ELEMENTOS DE SEGURIDAD EN INTERNET

En ERC La seguridad en Internet es fundamental para proteger la información y los dispositivos de posibles amenazas. A continuación, se presentan algunos conceptos y elementos clave para entender y mejorar la seguridad en línea.

CONCEPTOS GENERALES DE SEGURIDAD

1. **Confidencialidad**: Garantiza que la información solo sea accesible para personas autorizadas.

2. **Integridad:** Asegura que la información no sea modificada o alterada sin autorización.

3. **Disponibilidad:** Garantiza que la información esté disponible cuando se necesite.

4. **Seguridad de la Información**: Conjunto de medidas para proteger la confidencialidad, integridad y disponibilidad de la información.

5. **Autenticación:** Proceso que verifica la identidad de los usuarios y dispositivos.

6. **Autorización**: Proceso que determina los permisos y accesos de los usuarios y dispositivos.

ELEMENTOS DE PROTECCIÓN

1. **Firewall**: Elemento de protección que filtra el tráfico de red y bloquea accesos no autorizados.

2. **Antivirus**: Programa que detecta y elimina virus informáticos y códigos maliciosos.

3. **Antispam**: Herramienta que bloquea correos electrónicos no solicitados.

4. **Criptografía**: Técnica que cifra la información para protegerla de accesos no autorizados.

3153989810
gerencia@ercexplorer.com

5. **Redes Privadas Virtuales (VPN)**: Tecnología que crea una conexión segura y cifrada entre dos puntos de la red.

AMENAZAS TÉCNICAS DE SEGURIDAD

1. **Spam:** Correos electrónicos no solicitados que pueden contener malware o phishing.

2. **Ingeniería Social:** Técnica que manipula a las personas para obtener información confidencial.

3. **Código Malicioso:** Software o hardware que se introduce en un sistema con fines maliciosos.

4. **Hoax:** Mensaje falso o engañoso que se distribuye en cadena y puede causar problemas de seguridad.

5. **Suplantación:** Técnica que consiste en hacerse pasar por alguien o algo para obtener información confidencial.

6. **Phishing:** Técnica que consiste en engañar a los usuarios para obtener información confidencial.

7. **Vishing**: Utilización de técnicas de phishing pero para servicios asociados con voz sobre IP (VoIP).

8. **Smishing**: Utilización de técnicas de phishing en los mensajes de texto de teléfonos móviles.

¿Cómo funciona?

A través de Sitio Web: En primera instancia los atacantes crean un sitio Web similar al original, trascribiendo textos, pegando las mismas imágenes y los mismos formularios para digitar los datos. Una vez creado el sitio, lo publican en la Web con un alias parecido al sitio original.

Ejemplo: Reemplazando un simple de caracteres, usando un dominio real como prefijo:

- Sitio oficial – www.muyReal.com
- Sitios falsos:
  - www.muyReal.com.sitio.com o
    Variaciones: www.muyReal-account.com
  - www.sitioReal.actualiza.com

- Jugar con la percepción y la lectura del usuario:
  www.muuy.Real.com
  www.muy.Rea1.com
  www.muy.Real.com/bin/actualiza

Adicional a esto, fijan una imagen simulando ser un sitio seguro (con certificados digitales) que a simple vista, da mucha confianza pero son FALSOS:

Aunque en algunos casos, los atacantes adquieren un certificado original para hacer el fraude.

Una vez realizado esta labor y utilizando mecanismos masivos de comunicación como el spam, envían correos indicando a los "posibles" clientes o usuarios del portal a que actualicen sus datos, invocando la posibilidad de dar obsequios o premios si hacen esta acción.

9. **Fraude a través de Correo electrónico:** Esta modalidad es realizada enviando correos masivos a las personas solicitando informen sus datos personales, lo correos engañosos pueden indicar que existe un problema técnico y es necesario restablecer las contraseñas. Los correos llegan a nombre de una empresa o razón social, donde el atacante suplanta el nombre de dicha empresa.

¿A quién le puede pasar?

A cualquier usuario que tenga un correo electrónico y acceso a Internet, donde periódicamente haga consultas y/o actualizaciones en portales que le presten servicios.

¿Dónde está el peligro y cómo podemos ser víctimas?

