Ministerie van Binnenlandse Zaken
en Koninkrijksrelaties

Factsheet

Digitale veiligheid (kandidaat) volksvertegenwoordigers

De Nederlandse democratie is open en digitaal verbonden. Dat maakt ons sterk, maar ook kwetsbaar. Als (kandidaat) volksvertegenwoordiger bent u een zichtbaar doelwit voor buitenlandse mogendheden, cybercriminelen en andere kwaadwillenden. Uw persoonlijke en officiële digitale accounts vormen toegangspoorten tot gevoelige informatie en een breed publiek. Wordt een account gehackt, dan kan dit leiden tot verlies van persoonlijke gegevens of reputatieschade, en bovendien worden misbruikt om desinformatie of andere schadelijke content te verspreiden.

Ook kunt u zelf te maken krijgen met illegale of schadelijke content, zoals haatzaaien, georganiseerde desinformatiecampagnes of de impersonatie van uw accounts. Het is daarom van belang dat u weet hoe u uw digitale veiligheid versterkt en hoe u zich tegen dergelijke dreigingen kunt beschermen.

Tips voor het beschermen van uw persoonlijke en officiële digitale accounts

Uw digitale accounts – persoonlijk én officieel – zijn waardevolle doelwitten. Met enkele eenvoudige, maar cruciale stappen verkleint u het risico aanzienlijk.

1. Kies sterke wachtwoorden of wachtzinnen

Een sterk wachtwoord is lang, uniek en moeilijk te raden. Kies liever een wachtzin van minimaal 12 tekens. Bijvoorbeeld: *De Kleine Blauwe Beer Loopt 20KM?*. Vermijd namen, geboortedata of reeksen zoals *12345* of *Welkom01*.

2. Log in met twee stappen

Met multifactorauthenticatie (MFA/2FA) voegt u een extra beveiligingslaag toe, bijvoorbeeld via een sms-code of een authenticatie-app. Zelfs als een wachtwoord uitlekt, blijft uw account beschermd. Zet MFA altijd aan, zeker voor e-mail en sociale media.

3. Ga veilig om met uw wachtwoorden

Deel uw wachtwoorden nooit en schrijf ze niet op of rond uw computer. Gebruik voor elk account een ander wachtwoord en wijzig ze direct als u een datalek vermoedt. Sla wachtwoorden nooit onbeveiligd of in de browser op.

Maak daarnaast gebruik van een wachtwoordmanager. Een wachtwoordmanager helpt u sterke, unieke wachtwoorden te bedenken en veilig op te slaan. U hoeft slechts één hoofdwachtwoord of -zin te onthouden. Kies een betrouwbare wachtwoordmanager en zet MFA ook daarop aan.

4. Ben alert op phisingmails

Let op kleine verschillen in domeinnamen en wees alert bij algemene aanheffingen. Klik nooit zomaar op links of open bijlagen in verdachte mails. Neem bij twijfel direct contact op met de betreffende organisatie via hun officiële contactgegevens.

5. Besteed speciale aandacht aan de beveiliging van uw e-mail

Uw e-mail is vaak de sleutel tot al uw andere accounts, omdat veel wachtwoorden via e-mail kunnen worden gereset. Pas de eerder genoemde beveiligingsstappen daarom niet alleen toe op uw sociale media, maar zeker ook op uw e-mailaccount. Let bovendien op meldingen van verdachte inlogpogingen: u ontvangt dan vaak een bericht dat er vanaf een onbekende locatie is geprobeerd in te loggen. Krijgt u een dergelijke melding, wijzig dan direct uw wachtwoord.

6. Bescherm uw apparaten

Kwaadwillenden kunnen ook toegang krijgen tot uw accounts via onvoldoende beveiligde apparaten. Zorg daarom dat beveiligings-updates automatisch worden geïnstalleerd en vergrendel altijd uw telefoon, laptop of tablet. Ook als u maar kort weggaat.

Vervelende online ervaringen: wat kun je doen als gebruiker?

Het belang van de Digital Services Act voor het omgaan met illegale of schadelijke content

De DSA verplicht online platforms om transparanter, verantwoordelijker en veiliger te opereren. De DSA geeft meer rechten aan gebruikers van online platforms.

De DSA bepaalt niet wat illegale of schadelijke content is. Rapporteren van deze content bij het platform draagt bij aan een veiligere online omgeving voor jezelf én anderen

1. Hoe herken ik illegale & schadelijke content?

Illegale content = content verboden onder EU- of NL wetgeving. Het kan gaan om berichten, foto's, advertenties, video's of ander online materiaal:

- Discriminatie;
- Bedreigingen;
- (seksuele) intimidatie;
- Aanzetten tot haat of geweld;
- Delen van persoonsgegevens zonder toestemming of andere grondslag;
- Zonder toestemming gebruiken van (partij)logo's van anderen

Schadelijke content = content die niet illegaal is maar mogelijk wel *schadelijk voor personen of de maatschappij*, en vaak in strijd met de *voorwaarden* van het platform:

- Desinformatie: opzettelijk onjuiste informatie verspreiden
- Impersonatie: voordoen als een ander met een nepaccount of in content, zoals *deepfakes*. Impersonatie kan in bepaalde situaties ook illegaal zijn (bijvoorbeeld onder auteursrecht).
- Pesten

Let op: Het platform oordeelt of gerapporteerde content wel of niet toegestaan is. ACM gaat over zorgvuldigheidsverplichtingen die onder de DSA gelden voor platformen, en oordeelt niet over de inhoud.

