CURSO DE INFORMACIÓN EN SEGURIDAD INFORMÁTICA

---------- SEMANA 2 HOJA DE REFERENCIA: Redes Sociales ----------

IDEAS PRINCIPALES	NOTAS
Amenazas de las redes sociales	Dos de las grandes amenazas para usted a través de las redes sociales son: Clickjacking Ingeniería Social Las redes sociales han hecho del mundo un lugar más conectado, pero todas esas conexiones también crean un acceso sin precedentes a la información de las personas y los negocios.
¿Qué es el "Clickjacking"?	El clickjacking es un método de ataque, también conocido como Redressing de la Interfaz de Usuario, porque se establece disfrazando (o corrigiendo) un enlace con una superposición que engaña al usuario para que haga algo diferente de lo que él o ella piensa.
¿Qué es la ingeniería social?	La ingeniería social es el arte de manipular a la gente para que entregue información confidencial. Los delincuentes utilizan tácticas de ingeniería social porque suele ser más fácil explotar su inclinación natural a la confianza que descubrir formas de hackear o piratear su software.
MEJORES PRÁCTICAS	
Seguridad de las redes sociales Las mejores prácticas	1. Cierre las cuentas que tenga desatendidas en las redes sociales 2. Proteja sus contraseñas • Evite el uso de información personal como la fecha de nacimiento, el nombre de la mascota, el nombre de su hijo/a, etc. como contraseñas de acceso • No use una contraseña débil. Si no puede recordar una compleja, entonces use un gestor de contraseñas • Empiece a usar la autenticación de 2 factores 3. Activar las alertas de acceso • Si habilita esta función, se le notificará por correo electrónico si se accede a su cuenta desde un nuevo dispositivo y/o ubicación 4. Proteja su computadora y su teléfono inteligente con un fuerte y actualizado software de seguridad
AUTENTIFICACIÓN DE DOS FACTORES	
¿Qué es la autenticación de dos factores?	2FA es una capa extra de seguridad que se utiliza para asegurarse de que las personas que intentan acceder a una cuenta en línea son quienes dicen ser. Primero, un usuario introducirá su nombre de usuario y una contraseña. Luego, en lugar de obtener acceso inmediato, se les pedirá que proporcionen otra información.
Este segundo factor podría provenir de una de las siguientes categorías:	Algo que usted sabe: Puede ser un número de identificación personal (PIN), una contraseña, respuestas a "preguntas secretas" o un patrón específico de pulsación de teclas. Algo que tiene: Típicamente, un usuario tendría algo en su posesión, como una tarjeta de crédito, un smartphone, o un pequeño token de hardware. Algo que es: Esta categoría es un poco más avanzada, y podría incluir el patrón biométrico de una huella dactilar, un escaneo del iris o una huella de voz.