Investigación de ciberseguridad

Equipo: The Unwanted

Ana Laura Arrieta

Ainé Fernández

Victor Emiliano Mayen

Ian Oswaldo Carbajal

Alejandro César Moya

Investigación Ciberseguridad

1. **Riesgos Socio-Emocionales:**

El 70% de los mexicanos usan internet y los principales usuarios son adolescentes y jóvenes como tú. Tan solo entre el 80 y 94% de los jóvenes de 12 a 17 años, tienen acceso a internet o una computadora. Internet es un lugar buenísimo para encontrar información, chatear, estar en contacto con las personas que quieres, seguir con tus estudios y también encontrar mucho contenido para divertirte. Lo malo es que internet también representa riesgos, por ejemplo, según algunas encuestas nacionales, 25% de las y los adolescentes de entre 12 y 17 años ha vivido alguna forma de ciberacoso en México. Además del ciberacoso, estamos sujetos a otros riesgos como el robo de información, las noticias falsas y el sexting sin medidas de seguridad.

Cuando navegas en internet, redes sociales y otras aplicaciones tienes que preocuparte por implementar mecanismos de seguridad para evitar robos de información, de identidad, pérdidas de datos y otros múltiples riesgos. Malware es un código malicioso diseñado para infiltrarse en tu dispositivo cuando lo instalas o descargas, aunque no necesariamente te das cuenta. Cuando hay uno en tu computadora, teléfono o tableta, puede:

- Acceder a toda tu información, incluyendo ubicación en tiempo real y lista de contactos.
- Acceder a tus fotos y archivos y publicarlos en internet o en páginas maliciosas y tu ni en cuenta.
- Hackear contraseñas, email, redes sociales y demás.

Hay algunas prácticas que hacen que sea más sencillo que tu dispositivo adquiera un *malware*, a veces son acciones tan cotidianas que no nos damos cuenta de que pueden ser riesgosas. Además del *malware* que puede robar tus datos, tú mismo/a puedes ponerte en riesgo al compartir información personal con otras personas y ser susceptible al robo de identidad. Por ejemplo, al tener las redes sociales públicas te expones riesgos como, suplantación de la identidad, ciberbullying, extorsión cibernética, grooming, robo de datos y más.

Sexting:

El sexting es una práctica que ha aumentado en los últimos años, sobre todo en preadolescentes, aunque se da en todas las edades. Es una práctica que conlleva riesgos, ya que se utilizan datos personales, tanto en texto como en fotos y vídeos. Un reciente análisis publicado en la revista JAMA Pediatrics, reveló que una parte considerable de la juventud, sobre todo menores de 18 años, practica sexting.

En la actualidad, la mayoría de niños y jóvenes tienen móviles con acceso a internet u ordenadores sin control parental, por lo tanto, al navegar por internet no siempre lo hacen en páginas seguras ni conocidas, exponiéndose al peligro de lo que esto significa. Muchos jóvenes y niños practican **sexting** por diversión o porque saben que los adultos lo hacen, sin saber que podrían ser víctimas de otras personas que, con malas intenciones, podrían captarlos y conseguir que lo hagan sin consentimiento.

Aquí ya estamos hablando del **Grooming**, que consiste en establecer lazos de amistad con un niño o niña, de manera deliberada por parte de un adulto, para obtener satisfacción sexual por medio de fotos o vídeos del menor. Esto es lo que se llama pederastia y es un grave problema sobre la seguridad de los menores en internet. Esto lleva a otro problema, la **sextorsión** o chantaje sexual que se da en todas las edades y se combate con menos herramientas y más miedos, sobre todo en los más inmaduros emocionalmente.

Los **ciberdelincuentes** que realizan dichas sextorsiones juegan con la vergüenza y la culpa de la víctima para chantajearla y conseguir que haga lo que ellos le piden a cambio de no contar nada de lo sucedido. Lo que obviamente no se cumple y ya estaríamos hablando de **ciberacoso** o **ciberbullying.**

Ciberacoso:

Ciberacoso es acoso o intimidación por medio de las tecnologías digitales. Puede ocurrir en las redes sociales, las plataformas de mensajería, las plataformas de juegos y los teléfonos móviles. Es un comportamiento que se repite y que busca atemorizar, enfadar o humillar a otras personas. Por ejemplo:

- Difundir mentiras o publicar fotografías vergonzosas de alguien en las redes sociales.
- Enviar mensajes hirientes o amenazas a través de las plataformas de mensajería.
- Hacerse pasar por otra persona y enviar mensajes agresivos en nombre de dicha persona.

