# Lifestyle Bundle: Socializing Security Risks

Training content for everyday living you can implement with ease.

As humans, we're wired to socialize. In a world that's increasingly connected and where personal and work lines are increasingly blurred, this can open the door to scammers and social engineers seeking to exploit our desire to connect.

Social interactions can lead to information leaks through casual conversations, shoulder surfing, or unauthorized access to physical documents and devices. For instance, discussing sensitive work details in public spaces or leaving unattended devices in easily accessible areas can lead to unintended data breaches.

Online social interactions pose significant risks due to the vast amount of personal information shared on social media platforms and through various digital communication channels. Cybercriminals can craft deceptive emails or messages that appear legitimate to extract sensitive information. Oversharing on social media can provide attackers with enough data to guess passwords or answer security questions, facilitating unauthorized access to personal or business accounts.

Mitigating these risks involves adopting several practices:

- Educate individuals on the dangers of social engineering and the importance of safeguarding sensitive information.
- Use encrypted communication channels for sharing sensitive information, both online and offline.
- Limit the amount of personal and professional information shared in social settings and on social media.
- Always verify the identity of individuals requesting sensitive information, whether in person or online.
- Ensure that devices and documents are not left unattended and are securely stored.
- Keep software and systems updated with the latest security patches and use strong, unique passwords for different accounts.

By implementing these measures, individuals and organizations can reduce the risks associated with in-person and online social interactions.

**Build Your Own Socializing Security Risks Bundle**

The modules below address a wide range of issues associated with in-person and online socializing. Available in the Content Center now, just search them by number to make them part of your overall training curriculum.

**Social Media** A102A-2

Takes a closer look at popular social media scams and how to avoid them.

**Catfishing** A103A-10

Explores the motives of catfishers and how to avoid becoming a target.


**Social Engineering** A101A-4

Explores tactics scammers use to "hack the human mind" to gain access to confidential data.