Tipos de Ingeniería Social

Phishing	Correos electrónicos que contienen enlaces maliciosos o archivos adjuntos que intentarán comprometer sistemas y/o credenciales.
Vishing	Llamada telefónica o mensaje de voz donde el actor de la amenaza intenta manipular socialmente a la víctima para realizar ciertas tareas.
Smishing	Mensajes de texto que piden a las víctimas hacer clic en un enlace, abrir un archivo adjunto o llamar a un número.
Acceder por seguimiento	Seguir a alguien a un área no autorizada fingiendo tener autorización o actuando como si tuviera prisa.
Acceder por engaengaño	Ingresar a un área restringida con una persona autorizada mediante engaño o sin que la persona autorizada se dé cuenta.
Impersonificacion	Fingir ser una persona autorizada para obtener acceso a un área restringida.
escuchas clandestinas	Escuchar conversaciones para tratar de adquirir información sensible.
Espionaje por encima del hombro	Mirar por encima del hombro de alguien, en su área de trabajo personal, para observar información como credenciales u otra información sensible.
Busqueda en la basura	Buscar en la basura información sensible que ha sido descartada.
Robo físico	Robar dispositivos físicos, medios o documentos para obtener acceso a información sensible.

Preocupaciones cibernéticas para MFA

Phishing	Intercambio de SIM	Clonación de dispositivos
Compromiso de servicios	Fatiga del usuario de MFA	

El MFA no es infalible. Los atacantes expertos utilizan ingeniería social para dirigirse a los empleados, robar credenciales y lanzar ataques de fatiga de MFA.

Preocupaciones de ciberseguridad del BYOD

Seguridad del sistema y los datos	Cumplimiento legal y normativo
Mezcla de vida personal y profesional	Compatibilidad de dispositivos
Software antiguo	Falta de controles de seguridad

Defensa contra la ingeniería social física

Acceder por seguimiento y engaño

1) No permitir el acceso a áreas restringidas sin la autorización adecuada.

2) Desafiar amablemente a quienes intenten entrar utilizando tu acceso.

3) No aceptar excusas por la falta de credenciales.

Shoulder Surfing:

1) Utiliza un filtro de privacidad en las pantallas.

2) Mantén los escritorios libres de documentos sensibles.

3) Restringe el acceso con áreas controladas por tarjetas de identificación.

Buscar en la basura:

1)Tritura los documentos innecesarios.

2)Destruye de manera segura computadoras y medios físicos.

3)Asegúrate de que los botes de basura y reciclaje estén asegurados.

Robo físico:

1) Cifra discos duros, USBs y dispositivos de almacenamiento.

2) Guarda los dispositivos y documentos cuando no estén en uso.

3) Nunca dejes dispositivos sin supervisión.

Suplantación de identidad:

1) Siempre valida las identidades.

2) Prepárate para hacer preguntas que confirmen la autenticidad.

Escucha secreta:

1) Mantente consciente de tu entorno.

2) Discute datos sensibles en lugares seguros.

3) Usa audífonos para reuniones virtuales.

Red Privada Virtual (VPN)

Una VPN cifra las conexiones a internet para una transmisión de datos segura, evitando el acceso no autorizado. Las organizaciones utilizan VPNs para un acceso remoto seguro, incluso en redes no confiables como Wi-Fi público.

Beneficios de las VPNs

Cifrado y privacidad	Las VPNs cifran las conexiones para proteger los datos, creando un túnel seguro para el envío y recepción seguros de la información.
Acceso a contenido restringido	Las VPNs permiten a los empleados acceder de forma segura a la red de la organización de manera remota desde ubicaciones aprobadas.
Protección contra amenazas cibernéticas	Las VPNs cifran los datos para evitar la escucha secreta y bloquear las amenazas cibernéticas.