El acoso cara a cara y el ciberacoso ocurren juntos a menudo. Pero el ciberacoso deja una huella digital; es decir, un registro que puede servir de prueba para ayudar a detener el abuso.

Ciberbullying

Ciberbullying es un término que se utiliza para describir cuando un niño o adolescente es molestado, amenazado, acosado, humillado, avergonzado o abusado por otro niño o adolescente, a través de Internet o cualquier medio de

comunicación como teléfonos móviles o tablets. Se caracteriza por que el acoso se da entre dos iguales, en este caso, menores.

Es importante distinguirlo, ya que existen otras prácticas en la que se involucran adultos y que se denominan simplemente ciberacoso o acoso cibernético, con las consecuencias legales que tienen los actos de un mayor de edad en contra de un menor.

El ciberbullying no es algo que ocurra una sola vez y además se presenta de distintas formas, desde insultos, discriminación o burla sobre características físicas, forma de vestir, gustos, hacer pública información o fotografías que avergüenzan a la víctima, robo de identidad y suplantación, hasta amenazas de daño físico y otros cargos que pueden ser tipificados como delincuencia juvenil.

Extorsión cibernética:

El envío de un correo electrónico, o de un programa de software para hacer llegar a una víctima potencial, un engaño o amenaza, con indicaciones precisas para realizar un envío o depósito de dinero, se ubican dentro de los tipos de delitos a distancia que, en la mayoría de los casos, suelen ser simples intentos de fraude pero que, en muchos otros, se convierten en verdaderas extorsiones. Este tipo de delitos surgen al presentarse fugas de información en bases de datos, que son utilizadas por delincuentes cibernéticos y que, usurpando la identidad principalmente de bancos o comercios, contactan a *"sus clientes"*, haciéndoles llegar alguna promoción irresistible o bien, indicando que su cuenta presenta un problema y requiere alguna acción de su parte. Si la víctima cae en el engaño contestando alguno de estos correos, estableciendo así contacto con el delincuente, de no lograr éste sus fines fraudulentos mediante el pago de productos o servicios o el robo de datos de tarjetas bancarias, procederá con intimidaciones y amenazas, intentando entonces extorsionar a la víctima a toda costa. En otra modalidad, con un software especializado, los criminales roban cuentas de correo electrónico o de redes sociales con el fin de obtener información sensible de la víctima para exigirle dinero a cambio de no ser utilizada en su contra o divulgada. Los delincuentes cibernéticos, asimismo, logran mediante la implantación de un código malicioso *'ransomware'*, al visitar la víctima sitios fraudulentos o abrir correos electrónicos, acceder a su computadora para bloquearla o encriptar remotamente archivos o programas y, para su liberación, exigen el pago de un rescate.

2. Redes sociales:

Las redes sociales forman una parte central de la vida de los estudiantes, la mayoría empieza usarlas para uso personal, pero también existe el potencial de hacer uso de ellas como un apoyo para sus estudios profesionales. Los beneficios de usar redes sociales en sus estudios pueden ser: email, mensajes instantáneos, videoconferencias, descarga de documentos, comunicación profesor alumno, plataformas de colaboración como Google Drive. Sin embargo, los estudiantes tienden a preferir la educación presencial porque sienten que las redes sociales le quitan el factor humano a la educación el que consideran importante.
Los estudiantes no suelen usar las mismas redes sociales para usos educativos que las que usan de manera personal, pero al momento de coordinar y ponerse de acuerdo para trabajos en equipo algunos si usan las mismas redes sociales, que les permiten hacer preguntas cortas y recibir respuestas rápidamente por medio de mensajes instantáneos. Aunque varios estudiantes reconocen los beneficios de tener las redes sociales como un apoyo para sus estudios, muchos no usan tanto las redes sociales para su educación como lo hacen para su uso personal. Muchos también las ven como un complemento, pero nunca dejarían que se convirtiera en el 100% de su educación.

