



Dienst Justitiële Inrichtingen
Ministerie van Justitie en Veiligheid

Brochure

(Online) veiligheidsbewustzijn bij werken met radicalisering en extremisme



Vergroot jouw impact

Rijksopleidingsinstituut
tegenaan
Radicalisering





(Online) veiligheidsbewustzijn

Veiligheid is een essentieel onderdeel om goed je werk te kunnen doen, zowel in de fysieke omgeving, maar ook in toenemende mate online. Als je werkt in het zorg- of veiligheidsdomein en op het onderwerp radicalisering en extremisme in het bijzonder kan het helaas voorkomen dat mensen niet netjes omgaan met jouw (online) veiligheid of hier zelfs een dreiging voor vormen. Zo kan je bijvoorbeeld slachtoffer worden van doxing, zeker omdat je in aanraking komt met doelgroepen die zich hier schuldig aan kunnen maken. Daarom is het belangrijk om je bewust te zijn van je eigen (online) veiligheid en gedrag om preventieve maatregelen te nemen waar mogelijk. Hierin speelt niet alleen je werkgever een belangrijke rol: het is belangrijk om ook zelf stappen te zetten om je veiligheid te beschermen. In deze brochure lees je hoe je dit kan doen.

Goede voorlichting helpt om mogelijke risico's voor zowel het individu als het team te voorkomen en te beheersen. In deze brochure lees je meer over online vindbaarheid en hoe je jouw online veiligheid kunt vergroten. Deze brochure is bedoeld als een praktisch hulpmiddel, voorzien van algemene informatie, tips & tricks en een doorverwijzing naar aanvullend materiaal. Het biedt richtlijnen voor stappen die je kan zetten om je veiligheid te beschermen, maar het is aan jou om te beslissen hoe je deze adviezen toepast. Bij deze brochure ligt de nadruk op de preventie van online incidenten. Meer informatie over de afhandeling van incidenten vind je hier.



Doxing

Medewerkers met een publieke taak kunnen te maken krijgen met doxing. Sinds 1 januari 2024 is doxing **strafbaar**.

Doxing is het (digitaal) aanbieden of verspreiden van identificerende persoonsgegevens, met de intentie om het slachtoffer angst aan te (laten) jagen, ernstige overlast aan te (laten) doen of de medewerker in diens ambt of beroep ernstig te (laten) hinderen. Anders gezegd: om anderen lastig te vallen of te intimideren. Ook het verzamelen van gegevens met deze doelen is strafbaar. Denk hierbij aan persoonsgegevens zoals een (achter)naam, woonadres of telefoonnummer.

Doxing kan verstrekken gevolgen hebben. Het kan invloed uitoefenen op:

- Je privéleven
- Je sociale omgeving
- Je werk (taakuitoefening en werkplezier)

Bij doxing is de schade niet alleen fysiek of direct zichtbaar, maar kan het effect langdurig of zelfs permanent doorwerken in je dagelijks leven. Ook is het moeilijk te voorspellen hoe lang de dreiging aanhoudt of wanneer deze weer kan opblazen. Het is belangrijk om deze bedreiging serieus te nemen en passende maatregelen te treffen.

Tips & tricks voor het beschermen van je eigen veiligheid

1. Beperk het delen van persoonlijke informatie (zowel op sociale media als in gesprekken met externe personen)

- ✓ **Beheer je privacy-instellingen:** Controleer op sociale media wie jouw informatie kan zien en pas je privacy-instellingen aan om te voorkomen dat je gegevens openbaar worden gedeeld. Controleer dit regelmatig, zeker na updates die instellingen mogelijk kunnen terugzetten. Denk goed na over welke media je gebruikt;
- ✓ **Deel geen persoonlijke gegevens** zoals je adres, telefoonnummer, geboortedatum of financiële informatie op sociale media. Maak ook afspraken over wat je (schoon)familie en vrienden over je delen;
- ✓ **Wees voorzichtig met foto's en video's:** Deel geen beelden die persoonlijke of gevoelige informatie bevatten;
- ✓ **Controleer je online aanwezigheid regelmatig:** Houd je online profiel up-to-date en bekijk regelmatig wat er over jou op het internet te vinden is.

