T2026_04 Risks of Oversharing Information on Social Media (April 10th, 2026)

Social media platforms have become an integral part of personal and professional communication, but oversharing information can expose individuals and organizations to significant cybersecurity risks. Employees may unintentionally disclose sensitive details such as job roles, internal processes, travel plans, system information, or organizational structure. Even seemingly harmless posts, such as photos of workspaces, badges, or events, can provide attackers with valuable intelligence.

Cybercriminals actively monitor social media to gather information for targeted attacks, a technique known as open-source intelligence (OSINT). By analyzing publicly available information, attackers can craft highly convincing phishing emails, impersonate employees or executives, or answer security questions used in account recovery processes. For example, sharing details about a recent project, system upgrade, or business trip could enable attackers to create believable pretexts for social engineering attacks.

In corporate and government environments, the impact of oversharing can include unauthorized access to systems, credential compromise, and increased risk of spear-phishing or business email compromise (BEC) attacks. Publicly available information can also assist adversaries in mapping organizational hierarchies and identifying high-value targets. Additionally, oversharing may lead to reputational damage or inadvertent disclosure of confidential or classified information.

To mitigate these risks, organizations should establish clear social media policies and provide regular security awareness training. Employees should be encouraged to limit the amount of work-related information shared online, review privacy settings on their accounts, and avoid posting sensitive details about their roles or organization. Verifying connection requests and being cautious about unknown contacts can also reduce exposure. By practicing mindful sharing and maintaining strong privacy controls, individuals can significantly reduce the risk of social media-based attacks.

References

- Cybersecurity and Infrastructure Security Agency. (2023). *Social Media and Cybersecurity Best Practices.* Retrieved from https://www.cisa.gov
- National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations (SP 800-53).* Retrieved from https://www.nist.gov
- SANS Institute. (2022). *The Risks of Social Media Oversharing.* Retrieved from https://www.sans.org
- Federal Trade Commission. (2023). *Social Media Privacy and Security Tips.* Retrieved from https://www.ftc.gov

- ENISA. (2022). *Cybersecurity Guidelines for Social Media Use.* Retrieved from https://www.enisa.europa.eu