Uno de los grandes inconvenientes de Internet y en especial de las redes sociales es la facilidad con la que información privada o confidencial puede hacerse pública o caer en malas manos. Desde datos tan simples como la ubicación (registrada por el teléfono celular o cualquier aparato dotado de un GPS), edad, dirección de nuestro trabajo, escuela u hogar, hasta otros mucho más sensibles como el número de nuestra tarjeta de crédito (o la de nuestros padres), nuestro número telefónico o de cuenta bancaria, todos pueden ser interceptados.

El robo de información pueden realizarlos hackers o usuarios inescrupulosos que se hacen pasar por amigos, o bien interceptan mensajes destinados a terceros. En otros casos, la información se obtiene a través de campañas fraudulentas de venta, donación u ofertas engañosas.

Algo semejante ocurre con el material íntimo (como fotografías de desnudos o mensajes eróticos), que si bien está destinado a un usuario concreto y no a divulgarse libremente, puede hacerse público o venderse en páginas de pornografía, sin el consentimiento de quien los emitió, creyéndose a salvo en la privacidad de un mensaje directo.

El consejo general para evitar estas situaciones es administrar la información privada con un criterio de alerta: saber que nuestra información puede ser empleada con fines nocivos, y que no todo el que emplea las redes sociales lo hace con el mismo fin. No aceptar solicitudes de ningún tipo de personas extrañas o misteriosas, ni brindar nunca información sensible en respuesta a ofertas que parezcan

demasiado buenas para ser verdad. Borrar la información privada sensible o encriptarla detrás de contraseñas seguras, que deberán renovarse cada cierto tiempo.

En el caso de los menores de edad, es necesario instruirlos al respecto y enseñarles que, si bien parecen un lugar seguro, las redes sociales son tan peligrosas como una calle solitaria o la plaza.

3. Amenazas en redes sociales

Phishing:
Phishing es una técnica usada por los ciberdelincuentes por medio de la cual engañan a usuarios para dar click en un link que les permite a los atacantes descargar viruses o *malware* en el dispositivo del usuario, sabotear sistemas o robar datos y dinero. Phishing se hace por medio de emails, redes sociales o teléfono aunque el término phishing se usa mayoritariamente para los ataques que llegan por email.
Esta técnica es muy usada en redes sociales como Instagram, con la que los atacantes crean cuentas falsas para aparentar ser cuentas oficiales y verificadas y así enviar mensajes directos a usuarios, engañarlos para que descarguen un archivo. Estas estafas también se pueden dar en *giveaways* o correos que dicen ser de parte de Instagram donde le piden al usuario datos personales innecesarios como datos bancarios. Una capa de seguridad extra que pueden tomar los usuarios de Instagram para protegerse del phishing es la autenticación en dos pasos (VF2) que les permite a los usuarios proteger sus cuentas digitales en caso de que su contraseña sea comprometida. Esta funciona cuando el usuario intenta acceder a su cuenta con usuario y contraseña, además le pedirá un código de verificación que le llegará por medio de SMS, correo electrónico o a través de una app.

Spoofing:
Correo electrónico falsificado: los correos electrónicos que contienen un virus informático se envían desde direcciones de correo electrónico existentes, con el fin de engañar mejor al destinatario. De este modo, este último propagará involuntariamente el virus cuando se abra el correo. El hacker puede entonces extraer datos personales o incluso controlar remotamente el ordenador.
El spoofing IP es el proceso de envío de paquetes IP desde una dirección IP de origen que no ha sido asignada al ordenador que los envía.
Smart-spoofing: permite utilizar cualquier aplicación cliente gracias a la usurpación de una dirección IP. Esto evita las reglas de seguridad de la red. Esta técnica, si se combina con la traducción de direcciones, puede incluso neutralizar los cortafuegos.

