Seguridad en Internet

Seguridad, privacidad, riesgos que se tienen en Internet y cómo preverlos

Escuela normal de Cuautitlán Izcalli

Tecnologías Digitales para el Aprendizaje y la Enseñanza

LEPRE Primero 3

López Camacho Mariana

Contenido

Seguridad en Internet

La seguridad en Internet es una rama de la seguridad informática que se dedica a identificar y prevenir todas las amenazas que afectan a la red de redes. Básicamente internet se usa para el intercambio de información, información que puede estar en riesgo. Entre los peligros más habituales que afectan a usuarios y páginas web destacan: Robo de datos: bancarios, personales, etc…

- Virus
- Pishing (robo de identidad)
- Ataques DDoS: los ataques DDoS consisten en hacer un gran número de peticiones a una web en un corto espacio de tiempo para hacer que ésta se caiga.
- Spam
- Como ves son varias las amenazas a las que nos enfrentamos cuando navegamos por internet. Por suerte, hay formas de protegerse de ellas.

Medidas de privacidad y seguridad en internet

Antivirus: La primera medida de seguridad básica en internet es contar con un antivirus. Son el primer filtro de protección contra amenazas y existen soluciones gratuitas bastante interesantes. Cualquier dispositivo con conexión debe contar con la protección de un antivirus, y eso incluye a tablets y smartphones.

Contraseñas: Las contraseñas son otra de las brechas de seguridad que hay que controlar. Seguramente tengas cuenta en Google, Facebook o Twitter, por citar algunos servicios conocidos. Pero si sientes la tentación de usar siempre la misma contraseña por comodidad, piénsalo dos veces porque es lo contrario que recomiendan los expertos en seguridad informática. Además, de tener una contraseña diferente para cada cosa, éstas deben ser lo bastante seguras y difíciles de adivinar.

Seguridad de datos: Si eres el responsable de una clínica, debes asegurarte de que la información de tus pacientes esté completamente a salvo. C

Navegación: La seguridad navegando por Internet es en gran medida cuestión de sentido común. Entre los consejos habituales está evitar las páginas webs sospechosas (la mayoría de los antivirus detectan este tipo de virus). Las webs seguras cuentan con un certificado SSL, lo que significa que la url de la web llevará un https en vez de un http. (Marqués, 2023)

Riesgos en internet.

Cuando navegas por Internet puedes encontrarte con diferentes situaciones que ponen en peligro tu seguridad y privacidad en la red. El primer paso para prevenirlas es conocerlas para poder identificarlas y evitarlas. Por ello, en este artículo te explicamos de forma sencilla cuáles son los principales riesgos que debes tener en cuenta cuando haces uso de Internet.

Ataques DDoS[1]

Se trata de un ataque a un servidor desde diferentes equipos al mismo tiempo, lo que provoca un colapso en su tráfico y, por tanto, que deje de funcionar. En otras palabras, podría entenderse como una sobrecarga al sistema que impide que las personas interesadas lleguen a su destino.

A pesar de que es una amenaza que no suele ir dirigida a personas concretas, suele utilizarse para bloquear páginas web o servicios online de cualquier empresa u organización y molestar así a las personas que las utilizan.

[1] Estas siglas significan Distributed Denial of Service y se traduciría como “ataque distribuido denegación del servicio”.

Phishing[2]

Suplantan la identidad de ciertas entidades, como bancos, agencias tributarias o compañías energéticas empleando diferentes medios: una llamada telefónica, un mensaje de texto, a través de una página web falsa o también por redes sociales. Aunque el más frecuente es el correo electrónico.

Básicamente te llega un mensaje al buzón de entrada que a primera vista parece normal, pero en realidad contiene un enlace malicioso. Suele ir acompañado de unos asuntos llamativos como “Alerta de seguridad”, “Nuevos gastos detectados”, “Factura vencida” o similares que incitan a abrirlos y clicar en dichos enlaces que, automáticamente, descargan un archivo infectado.

Robo de datos

En relación al riesgo anterior, existen también los ataques a las bases de datos para recopilar información muy variada: nombres, números de teléfono, correos electrónicos, números de cuenta, direcciones, contraseñas, etc.

Pero el principal propósito de esta ofensiva es usurpar información financiera o datos corporativos a clientes o empresas.

---

[2] Es un concepto que proviene de la palabra inglesa fishing (pesca), dado que se refiere a cuando un o una ciberdelincuente navega por Internet intentando “pescar” información confidencial de internautas que “muerden el anzuelo”.

El modus operandi más destacado consiste en una inyección SQL[3] que no solo permite tener acceso a datos sensibles de una base de datos, sino que también los destruye, aprovechando las posibles vulnerabilidades existentes de una página web.

Spam

Se le conoce también como “correo basura” o “correo no deseado”. Y es que se trata de mensajes que se envían de forma masiva por un remitente anónimo o desconocido y que la persona destinataria no ha solicitado.

En la mayoría de los casos se trata de campañas publicitarias y promociones, aunque actualmente la Ley de Protección de Datos prohíbe expresamente a las empresas enviar correos no autorizados.

