Types of Social Engineering

Phishing	Emails that contain malicious links or attachments that will attempt to compromise systems and/or credentials.
Vishing	Phone call or voicemail where the threat actor attempts to socially engineer a victim to perform certain tasks.
Smishing	Text messages that ask victims to click a link, open an attachment, or call a number.
Tailgating	Following someone into an unauthorized area by pretending to have proper authorization or by acting to be in a hurry.
Piggyb-acking	Entering a restricted area with an authorized person through deception or unawareness of the authorized person.
Impers-onation	Pretending to be an authorized person to gain access to a restricted area.
Eavesd-ropping	Listening in on conversations to try to acquire sensitive information.
Shoulder surfing	Looking over someone's "shoulder," in their personal work area, to observe information like credentials or other sensitive information.
Dumpster diving	Searching trash for sensitive information that has been discarded.
Physical theft	Stealing physical devices, media, or documents to gain access to sensitive information.

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.

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

Defense Against Physical Social Engineering

Piggybacking & Tailgating:
1) Do not allow entry to restricted areas without proper authorization.
2) Politely challenge those trying to enter using your access.
3) Do not accept excuses for missing credentials.

Shoulder Surfing:
1) Use a privacy filter on screens.
2) Keep desks clear of sensitive documents.
3) Restrict access with badge-controlled areas.

Dumpster Diving:
1) Shred unneeded documents.
2) Securely destroy computers and physical media.
3) Ensure trash and recycling bins are secure.

Physical Theft:
1) Encrypt hard drives, USBs, and storage devices.
2) Lock away devices and documents when unattended.
3) Never leave devices unsupervised.

Impersonation:
1) Always validate identities.
2) Be prepared to ask questions to confirm authenticity.

Eavesdropping:
1) Stay aware of your surroundings.
2) Discuss sensitive data in secure locations.
3) Use headphones for virtual meetings.

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.