Social Media Oversharing

What you share online may seem harmless, but attackers can use it to target you or your organisation. Details posted on LinkedIn, Facebook, or Instagram can provide the perfect clues for scams or password guessing.

How Attacks Happen

Personal Clues

Pet names, birthdays, anniversaries, and other personal details are often used as passwords or security questions. Criminals scan social profiles to collect this information.

Tip: *Limit how much personal detail you share online, especially in public posts.*

Privacy Gaps

Weak privacy settings can expose your posts to people outside your trusted circle. Even if you think only friends can see them, attackers may still gain access.

Tip: *Review and strengthen your privacy settings regularly.*

Travel & Absences

Posting real-time holiday or travel updates tells criminals when you are away from home or work, making you more vulnerable to scams or theft.

Tip: *Avoid posting travel updates until after you return.*

Professional Exposure

Oversharing on LinkedIn can reveal company projects, job details, or contact lists that criminals use for spear phishing or business scams.

Tip: *Keep personal and professional profiles separate and share work details cautiously.*