2. Wat kan ik doen bij het zien van dit soort content?

a. Rapporteer content bij het platform: In de buurt van de content vind je een mechanisme om (vermoedelijk) illegale en/of schadelijke content te rapporteren. Je ziet bijvoorbeeld een vlag-icoon of 'rapporteer'.
   - Dit is verplicht onder de DSA.

b. Je ontvangt van het platform tijdig een reactie waarin ten minste moet staan wat zij n.a.v. jouw rapportering gaan doen en waarom.
   - Het platform kan bijvoorbeeld besluiten de content te verwijderen, te verbergen of te laten staan. Al deze opties moeten onderbouwd worden.

c. Ben je het niet eens met de beslissing?
   - Dan heb je recht om bij het platform bezwaar te maken. Het platform moet dit mogelijk maken met een online mechanisme dat makkelijk vindbaar is.

d. Gaat het proces niet zoals het hoort?
   - Kun je bijvoorbeeld niet rapporteren, volgt er geen reactie of kun je niet in bezwaar gaan? Meld dit dan bij de ACM
   - Ben je het na de reactie op jouw bezwaar nog steeds niet eens met de inhoudelijke beslissing? Dan kun je terecht bij een buitengerechtelijk geschillenorgaan of de civiele rechter. Deze organisaties beoordelen wie er gelijk heeft.

5. Wat is het effect van mijn handelen?

Rapporteren bij het platform:

- Je draagt bij aan een veiligere online omgeving voor jezelf én anderen: Melden bij het platform is de snelste manier om te zorgen dat er minder slachtoffers zijn van illegale en schadelijke content, nu en in de toekomst. Meldingen helpen platforms namelijk om hun online omgeving veilig te houden; zij zien niet alles wat er gebeurt en hebben jou hiervoor nodig. Het creeëren van een veilige online omgeving is een doorlopend proces: normen van welke content we aanvaardbaar of juist schadelijk vinden, maken we met elkaar.
- Jouw melding bij het platform zorgt ervoor dat zij snel moeten beslissen welk gevolg ze hieraan geven. Het platform kan bijvoorbeeld besluiten om de content te verwijderen, ontoegankelijk of minder zichtbaar te maken, de gebruiker waarschuwen of zijn account blokkeren. Het platform kan ook besluiten geen maatregel te nemen. Over deze beslissing moet het platform je duidelijk gemotiveerd informeren.

Melden bij de ACM:

- Meldingen bij ACM over een onzorgvuldig behandelingsproces bij het platform dragen bij aan het beeld wat mogelijk niet goed gaat bij een platform. Meldingen kunnen door ACM worden gedeeld met de Europese Commissie die toezicht houdt

*En wat gebeurt er **niet**?*

- De ACM bepaalt niet welke content wel en niet toegestaan is, en welke content het platform moet verwijderen. Dit is aan het platform zelf om te beoordelen. De ACM houdt wel toezicht op de processen die platforms hebben ingericht voor een veilige online omgeving.

- Accounts van gebruikers mogen niet zomaar geblokkeerd worden na meldingen. Ook mag content niet zomaar verwijderd worden. Platforms moeten dit soort keuzes goed kunnen onderbouwen. Zij moeten naast zorgen voor veiligheid, ook rekening houden met andere belangen van gebruikers en de vrijheid van meningsuiting beschermen.

6. Wat kan ik doen als mijn account of content onterecht is geblokkeerd of verwijderd?

a. Een online platform mag niet zomaar jouw account of content blokkeren of verwijderen. In de voorwaarden van het platform kun je lezen wanneer zij dit wel mogen doen (dit is verplicht).
   - Bijvoorbeeld wanneer jouw content illegaal is, of in strijd met de voorwaarden omdat het schadelijk is voor personen of de maatschappij

b. Bent je het niet eens met de blokkering of verwijdering? Dien dan een klacht in bij het platform.
   - In de voorwaarden moet staan hoe u een klacht kunt indienen. Het platform moet zorgen dat je contact kunt opnemen met een persoon (alleen een chatbot is niet voldoende). Het platform moet tijdig beslissen en jou op de hoogste stellen. Sommige platforms bieden een extra contactpunt aan voor invloedrijke gebruikers. Kijk hiervoor bij de service-pagina van het platform.

c. Ben je het niet eens met de beslissing? Maak dan bezwaar bij het platform.
   - Het platform moet dit mogelijk maken met een online mechanisme dat makkelijk vindbaar is.

d. Gaat het proces niet zoals het hoort? Verwijdert of blokkeert het online platform jouw content of account zonder uitleg? Reageert het online platform niet op jouw klacht? Of heeft het geen contactpunt waar je makkelijk een klacht kunt indienen?
   - Meld dit dan bij de ACM
   - Ben je het na de reactie op jouw bezwaar nog steeds niet eens met de inhoudelijke beslissing? Dan kun je terecht bij een buitengerechtelijk geschillenorgaan of de civiele rechter. Deze organisaties beoordelen wie er gelijk heeft.

Dit is een uitgave van

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

In samenwerking met het Nationaal Cyber Security Centrum en de Autoriteit Consument & Markt