2. Neem maatregelen om je privacy te beschermen

- ✓ **Wees selectief met connecties:** Accepteer alleen connectieverzoeken van mensen die je kent en vertrouwt;
- ✓ **Gebruik sterke en unieke wachtwoorden en voorkom dat je gegevens op straat komen te liggen:** Zorg voor unieke, sterke wachtwoorden voor al je online accounts en verander ze regelmatig. Gebruik een wachtwoordkluis om jouw wachtwoorden te bewaren en beveiligen. Je kan ook een alias gebruiken als gebruikersnaam om je privacy extra te beschermen;
- ✓ **Gebruik tweestapsverificatie** voor een extra beveiligingslaag;
- ✓ **Gebruik een VPN:** Door het gebruik van een VPN zien anderen niet wat jij op het internet doet en ben je moeilijker te traceren;
- ✓ **Laat geen visitekaartjes slingeren:** Als je gebruik maakt van visitekaartjes, denk dan goed na over aan wie je deze uitdeelt en laat ze niet slingeren. Mensen kunnen mogelijk misbruik maken van de informatie die hierop staat.



3. Wees je bewust van mogelijke risico's in contact met burgers

- ✓ Gebruik het **algemene mailadres** van je organisatie;
- ✓ **Bel anoniem** door #31# te typen voor het telefoonnummer dat je anoniem wilt bellen;
- ✓ Noem alleen je voornaam en je werkgever;
- ✓ Stem in contact met burgers vooraf af of het gesprek mag worden opgenomen en op welke manier;
- ✓ **Wees alert** wanneer er lange gesprekken worden gevoerd en de burger uit lijkt te zijn op uitspraken van een ambtenaar. Wanneer deze gesprekken worden gedeeld kan dit negatieve gevolgen hebben voor jou of je organisatie;
- ✓ Neemt de burger niet op, **wees dan zorgvuldig** in jouw overweging om wel of geen voicemail en nummer achter te laten. Benoem alleen je voornaam en organisatie of stuur vanuit je organisatie een mail met verzoek tot contact;
- ✓ **Deel niet zomaar gegevens van collega's**, ook niet als de burger al een deel van de informatie heeft;
- ✓ **Ga nooit alleen op huisbezoek** en deel met collega's waar en wanneer het huisbezoek plaatsvindt;
- ✓ **Bereid kantoorbezoeken goed voor.** Bespreek mogelijke risico's met de beveiliging en de receptie en kies een geschikte ruimte. Ga na of er een bouwverbod is.

4. Weet wat je kan en moet doen bij een incident

- ✓ Ga na of er binnen jouw organisatie een **veiligheidsprotocol** is met extra maatregelen en afspraken die je veiligheid beschermen;
- ✓ Weet dat je **aangifte** kan doen van doxing;
- ✓ Weet waar je terecht kan als je slachtoffer bent van doxing en informeer je leidinggevende;
- ✓ Maak met je organisatie **afspraken over de grenzen** die je als medewerker kan trekken en geef deze duidelijk aan;
- ✓ **Trek tijdig aan de bel** als je zorgen hebt over je eigen veiligheid.

Meer weten?

- Deze brochure is gemaakt door het Rijksopleidingsinstituut tegengaan Radicalisering (ROR). Ga voor meer informatie naar onze website: www.tegengaanradicalisering.nl.
- Slachtoffer van doxing? Download het Handelingskader doxing voor slachtoffers of zoek hulp bij HelpWanted.
- Weten wat je als werkgever kan doen? Bekijk het Handelingskader doxing voor Werkgevers.
- Informatie en praktische tips en tricks over veilig gebruik van internet vind je op veiliginternetten.nl.
- Voor meer informatie over veilig en slim gebruik van (digitale) media ga je naar Mediawijsheid.nl.
- Behoeftte aan meer algemene informatie over hacken en tips over hoe je jezelf beschermt tegen hackers? Lees de handleiding van Laat je Niet Hack Maken.

