**Redes Sociales**

*Amenazas a la ciberseguridad 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.

**Preguntas Encuesta:**

1 ¿Tienes activada la autenticación en dos pasos (VF2) en tus cuentas de redes sociales?

1. Sí
2. No
3. No sé qué es la autenticación en dos pasos (VF2)

2) ¿Has recibido un mensaje directo sospechoso por redes sociales pidiéndote que le des click a un link, descargues un archivo o proporciones datos personales como datos bancarios?

1. Sí
2. No

2a) En caso de haber respondido sí en la (2), ¿hiciste lo que se te pedía en el mensaje?

1. Sí
2. No

2b) En caso de haber respondido sí en la (2), ¿reportaste la cuenta?

1. Sí
2. No

¿Qué tan confiable es para ti que una cuenta esté verificada para saber si la cuenta es legítima?

1. Nada confiable
2. Algo confiable
3. Neutral
4. Confiable
5. Muy confiable

**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.

**Preguntas Encuesta:**

Durante la pandemia de COVID-19 dirías que tus compras en línea:

1. Aumentaron
2. Disminuyeron
3. Se mantuvieron igual

¿Qué tan confiables son las compras en línea?

1. Nada confiable
2. Algo confiable
3. Neutral
4. Confiable
5. Muy confiable

¿Revisas los comentarios o el *feedback* de un producto o tienda en línea antes de comprarlo?

1. Sí
2. No
3. Algunas veces

¿Cuál es tu usual método de pago al realizar compras online?

1. Tarjeta de crédito
2. Tarjeta de débito
3. Plataformas de pago en línea como PayPal, Apple Pay y similares
4. Otro

¿Creas una cuenta cada vez que visitas una tienda en línea nueva o permites que guarden tu información de pago?

1. Sí
2. No

**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>