Actividad 06. Seguridad en redes sociales

1. Busca información en Internet sobre las amenazas y vulnerabilidades existentes en el uso de las redes sociales y elabora un documento explicándolo, así como las estrategias a seguir para protegerlas
2. . Muestra también las opciones de seguridad de una red social que utilices (Instagram, TikTok, Facebook, LinkedIn, etc.)

1. Busca información en Internet sobre las amenazas y vulnerabilidades existentes en el uso de las redes sociales y elabora un documento explicándolo, así como las estrategias a seguir para protegerlas

PRINCIPALES AMENAZAS

1. ***Phishing y Estafas***.
   - **Phishing**: Engaños que quieren obtener información confidencial a través de correos o mensajes falsos que parecen verídicos. Los atacantes pueden hacer este tipo de acciones para enviar mensajes fraudulentos a través de las redes sociales.
   - **Estafas de Marca**: Suplantación de la identidad de marcas conocidas para engañar a los usuarios y así obtener información confidencial, o incluso dinero.
2. ***Malware***.
   - **Distribución de Malware**: Enlaces que son maliciosos a través de publicidad o mensajes directos que instalan software dañino en los dispositivos de las víctimas afectadas.
3. ***Cuentas Impostoras***.
   - **Creación de Cuentas Falsas**: Perfiles falsos que se hacen pasar por otros usuarios o incluso marcas para engañar a

los usuarios y así obtener información personal sensible o financiera.

4. ***Ciberacoso***.
    - **Acoso en Línea**: Conductas intimidatorias, hostigamiento o abuso a través de las redes sociales, afectando así a las personas y/o empresas.
5. ***Robo de Información***.
    - **Distribución Excesiva de la Información**: Los usuarios comparten excesiva información personal y profesional a través de las redes sociales, lo que puede ser accesible a los atacantes para realizar ataques dirigidos hacia los propios usuarios.

PRINCIPALES ESTRATEGIAS PARA PROTEGERSE DE LAS AMENAZAS

1. **Contraseñas Seguras**: Utilizar contraseñas complejas y cambiarlas regularmente (No usar la misma para diferentes cuentas).
2. **Autenticación de Dos Factores (2FA)**: Implementar Autenticación de Dos Factores para añadir una capa extra de seguridad al inicio de sesión en las cuentas de las redes sociales.
3. **Revisión de Privacidad y Configuración**: Revisar y ajustar regularmente la configuración de privacidad de las redes sociales para limitar quién puede ver y acceder a la información personal del usuario.
4. **Monitoreo y Auditorías**: Realizar auditorías periódicas de seguridad en las redes sociales, monitoreando así las actividades sospechosas y revisando los permisos de acceso.
5. **Educación y Concienciación**: Capacitar a los empleados sobre las mejores prácticas de seguridad en redes sociales, incluyendo identificación de intentos de Phishing y comportamientos sospechosos.
6. **Uso de Herramientas de Seguridad**: Utilizar herramientas de gestión y monitoreo de redes sociales como Hootsuite, ZeroFOX y BrandFort para detectar y responder rápidamente a amenazas.
7. **Políticas de Uso de Redes Sociales**: Establecer y mantener las políticas claras sobre el uso de las redes sociales dentro de la empresa, formando una cultura de respeto y seguridad.

2.. Muestra también las opciones de seguridad de una red social que utilices (Instagram, TikTok, Facebook, LinkedIn, etc.)

En el caso de una de las redes sociales que uso (TikTok), voy a explicar las funciones de seguridad y privacidad para protegernos.

Para acceder y modificar las configuraciones hay que abrir la aplicación y dirigirse a nuestro perfil, tocar el icono de los tres puntitos de la esquina superior derecha para abrir el menú de configuración, y seleccionar "**Privacidad**" o "**Seguridad**" para ajustar las opciones que deseamos.

Algunas opciones disponibles:

PRIVACIDAD DE LA CUENTA

- **Cuenta Privada**: Se puede configurar la cuenta como privada, lo que sólo las personas que se aprueben como seguidores podrán ver los vídeos.
- **Aprobar Seguidores**: Permite al usuario decidir quién puede seguir su cuenta.

GESTIÓN DE INTERACCIONES

- **Control de Comentarios**: Pueden filtrar o desactivar comentarios en los vídeos, además de establecer filtros para bloquear automáticamente los comentarios que contengan palabras específicas.
- **Mensajes Directos**: Opción para decidir con quién puede enviar mensajes directos (todos, amigos o nadie). Los menores de 16 años tienen restringido el acceso a mensajes directos por defecto
- **Dúos y Stitch**: Permite con quién puede hacer dúos o usar la función Stitch con sus vídeos (todos, amigos o nadie).

CONTROL DE CONTENIDO

- **Filtrado de Contenido**: Ofrece una opción de activar el modo restringido para limitar la aparición de contenido inapropiado en la cuenta.
- **Informar Contenido**: Pueden reportar vídeos, comentarios o cuentas que se consideren inapropiadas o que violen las normas comunitarias.

CONFIGURACIÓN DE SEGURIDAD

- **Autenticación en Dos Factores (2FA)**: Pueden activar la Autenticación en Dos Factores para añadir una capa adicional de seguridad a su cuenta.
- **Administrar Sesiones**: Opción para ver y gestionar las sesiones activas en diferentes dispositivos y cerrar las que no reconozca.

PROTECCIÓN PARA MENORES

- **Sincronización Familiar**: Permite a los padres vincular su cuenta con la de sus hijos para establecer controles de tiempo de pantalla, mensajes directos y contenido adecuado.
- **Restricciones de Edad**: TikTok aplica restricciones automáticas de funcionalidad para cuentas de usuarios menores de 16 años, limitando así las opciones como mensajería directa y la capacidad de hacer dúos.

CONFIGURACIONES DE PUBLICIDAD

- **Personalización de Anuncios**: Pueden ajustar si desean recibir anuncios personalizados basados en su actividad en TikTok.