4. E-commerce:

Por la pandemia del COVID-19 muchos consumidores decidieron comprar en línea, ya que es más seguro y fácil en las circunstancias actuales. Debido a esto las

compras en línea han crecido a un ritmo acelerado por lo que muchos se preguntan si es seguro comprar online. El *e-commerce* siempre ha sido el blanco más buscado por los ciberdelincuentes y el reciente aumento en este tipo de ventas hizo que se volviera todavía más atractivo para los cibercriminales debido a que los datos personales se han convertido en uno de los activos más valiosos.
Tanto las tiendas en línea como los clientes son afectados por los riesgos de ciberseguridad de las compras en línea. Para comprar algo, los clientes tienen que proporcionar sus datos personales a la tienda, tienen que confiarle su información de tarjeta de crédito, su email, usuarios y contraseñas etc. Los cibercriminales pueden robar esta información de las bases de datos de la tienda para ganar dinero, cuando esto ocurre puede dañar severamente la reputación de la compañía.
Se recomienda checar si la tienda en línea es legítima antes de comprar, ya que algunas páginas de internet pueden ser falsas, una forma de hacerlo es checar los comentarios y el *feedback* de otros clientes u organizaciones confiables.
También se recomienda usar una tarjeta de créditos para comprar en línea, si es posible, ya que la mayoría de los proveedores de crédito protegen las compras en líneas y están obligadas a dar una devolución en ciertas circunstancias, también al usar una tarjeta de crédito si los datos de pago son robados la cuenta bancaria no será afectada directamente. Al hacer compras en línea con tarjetas de débito pueden no estar tan protegidas como las de tarjetas de crédito. Otra opción de pago para compras en línea es la de plataformas de pago en línea como PayPal, Apple Pay, Google Pay, etc. Al usar estas plataformas para autorizar los pagos, la tienda no tiene acceso a los datos de pago y también ofrecen una solución si algo sale mal. Sin embargo, pueden no ofrecer la misma protección que los proveedores de crédito por lo que se recomienda checar sus términos y condiciones antes de usarlas.
A la hora de hacer el pago, se recomienda checar si la conexión es segura y solo llenar los datos que son obligatorios para el pago. Si el usuario no se va a convertir en un cliente frecuente de la tienda se recomienda no crear una cuenta ni permitir que la tienda guarde la información de pago. Por último, se recomienda mantener cuentas seguras mediante una autenticación de dos pasos y tener contraseñas diferentes para cada cuenta, además de identificar emails sospechosos y reportarlos.

5. Manejo de contraseñas

Riesgos:
Las contraseñas también están expuestas a riesgos que pueden posibilitar ciberataques. Aunque la buena práctica es tener una contraseña diferente para cada cuenta, desafortunadamente no muchos usuarios la siguen y tienden a repetir contraseñas, lo que abre la puerta a ciberataques no solo en una cuenta sino en múltiples cuentas, esto también posibilita a que no conozcan la seguridad de sus contraseñas y cómo responder si una contraseña es vulnerable.
Otro riesgo que pueden sufrir las contraseñas son las contraseñas de default, que son contraseñas estándar preconfiguradas, el problema está en que estas

contraseñas son muy bien conocidas por los hackers o los atacantes lo que hace que la cuenta sea vulnerable.
Si una contraseña no es lo suficientemente compleja, esta no detendrá a los ciberatacantes de ingresar a la cuenta del usuario y robar datos e información personal. Aunque las contraseñas sean complejas a veces son muy cortas y esto les facilita el trabajo a los atacantes, las autoridades recomiendan el uso de frases o secuencias de números aleatorios para hacer la contraseña más larga.
También una contraseña puede estar en riesgo de ser comprometida si no se cambia con regularidad por lo que varias páginas de internet y redes sociales le piden al usuario cada cierto tiempo que cambie sus contraseñas.

Administrador de contraseñas:
Un administrador contraseñas es una aplicación diseñada para almacenar credenciales de acceso en una bóveda cifrada y que además cuenta con la funcionalidad de generar contraseñas complejas y seguras. Esto garantiza que el usuario pueda tener una contraseña diferente para cada una de sus cuentas en línea. Solo puede tener acceso a todas las contraseñas guardadas en un administrador de contraseñas si ingresa la contraseña maestra.