El peligro radica en que, al ser una página falsa, inducen a los usuarios a que ingresen los datos personales, como cuentas de correo, número de tarjetas de crédito, claves, etc. y estos datos son recogidos por el atacante en bases de datos ajenas a las entidades oficiales de los sitios.

Al sitio Web “similar” al original, es difícil que el usuario se percate, en primera instancia, de que se trata de un engaño.

Cuando llega un correo indicando sean actualizados los datos, los usuarios validan las bondades de estar actualizados e ingresan desde el enlace o link del correo, directamente a la página falsa.

Al ser un spam “atractivo”, los usuarios hacen un reenvió de este a más usuarios, formándose una cadena o Hoax para capturar más y más personas. Y si es a través del correo, los usuarios enviarían los datos personales (usuario y contraseña) a un correo desconocido.

¿Cuáles son las consecuencias?

Una vez se ingresen los datos personales, son almacenados en bases de datos del atacante, que posteriormente utilizará en beneficio propio para realizar estafas, suplantaciones o robos de dinero, dado que éste atacante posee las claves de acceso a los sistemas y servicios.

¿Cómo se puede evitar?

Siempre que llegue este tipo de mensajes, ingrese directamente al sitio oficial desde el browser o navegador, nunca desde el enlace link enunciado en el correo, ni dando clic a dicho enlace.

Evite el envío de mensajes cadena, pornografía, mensajes no solicitados, bromas a otros remitentes de correo. Cuando ingrese al sitio, valide que la seguridad que se indica a través de certificados digitales, si estén respaldados, de doble clic el icono de seguridad, que debe estar ubicado en la parte inferior derecha del navegador (no dentro de la página).

3153989810
gerencia@ercexplorer.com

Ejemplo:

Conozca de antemano cual es la dirección o URL del sitio real y valide este nombre cada que ingrese a realizar un proceso donde deba ingresar sus datos. Recuerde que el atacante utiliza técnicas que pueden engañar la percepción del sitio cuando se lee.

Si usted es un usuario frecuente de portales donde se ingresan datos personales, manténgase actualizado, consultando en la página de la policía nacional (http://www.policia.gov.co/), CAI virtual, los últimos eventos, recomendaciones y consultas en línea.

CONSEJOS PARA MEJORAR LA SEGURIDAD

1. Utiliza contraseñas fuertes y únicas para cada cuenta en línea.
2. Mantén actualizado tu sistema operativo, navegador y software de seguridad.
3. Utiliza herramientas de seguridad como firewall, antivirus y antispam.
4. Sé cauteloso con los enlaces y archivos adjuntos en correos electrónicos desconocidos.
5. Utiliza la autenticación de dos factores siempre que sea posible.
6. Realiza copias de seguridad de tus datos importantes
7. Pornografía Infantil**:** Evite Alojar, publicar o trasmitir información, mensajes, gráficos, dibujos, archivos de sonido, imágenes, fotografías, grabaciones o software que en forma indirecta o directa se encuentren actividades sexuales con menores de edad, en los términos de la legislación internacional o nacional, tales como la Ley 679 de 2001 y el Decreto 1524 de 2002 o aquella que la aclare, modifique o adicione o todas las leyes que lo prohíban.
8. No publique su cuenta de correo en sitios no confiables.

BENEFICIOS DE IMPLEMENTAR MEDIDAS DE SEGURIDAD

- **Protección de la información:** Evita la pérdida o robo de información confidencial.

- **Prevención de ataques**: Reduce el riesgo de ataques cibernéticos y malware.

- **Mejora de la confianza:** Aumenta la confianza en la seguridad de la información y los sistemas.

- **Reducción de riesgos**: Minimiza los riesgos asociados con la seguridad en línea.

CONCLUSIÓN

La seguridad en Internet es un tema importante que requiere atención y medidas proactivas para proteger la información y los dispositivos. Al entender los conceptos y elementos de seguridad, puedes tomar medidas efectivas para mejorar la seguridad en línea y reducir los riesgos asociados.

NUESTRO COMPROMISO CON LA SEGURIDAD

En ERC Explorer, nos comprometemos a proteger la seguridad y privacidad de nuestros clientes en línea. Nuestro objetivo es proporcionar una experiencia en Internet segura y confiable, y estamos dedicados a ayudar a nuestros clientes a navegar en un entorno en línea cada vez más complejo y dinámico.

3153989810
gerencia@ercexplorer.com