoonlijke verhalen op van mensen die hier bewuster mee om zijn gegaan na een gebeurtenis.
- Op **geosocialfootprint.com** kun je de locaties zien van Twitter-accounts (van jezelf en van anderen).
- De website **webmii.com** geeft een overzicht van jouw aanwezigheid op verschillende social media.
- **veiliginternetten.nl** en **laatjeniethackmaken.nl** zijn websites met tips en trucs over online veiligheid.
- Problemen met je online veiligheid? Check dan deze website **digitalfirstaid.org**
- Dit is een veiligheidsplanner: **securityplanner.consumerreports.org**.
- Neem contact op met Google als er privégegevens in de zoekmachine staan. Ga naar de Google Beschermingspagina: **landing.google.com/advancedprotection**

Tips voor uitgevers

Preventie en veiligheidsbeleid:

- Zorg ervoor dat schrijvers getraind worden in weerbaarheid en in het (veilig) gebruik van social media.
- Als freelancer voel je je extra kwetsbaar en mogelijk bang de dreiging te melden. Zorg voor een veilige werkomgeving waarin dit melden wel mogelijk is.
- Spreek met de social media afdeling af, dat schrijvers niet getagd worden in berichten van de uitgever als zij dit liever niet hebben.
- Monitor social media reacties en haal dreigende en intimiderende reacties onmiddellijk weg door het techbedrijf.
- Voer een zerotolerance-beleid als het gaat om online dreiging en intimidatie binnen de uitgeverij.

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

- Vraag waar de schrijver behoefte aan heeft. Iedereen, die te maken heeft gehad met massale online dreiging, kent een gevoel van eenzaamheid en verlatenheid.
- Begrijp de ernst van de situatie voor de betrokken schrijver. Een schrijver die getroffen wordt door online aanvallen heeft behoefte aan erkenning. Bied die.
- Zorg ervoor dat schrijvers alle steun krijgen inclusief psychosociale hulp. Neem online dreiging serieus. De gevolgen voor hen kunnen groot zijn. Online dreiging is geen *part of the job*. Verzeker de schrijver dat hij/zij niets fout heeft gedaan.
- Getroffen schrijvers voelen zich vaak eenzaam. Betrek de directe redacteuren erbij. Bied aan de social media accounts te monitoren of om het belastende materiaal te verzamelen. Dat kan de getroffen schrijver enorm helpen.
- Indien nodig, is een publicitaire steunbetuiging aan de schrijver te overwegen. Zeker als het gaat om een massale aanval.

Over SchrijversVeilig

SchrijversVeilig is een gezamenlijk initiatief van de Auteursbond en de Groep Algemene Uitgevers en heeft tot doel de positie van schrijvers te versterken tegen geweld, agressie en intimidatie. Zowel online als fysiek. SchrijversVeilig wordt ondersteund door het ministerie van OCW.

SchrijversVeilig wordt ondergebracht bij PersVeilig dat haar expertise inzet om auteurs en uitgevers te ondersteunen.

Auteursbond

GAU Groep Algemene Uitgevers