

8. Ga sociaal, maar let op je stappen

CYBERSECURITY

SUMMER



**GA SOCIAAL,
MAAR LET
OP JE
STAPPEN**

Privacy-
instellingen

Vriendschaps-
en connectieverzoeken
verifiëren

Wees
voorzichtig met
persoonlijke
informatie

Pas op voor
phishing en
oplichting

Sterke en
unieke
wachtwoorden

Regelmatige
account-
bewaking

Denk na
voordat je iets
plaatst

In het kort.
Het handhaven van de beveiliging op sociale media
is essentieel om verschillende risico's te voorkomen,
zoals phishing, inbreuk op de privacy, malware en
reputatieschade. We moedigen aan om actief te zijn
op LinkedIn, maar denk goed na over de content die je
deelt. Neem bij twijfel contact op met je afdelingshoofd
of de marketingcollega's.

voor meer
INFO en TIPS



Vragen?
ict@intersoft-electronics.com



Het gebruik van sociale media brengt verschillende beveiligingsrisico's met zich mee die mogelijk tot persoonlijke en professionele problemen kunnen leiden.

1. VEILIGHEIDSRISICO'S VAN HET GEBRUIK VAN SOCIALE MEDIA

1. Phishing-aanvallen
 - Oplichting: Cybercriminelen gebruiken sociale-mediaplatforms om phishing-berichten en links te verzenden, die gebruikers kunnen misleiden om persoonlijke informatie of inloggegevens vrij te geven.
 - Nabootsing van identiteit: Aanvallers kunnen nepprofielen maken om zich voor te doen als vrienden, collega's of bedrijven om je vertrouwen te winnen en gevoelige informatie te vragen.
2. Inbreuk op de privacy
 - Te veel delen: Het plaatsen van te veel persoonlijke informatie kan leiden tot inbreuken op de privacy. Deze gegevens kunnen door kwaadwillenden worden gebruikt voor identiteitsdiefstal of social engineering-aanvallen.
 - Gegevensverzameling: Sociale-mediaplatforms kunnen uitgebreide gegevens verzamelen over je gedrag, voorkeuren en persoonlijke gegevens, die aan derden kunnen worden verkocht.
3. Cyberstalking en intimidatie
 - Persoonlijke veiligheid: Openbaar beschikbare persoonlijke informatie kan gebruikers het doelwit maken van cyberstalking en intimidatie.
 - Professionele risico's: Intimidatie op professionele netwerken zoals LinkedIn kan je professionele reputatie en relaties schaden.
4. Malware en spyware
 - Kwaadaardige links: Het klikken op niet-geverifieerde links of het downloaden van bijlagen van sociale media kan leiden tot malware-infecties.
 - Gecompromitteerde accounts: Malware kan inloggegevens en andere gevoelige gegevens stelen die op je apparaten zijn opgeslagen.
5. Reputatieschade
 - Ongepaste inhoud: Berichten, opmerkingen of foto's die worden gedeeld zonder rekening te houden met de impact ervan, kunnen je persoonlijke en professionele reputatie schaden.
 - Verkeerde interpretatie: Inhoud die in een specifieke context wordt gedeeld, kan verkeerd worden begrepen of uit de context worden gehaald, wat kan leiden tot mogelijke reputatieschade.
6. Gerichte aanvallen
 - Gepersonaliseerde oplichting: Cybercriminelen kunnen informatie die is verzameld van sociale media gebruiken om gepersonaliseerde aanvallen uit te voeren, waardoor ze overtuigender worden.
 - Bedrijfsspionage: Informatie die wordt gedeeld op professionele netwerken zoals LinkedIn kan worden gebruikt voor bedrijfsspionage of om je bedrijf aan te vallen.

