Awareness Module 4 Cheat Sheet

by gonax133 via cheatography.com/211069/cs/45691/

Types of Social Engineering

Phishing	Deceptive emails with fake links/attachments.
Vishing	Phone/voicemail scams (“This is your bank, confirm PIN”).
Smishing	Fake texts with malicious links/apps.
Tailgating	Entering secure areas by following someone with a badge.
Piggybacking	Gaining entry when someone lets you in.
Impersonation	Pretending to be an authorized person to gain access.
Eavesdropping	Listening to private conversations.
Shoulder surfing	Watching screens/keystrokes to steal data.
Dumpster diving	Retrieving sensitive data from trash.
Physical theft	Stealing devices/documents.
Baiting	Enticing offers like free USBs or downloads hiding malware.

Defenses:
- Verify requests through official channels.
- Don’t click unknown links, open attachments, or plug in unverified USBs.
- Use privacy filters to block shoulder surfing.
- Challenge unknown people in restricted areas.
- Shred sensitive documents; securely destroy old devices.
- Encrypt hard drives/USBs; lock unattended devices.
- Be cautious with calls/texts/emails that use urgency or fear.

Multifactor Authentication (MFA)

Process of authentication that requires 2+ credentials (e.g., password + code) to keep Stronger identity verification and block unauthorized logins.

Examples
1. Password + SMS code.
2. Password + app-based push notification.
3. Password + biometric (fingerprint/face scan).

Benefit
- Protects against stolen passwords.
- Required for compliance and cyber insurance.

Cyber Concerns for MFA

Phishing	SIM Swapping	Device Cloning
Service Compromising	MFA User Fatigue	

MFA isn't foolproof. Skilled attackers use social engineering to target employees, steal credentials, and launch MFA fatigue attacks.

Virtual Private Network (VPN)

A VPN encrypts internet connections for secure data transmission, preventing unauthorized access. Organizations use VPNs for safe remote access, even on untrusted networks like public Wi-Fi.

Benefits of VPNs

Encryption and Privacy	VPNs encrypt connections to protect data, creating a secure tunnel for safe sending and receiving of data.
Access to restricted content	VPNs allow employees to securely access an organization’s network remotely from approved locations.
Protection against cyber threats	VPNs encrypt data to prevent eavesdropping and block cyber threats.

Public Wi-Fi Risks

Snooping/Eavesdropping	Others can view your activity.
Phishing/Malware	Attackers on the same network may send malware
Rogue Access Point	Fake Wi-Fi set up to steal info.

Organization Approved Softwares

Software that are vetted, patched, and supported by IT
Why use only approved?
Regular updates, reduced vulnerabilities.
Protects sensitive data (encryption, access controls)
Ensures compliance (HIPAA, GDPR, etc.)
Avoids crashes and compatibility issues.
Prevents malware from untrusted apps.
IT can provide support.

Best Practices
- Verify with IT before installing.
- Report unauthorized software immediately.
- Review policies regularly.

Cybersecurity Concerns of BYOD

System and data Security	Legal and compliance
Mixing of personal and professional life	Device compatibility
Old Software	Lack of security controls

Best Practices:

- Always check your agency’s BYOD policy.
- Encrypt personal devices (especially laptops/phones).
- Keep OS/software updated and patched.
- Separate work and personal data.
- Participate in cybersecurity awareness training.