1. Introducción a la Ciberseguridad

La ciberseguridad es el arte de proteger redes, dispositivos y datos del acceso ilegal a estos, así como también de asegurar la confidencialidad, integridad y disponibilidad de la información. Mucha información personal está almacenada en nuestra computadora, smartphone o tablet. Saber cómo proteger esta información es importante, no solo para individuos particulares sino también para organizaciones. Cada vez que utilizamos el internet nos encontramos con decisiones relacionadas a nuestra seguridad. Nuestra seguridad y la de la nación dependen de la toma de decisiones digitales responsable. Hacer del internet un lugar seguro requiere que todos seamos responsables de nuestro propio manejo de los principios de la ciberseguridad.

Algunos fundamentos de la ciberseguridad

- **Pensar antes de hacer click: Reconocer y Reportar el Phishing:** Si un URL se ve un poco extraño, se debe pensar antes de hacer click. Puede ser un intento de obtener información sensible o instalar software malicioso.
- **Actualizar el software**: Al recibir una notificación de actualización de software, se debe actuar rápidamente. Activar las actualizaciones automáticas puede ser incluso mejor.
- **Utilizar contraseñas seguras:** Es recomendable utilizar contraseñas que sean largas, únicas y generadas aleatoriamente. También es recomendable utilizar administradores de contraseñas para generar y recordar contraseñas diferentes y complejas para cada una de nuestras cuentas. Un administrador de contraseñas las encriptará, asegurándolas por nosotros.
- **Activar la autenticación de múltiples factores (AMF):** Se necesita más que una contraseña para proteger nuestras cuentas en línea, y activar la AMF nos hace significativamente menos propensos a ser hackeados.

Posibles amenazas

- **Software malicioso**: Una computadora o la información que contiene puede ser dañada por código malicioso (también conocido como malware). Un programa malicioso puede ser un virus, un "worm" o un troyano. Los hackers y atacantes usualmente aprovechan estas fallas en el software para obtener dinero.
- **Robo de identidad y estafas**: El robo de identidad y las estafas son crímenes de oportunidad, e incluso aquellas personas que nunca utilizan computadoras podrían ser víctimas. Existen diversas maneras en las que los criminales pueden acceder a nuestra información, incluyendo el robo de billeteras, escuchar una llamada, inspeccionar la basura, o agarrar un boleto de compra que contenga un número de cuenta.
- **Phishing**: Los ataques de phishing utilizan emails, mensajes de texto y sitios maliciosos que parecen ser confiables - como organizaciones de caridad o tiendas virtuales - para obtener información personal del usuario. *El phishing es conocido en español como "la técnica de suplantación de la identidad".*

Cómo nos persuaden los criminales

El phishing es una de las formas más comunes de estafas cibernéticas que los usuarios son propensos a encontrar. La clave está en que tanto emails como mensajes de texto deben provenir de una fuente confiable. Hay que saber a qué estar atento - aquí hay algunos ejemplos de phishing que podrían encontrarse en un email con fines persuasivos:

"Sospechamos que una transacción no autorizada fue realizada desde tu cuenta. Para asegurar que tu cuenta no haya sido comprometida, por favor haz click en el link de abajo y confirma tu identidad."

"No pudimos verificar tu identidad durante nuestra verificación regular de cuentas. Por favor, haz click aquí para actualizar y verificar tu información."

2. Por qué la ciberseguridad es importante y cómo aplicarla

La ciberseguridad es el arte de proteger redes, dispositivos y datos del acceso ilegal a estos, así como también de asegurar la confidencialidad, integridad y disponibilidad de la información. Mucha información personal está almacenada en nuestra computadora, smartphone, tablet, otros dispositivos inteligentes, o aplicaciones como Alexa, relojes inteligentes, etc. Saber cómo proteger esta información es importante, no solo para individuos particulares sino también para organizaciones.

El propósito de la ciberseguridad es mantener la confidencialidad, integridad y disponibilidad de los datos.

- **Confidencialidad**: Asegura que los datos sean accesibles solo para aquellos que los necesitan - una vez que se publica información en el internet, esta queda ahí para siempre.
- **Integridad**: Asegura que los datos sean concisos- los datos corruptos no poseen valor para aquellos que los necesitan.
- **Disponibilidad**: Asegura que los datos puedan ser accesibles para todos aquellos que los necesiten, cuando los necesiten - una conectividad rápida y confiable hace que los sistemas informáticos operen con mayor efectividad.

