COMMON SOCIAL ENGINERING CYBER CRIME TACTICS & HOW TO PROTECT AGAINST THEM

PHISHING AND SMISHING: DECEPTIVE MESSAGES

HOW IT WORKS:

You receive an email (phishing) or text message (smishing) that looks legitimate. It might appear to be from IT, HR, vendors, or even colleagues. These messages are designed to create urgency or curiosity, pushing you to click a malicious link or open a harmful attachment.

ATTACKER'S GOAL:

To steal your login credentials (username and password) by directing you to a fake login page, or to install malware on your computer.

YOUR ACTION:

- **STOP. LOOK. THINK.** Does this message feel off? Was it unexpected?
- NEVER click links or open attachments in suspicious messages.
- If prompted for your username / password, do NOT enter them. Instead, navigate directly to the official website or system login page by typing the address yourself.
- Report it immediately to your agency's IT security team.

SOCIAL ENGINEERING CALLS: IMPERSONATION & MANIPULATION

HOW IT WORKS:

Criminals call our help desks, HR, or even individuals, pretending to be a colleague, a new hire, or someone from IT with an urgent problem. They are often native English speakers and highly convincing.

ATTACKER'S GOAL:

To trick our staff into resetting passwords, providing MFA codes, granting remote access, or giving away internal information. This is how they've gained initial access in many high-profile breaches.

YOUR ACTION:

- **ALWAYS verify unexpected requests for sensitive information or access.**NEVER click links or
- open attachments in suspicious messages.
- If someone calls asking for credentials or system access, hang up. Call them back on a known,
- official company number (from our internal directory), not a number they provide.
- Never bypass security procedures for an "emergency" request without independent verification.