

8. Go social, but watch your steps

CYBERSECURITY



SUMMER

**GO SOCIAL,
BUT WATCH
YOUR
STEPS**

Privacy Settings	Think Before You Post	Our cybersecurity, Everyone's accountability for more INFO and TIPS  Questions? ict@intersoft-electronics.com
Be Cautious with Personal Information	Be Aware of Phishing and Scams	
Strong and Unique Passwords	Regular Account Monitoring	
Verify Friend and Connection Requests	In summary: Maintaining security on social media is essential to prevent various risks such as phishing, privacy invasion, malware, and reputational damage. We encourage being active on LinkedIn but think carefully about the content you share. When in doubt contact your department head or marketing colleagues. 	

Using social media comes with several security risks that can potentially lead to personal and professional issues.

1. SECURITY RISKS OF USING SOCIAL MEDIA

1. Phishing Attacks

- Scams: Cybercriminals use social media platforms to send phishing messages and links, which can trick users into disclosing personal information or login credentials.
- Impersonation: Attackers can create fake profiles to impersonate friends, colleagues, or companies to gain your trust and solicit sensitive information.

2. Privacy Invasion

- Oversharing: Posting too much personal information can lead to privacy breaches. This data can be used by malicious actors for identity theft or social engineering attacks.
- Data Harvesting: Social media platforms can collect extensive data about your behavior, preferences, and personal details, which can be sold to third parties.

3. Cyberstalking and Harassment

- Personal Safety: Publicly available personal information can make users targets for cyberstalking and harassment.
- Professional Risks: Harassment on professional networks like LinkedIn can damage your professional reputation and relationships.

4. Malware and Spyware

- Malicious Links: Clicking on unverified links or downloading attachments from social media can lead to malware infections.
- Compromised Accounts: Malware can steal login credentials and other sensitive data stored on your devices.

5. Reputational Damage

- Inappropriate Content: Posts, comments, or photos shared without considering their impact can harm your personal and professional reputation.
- Misinterpretation: Content shared in a specific context might be misunderstood or taken out of context, leading to potential reputational harm.

6. Targeted Attacks

- Personalized Scams: Cybercriminals can use information gathered from social media to craft personalized attacks, making them more convincing.
- Corporate Espionage: Information shared on professional networks like LinkedIn can be used for corporate espionage or to target your company.

2. BEST PRACTICES FOR USING SOCIAL MEDIA SAFELY

1. Privacy Settings

- Adjust Settings: Regularly review and adjust the privacy settings on your social media accounts to control who can see your information and posts.
- Limit Audience: Share personal information and posts with a limited audience (friends or connections) rather than the public.

2. Be Cautious with Personal Information

- Minimal Sharing: Avoid sharing sensitive personal information such as your home address, phone number, or financial details.
- Selective Sharing: Be selective about the personal and professional information you share to minimize the risk of misuse.

3. Strong and Unique Passwords

- Password Management: Use strong, unique passwords for each social media account and consider using a password manager to keep track of them.
- Enable MFA: Enable multi-factor authentication (MFA) for an added layer of security.

4. Verify Friend and Connection Requests

- Authenticity: Only accept friend or connection requests from people you know or can verify. Be wary of fake profiles.
- Check Profiles: Review profiles and mutual connections before accepting requests.

5. Think Before You Post

- Content Consideration: Consider the potential impact and audience before sharing posts, comments, or photos.
- Professionalism: Maintain a professional demeanor on all social media platforms to protect your reputation.

6. Be Aware of Phishing and Scams

- Suspicious Links: Avoid clicking on links or downloading attachments from unknown or suspicious sources.
- Report Scams: Report any suspicious activities or scams to the social media platform.

7. Regular Account Monitoring

- Activity Log: Regularly review your account activity logs for any unauthorized access or unusual activity.
- Logout Sessions: Ensure you log out of social media accounts when not in use, especially on shared or public devices.

3. LINKEDIN-SPECIFIC SAFETY TIPS

1. Professional Profile Management

- Accurate Information: Ensure the information on your LinkedIn profile is accurate and reflects your professional identity, but avoid oversharing sensitive details.
- Public Profile Settings: Adjust your public profile settings to control what information is visible to non-connections.

2. Verify Connection Requests

- Professional Network: Only connect with people you know or who have a legitimate professional interest. Verify the authenticity of connection requests, especially from strangers.
- Personalized Messages: Use personalized messages when sending connection requests to help recipients recognize your intent.

3. Be cautious off offers

- Be cautious of opportunities that seem too good to be true. Verify the authenticity of the offer.

4. Engage Wisely

- Professional Interactions: Engage in professional discussions and comments. Avoid controversial topics that could impact your professional image.
- Group Participation: Join and participate in groups relevant to your industry but be mindful of the information you share in group discussions.

5. Control your Profile Visibility

- Adjust Visibility: Control who can see your activity feed and updates to manage your professional presence and privacy.
- Public Searches: Limit what information is available to the public through search engines by adjusting your LinkedIn profile settings.

4. IN SUMMARY

Maintaining security on social media is essential to prevent various risks such as phishing, privacy invasion, malware, and reputational damage. We encourage being active on LinkedIn but think carefully about the content you share. When in doubt contact your department head or marketing colleagues.



Together we keep InterSoft Electronics cyber secure

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