Los atacantes aprovechan vulnerabilidades usando una variedad de ataques de phishing para comprometer la seguridad de las redes y los dispositivos. Para proteger una red, es vital familiarizarse con lo esencial:

- Los atacantes pueden obtener información sobre la identidad de la víctima robando sus credenciales comprometidas.
- Los criminales crean nuevas cuentas de email y hackean cuentas existentes para orquestar ataques de ingeniería social. Un ataque de ingeniería social es cuando un atacante utiliza la interacción social para obtener o comprometer información acerca de una organización o sus sistemas informáticos.
- Los emails de phishing contienen malware y archivos adjuntos maliciosos.
- El software malicioso aprovecha varias vulnerabilidades comunes en el software y otras aplicaciones.

Conocer los fundamentos de la ciberseguridad

- **Proteger la información personal**. Si los atacantes poseen detalles importantes sobre nuestra vida, profesión, fecha de nacimiento y nombre completo - que pudieron haber sido compartidos en línea - entonces pueden intentar un ataque de phishing contra nosotros. Los cibercriminales también pueden tratar de manipularnos para omitir protocolos normales de seguridad.

- **Ser precavido con los links o archivos adjuntos de fuentes sospechosas o desconocidas**. Los links en los emails deben ser inspeccionados. Se puede pasar el ratón por encima de los links para verificar su procedencia. Al realizar una transacción, hay que asegurarse de que los URL empiecen con "https". La "s" añadida al final indica que la encriptación para proteger la información de los usuarios está activada.

- **Utilizar antivirus y mantenerlo actualizado**. Esta es una medida de seguridad importante hacia cibercriminales y amenazas maliciosas, ya que los antivirus pueden detectar, poner en cuarentena y remover software malicioso automáticamente. También es recomendable activar las actualizaciones automáticas acerca de virus para asegurar la máxima protección hacia las amenazas más recientes.

- **Utilizar contraseñas largas, aleatorias y únicas**. Crear contraseñas seguras es vital para nuestra ciberseguridad. Deben utilizarse contraseñas diferentes, así como también frases de contraseña para programas y dispositivos diferentes. Siempre utilizar contraseñas seguras de 12 o más caracteres.

- **Utilizar un administrador de contraseñas para almacenar contraseñas personales de cada cuenta**. Esta herramienta es usada comúnmente para generar contraseñas largas, aleatorias y únicas para aplicaciones web. Una vez generadas, son puestas en una bóveda centralizada y encriptadas con una contraseña maestra.

- **Fortalecer la protección de inicio de sesión**. Activar la autenticación de múltiples factores para asegurar que seamos la única persona que tiene acceso a nuestra cuenta. Usar esta autenticación para el email, procesos bancarios, redes sociales y cualquier otro servicio protegido por contraseñas. Si la AMF está disponible, puede ser activada usando un dispositivo móvil de confianza, como nuestro smartphone, una aplicación de autenticación o un token de seguridad (un dispositivo físico pequeño que pueda engancharse a nuestro llavero).

- **Realizar copias de seguridad de nuestros datos**. Periódicamente, es importante realizar una copia de seguridad en todas nuestras computadoras y asegurarnos de que la copia esté almacenada fuera de línea. Pueden hacerse copias de documentos, bases de datos, planillas, archivos financieros, archivos de recursos humanos, archivos de cuentas de recibo y de pago, y más.

- **Controlar el acceso físico**. Es importante prevenir el acceso de individuos no autorizados a todas las copias de seguridad. Asegurarse de usar cuentas de usuario separadas para cada empleado y exigir contraseñas seguras. Los privilegios administrativos deben entregarse únicamente al personal informático de confianza.

Qué tener en cuenta

- **Mantenerse alerta ante el phishing**. El phishing permite a los cibercriminales recolectar información para realizar compras no autorizadas u obtener acceso a un sistema protegido. Siempre verificar la dirección de email del remitente para asegurar su autenticidad. Muchos emails de phishing intentan crear una sensación de urgencia, haciendo que el destinatario piense que su cuenta está en peligro. Si se sospecha que un email es fraudulento, es posible comunicarse con la compañía o persona directamente en una plataforma diferente y segura.

- **Ser consciente de los riesgos**. Además del software malicioso y los virus de phishing, la amenaza de seguridad número uno es el ransomware. El ransomware es una forma de software malicioso diseñado para encriptar archivos en cualquier dispositivo, haciendo que cualquier archivo - y los sistemas que dependen de ellos - queden inutilizados.
(En español, el ransomware es conocido como “secuestro de datos”).

- ***(Si se forma parte de una organización)*** **Regularmente educar a los empleados acerca de los fundamentos de la ciberseguridad**. Para los negocios pequeños, los empleados y los emails son la causa principal de violación y filtrado de datos, ya que son un camino directo hacia los sistemas internos.