6. Medidas que se pueden tomar para proteger la privacidad digital de los usuarios

Lo primero que se puede hacer es usar un administrador de contraseñas, esto le permitirá al usuario generar diferentes contraseñas complejas para cada cuenta en línea, también el administrador detectará contraseñas que son débiles y le sugerirá una nueva contraseña más fuerte, además se encarga de detectar cuando es necesario cambiar una contraseña. También se recomienda cambiar todas las contraseñas que sean el default como por ejemplo “1234” o “contraseña”.
Se recomienda tener la VF2 o autentificación en dos pasos activada, especialmente para sitios de bancos y cuentas que involucren pagos. La mayoría de las redes sociales también ofrecen esta opción.
Si los usuarios quieren reducir la cantidad de datos que las compañías y páginas web recolectan de ellos, pueden usar una extensión de navegador o VPN que bloquee los anuncios y los datos que las compañías quieran recolectar o elegir la navegación privada, esto es recomendable si frecuentemente los usuarios se conectan a redes de WIFI públicas. Por último se recomienda tener un antivirus descargado en todos los dispositivos.

Referencias:

National Cyber Security Centre. (2018). Phishing attacks: defending your organisation. 6 de noviembre de 2021 , de National Cyber Security Centre Sitio web: https://www.ncsc.gov.uk/guidance/phishing

SOCIALTIC. (2020). Seguridad y privacidad digital en Instagram. 6 de noviembre de 2021, de SOCIALTIC Sitio web: https://socialtic.org/blog/seguridad-digital-estafas-instagram/

Cybervore. (2021). E-commerce Cybersecurity - Enhancing Data Protection in 2021. 6 de noviembre de 2021, de Cybervore Sitio web: https://www.cybervore.com/blog/e-commerce-cybersecurity-enhancing-data-protection-in-2021/

National Cyber Security Centre. (2019). Shopping online securely. 6 de noviembre de 2021, de National Cyber Security Centre Sitio web: https://www.ncsc.gov.uk/guidance/shopping-online-securely

Klosowski, T. (2019). How to Protect Your Digital Privacy. 6 de noviembre de 2021, de The New York Times Sitio web: https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy

Hrastinski, Stefan & Aghaee, Nam. (2012). How are campus students using social media to support their studies? An explorative interview study. Education and Information Technologies. 17. 10.1007/s10639-011-9169-5.

National Cyber Security Centre. (2018). Top tips for staying secure online. 6 de noviembre de 2021, de National Cyber Security Centre Sitio web: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email

Owaida, A. (2020). Qué es un administrador de contraseñas y cómo elegir uno. 6 de noviembre de 2021, de Welivesecurity Sitio web: https://www.welivesecurity.com/la-es/2020/06/26/que-es-administrador-contrasenas-como-elegir-uno/

Concepto . (2021). Riesgos y peligros de las redes sociales . 6 de noviembre de 2021, de Concepto Sitio web: https://concepto.de/riesgos-y-peligros-de-las-redes-sociales/

UNICEF. (sin año). Ciberacoso: Qué es y cómo detenerlo Diez cosas que los adolescentes quieren saber acerca del ciberacoso.. 6 de noviembre de 2021 , de UNICEF Sitio web: https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

Corona P. (2016). ¿Qué es el ciberbullying?. 6 de noviembre de 2021 , de Asociación de Internet MX Sitio web: https://www.gob.mx/ciberbullying/articulos/que-es-el-ciberbullying

Lee D. (2020). Ciber extorsión: cómo prevenirla. 6 de noviembre de 2021 , de Manual de Seguridad para la prevención de delitos Sitio web: https://manualdeseguridad.com.mx/seguridad_newsletter/20/ciber_extorsion_como_prevenirla.asp

Oracle. (2021). ¿Qué es el spoofing?. 6 de noviembre de 2021, de Oracle Sitio web: https://www.oracle.com/es/database/security/que-es-el-spoofing.html

Esquema del cuestionario:

1) Preguntas generales sobre el usuario
2) Preguntas generales sobre ciberseguridad, redes sociales, streaming y videojuegos
3) Preguntas acerca de las redes sociales y su rol en la educación
4) Preguntas acerca de las amenazas en la web
5) Preguntas sobre la seguridad en la web
6) Preguntas acerca de la percepción de los peligros en la web como forma de conclusión