2. BEST PRACTICES VOOR VEILIG GEBRUIK VAN SOCIALE MEDIA

1. Privacy-instellingen

- Instellingen aanpassen: Controleer en pas regelmatig de privacy-instellingen op je sociale media-accounts aan om te bepalen wie je informatie en berichten kan zien.
 - Beperk het publiek: deel persoonlijke informatie en berichten met een beperkt publiek (vrienden of connecties) in plaats van met het publiek.
2. Wees voorzichtig met persoonlijke informatie
- Minimaal delen: Vermijd het delen van gevoelige persoonlijke informatie zoals je huisadres, telefoonnummer of financiële gegevens.
 - Selectief delen: Wees selectief over de persoonlijke en professionele informatie die je deelt om het risico op misbruik te minimaliseren.
3. Sterke en unieke wachtwoorden
- Wachtwoordbeheer: Gebruik sterke, unieke wachtwoorden voor elk social media-account en overweeg om een wachtwoordbeheerder te gebruiken om ze bij te houden.
 - MFA inschakelen: Schakel multi-factor authenticatie (MFA) in voor een extra beveiligingslaag.
4. Vriendschaps- en connectieverzoeken verifiëren
- Authenticiteit: accepteer alleen vriendschaps- of connectieverzoeken van mensen die je kent of kunt verifiëren. Wees op je hoede voor nepprofielen.
 - Profielen controleren: Bekijk profielen en onderlinge connecties voordat je verzoeken accepteert.
5. Denk na voordat je iets plaatst
- Inhoudsoverweging: Overweeg de potentiële impact en het publiek voordat je berichten, opmerkingen of foto's deelt.
 - Professionaliteit: Zorg voor een professionele houding op alle sociale-mediaplatforms om je reputatie te beschermen.
6. Pas op voor phishing en oplichting
- Verdachte links: Klik niet op links en download geen bijlagen van onbekende of verdachte bronnen.
 - Oplichting melden: Meld verdachte activiteiten of oplichting aan het socialemediaplatform.
7. Regelmatige accountbewaking
- Activiteitenlogboek: Controleer regelmatig de activiteitlogboeken van je account op ongeoorloofde toegang of ongebruikelijke activiteiten.
 - Afmeldsessies: Zorg ervoor dat je afmeldt bij sociale media-accounts wanneer je ze niet gebruikt, vooral op gedeelde of openbare apparaten.

3. LINKEDIN-SPECIFIEKE VEILIGHEIDSTIPS

1. Professioneel profielbeheer
- Nauwkeurige informatie: Zorg ervoor dat de informatie op je LinkedIn-profiel correct is en je professionele identiteit weerspiegelt, maar deel gevoelige details niet te veel.
 - Instellingen voor openbaar profiel: Pas de instellingen van je openbare profiel aan om te bepalen welke informatie zichtbaar is voor niet-connecties.
2. Verbindingsverzoeken verifiëren

- Professioneel netwerk: Maak alleen contact met mensen die je kent of die een legitiem professioneel belang hebben. Controleer de authenticiteit van verbindingsverzoeken, vooral van vreemden.
 - Gepersonaliseerde berichten: Gebruik gepersonaliseerde berichten bij het verzenden van verbindingsverzoeken om ontvangers te helpen je intentie te herkennen.
3. Wees voorzichtig met aanbiedingen
- Wees voorzichtig met kansen die te mooi lijken om waar te zijn. Controleer de echtheid van het aanbod.
4. Ga verstandig om
- Professionele interacties: Neem deel aan professionele discussies en opmerkingen. Vermijd controversiële onderwerpen die van invloed kunnen zijn op je professionele imago.
 - Groepsdeelname: Word lid van en neem deel aan groepen die relevant zijn voor je branche, maar houd rekening met de informatie die je deelt in groepsdiscussies.
5. Beheer de zichtbaarheid van je profiel
- Zichtbaarheid aanpassen: bepaal wie je activiteitsfeed en updates kan zien om je professionele aanwezigheid en privacy te beheren.
 - Openbare zoekopdrachten: Beperk welke informatie beschikbaar is voor het publiek via zoekmachines door je LinkedIn-profielinstellingen aan te passen.

4. SAMENGEVAT

Het handhaven van de beveiliging op sociale media is essentieel om verschillende risico's te voorkomen, zoals phishing, inbreuk op de privacy, malware en reputatieschade. We moedigen aan om actief te zijn op LinkedIn, maar denk goed na over de content die je deelt. Neem bij twijfel contact op met je afdelingshoofd of de marketingcollega's.



Samen houden we InterSoft Electronics cyber secure

INTERSOFT ELECTRONICS NV
Lammerdries-Oost 27 | B-2250 Olen | België
Tel. +32 14 23 18 11 | support@intersoft-electronics.com