Ahora probablemente te estarás preguntando ¿y cómo es posible que siga recibiendo spam? Principalmente porque muchas veces se autorizan comunicaciones comerciales sin ser conscientes de ello o bien porque hay ciberdelincuentes cuyo objetivo es infectar los dispositivos de los internautas.

Virus informático

Este tipo de malware está diseñado para provocar daños en un equipo, corrompiendo sus archivos, destruyendo datos o alterando su funcionamiento habitual. Son muy contagiosos ya que se replican automáticamente sin el consentimiento de las personas usuarias.

[3] (Structured Query Language)

Las formas más comunes de propagación de los virus informáticos son las siguientes, normalmente mediante la descarga de archivos adjuntos:

- Al abrir una imagen, que introduce el virus cuando el dispositivo la procesa.

- Cuando se reproduce un vídeo, mientras se está visualizando.

- Con una notificación que llega a través de un sitio web malicioso.

- A través de un enlace que, al clicar sobre él, redirecciona a una web fraudulenta que descarga el virus. (Agencia digital de Andalucía, 2022)

Privacidad en Internet

Recientemente nos hemos encontrado ante la necesidad de trabajar, socializar, estudiar o comprar desde casa a través de un entorno virtual con aplicaciones y plataformas en línea, pero esto ha llevado también a los cibercriminales a aprovecharse de la situación, evolucionando y explotando técnicas para delinquir.

Es así como debemos adoptar en mayor medida prácticas de seguridad para proteger, entre otras cosas, la información que intercambiamos, compartimos, enviamos y para lograr dicho fin, debemos considerar un aspecto importante como es la privacidad de este activo esencial.

Recomendaciones.

Para proteger la información recomendamos poner en práctica algunas técnicas y medidas de privacidad:

- Utiliza aplicaciones de mensajería instantánea y para envío e intercambio de archivos con tecnología de cifrado de extremo a extremo con esto evitamos la interceptación de archivos y comunicaciones.

- Protege archivos que contengan información sensible o confidencial con contraseñas, puedes incluso configurarlos como “sólo lectura”.

- Implementa un método de protección para navegar en internet, como una aplicación de anonimato con la cual podrás proteger tu privacidad en el ciberespacio.

- Puedes hacer uso de programas para cifrar unidades de almacenamiento como una unidad de disco duro u otros dispositivos móviles.

- Presta atención a las condiciones de uso de los servicios digitales como correo electrónico, redes sociales, entre otros, y no des ninguna información y dato que no quieras dar.

- Actualiza tus aplicaciones y sistemas operativos de tus dispositivos con acceso a Internet.

- Crea contraseñas seguras y actualízalas periódicamente.

- Cierra siempre las sesiones (Si utilizas un dispositivo que no es el tuyo, acuérdate siempre de cerrar sesiones una vez hayas acabado) (Guardia Nacional CERT-MX, 2023)

Mi Conclusión

En conclusión, la seguridad en Internet es una preocupación constante debido a la diversidad de amenazas que enfrentamos al navegar por la red. Desde el robo de datos y ataques DDoS hasta el phishing, spam y virus informáticos, la privacidad y la integridad de la información están constantemente en riesgo. Sin embargo, la información proporciona un conjunto de medidas de seguridad que los usuarios podemos adoptar para protegernos.

La instalación de un antivirus, la gestión cuidadosa de contraseñas, la atención a la seguridad de los datos y la navegación consciente son prácticas esenciales. Además, se destaca la importancia de estar al tanto de los riesgos específicos y adoptar medidas preventivas adecuadas, como el uso de aplicaciones de mensajería con cifrado de extremo a extremo y la protección de archivos confidenciales con contraseñas.

La evolución de la tecnología y la dependencia actual de plataformas en línea destacan la necesidad de prácticas de seguridad. La privacidad en Internet se ha vuelto crucial, especialmente en un entorno donde el trabajo, el estudio y las interacciones sociales ocurren cada vez más en línea. Adoptar medidas como el cifrado de unidades de almacenamiento, prestar atención a las condiciones de uso de servicios digitales y mantener actualizados los sistemas operativos son pasos esenciales para salvaguardar la privacidad en el ciberespacio.

En última instancia, la conciencia y la aplicación de estas medidas de seguridad son fundamentales para reducir los riesgos en Internet y garantizar una experiencia en línea más segura y protegida.

Bibliografía

Agencia digital de Andalucía. (13 de octubre de 2022). *Andalucía Vuela*. Obtenido de Andalucía Vuela: https://andaluciavuela.es/noticias/los-cinco-riesgos-mas-comunes-que-te-puedes-encontrar-en-internet/

Guardia Nacional CERT-MX. (15 de febrero de 2023). *DIRECCIÓN GENERAL CIENTÍFICA - CERT-MX*. Obtenido de DIRECCIÓN GENERAL CIENTÍFICA - CERT-MX: https://www.gob.mx/gncertmx/articulos/105225

Marqués, F. L. (6 de Febrero de 2023). *Clinic Club*. Obtenido de Clinic Club: https://clinic-cloud.com/blog/seguridad-en-internet-que-es-medidas/