Boletín N° 20

Octubre - Diciembre 2024

Amenazas que podrían comprometer tu seguridad:

Crimeware

Malware que busca infiltrarse en tus dispositivos para obtener datos sensibles.

Cibercriminales, listos para la temporada navideña

Tiendas falsas y ofertas engañosas diseñadas para robar tu dinero.

Quishing llega a los códigos QR

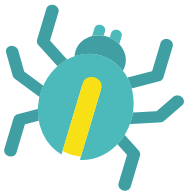
Fraudes mediante códigos QR que pueden redirigirte a sitios peligrosos.

Universidad de Santander UDES
VIGILADA MINEDUCACIÓN | SNIES 2832
ACREDITACIÓN INSTITUCIONAL ALTA CALIDAD UDES MIN EDUCACIÓN

Boletín N° 20

Octubre - Diciembre 2024

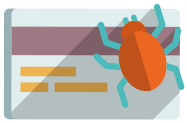
Crimeware



Crimeware es un término que se utiliza para describir **software diseñado con fines criminales,** principalmente para realizar actividades maliciosas en línea.

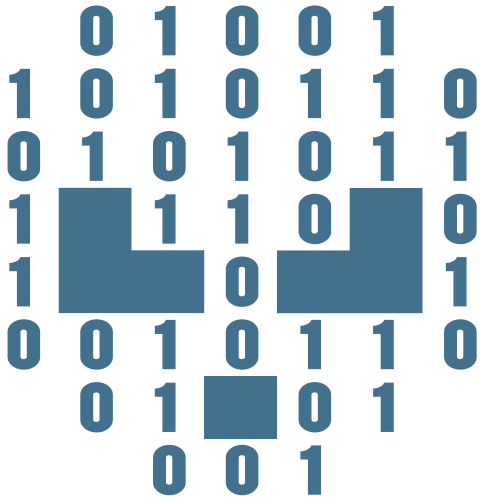
Los delincuentes cibernéticos utilizan crimeware para **robar información,** cometer fraudes financieros, o incluso para controlar dispositivos de manera remota.

Este tipo de software generalmente está diseñado para ser furtivo y difícil de detectar, lo que lo convierte en una **amenaza** significativa para la seguridad informática.



Algunos de los tipos de crimeware más comunes incluyen:

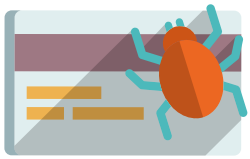
- **Troyanos**
- **Ransomware**
- **Keyloggers**
- **Botnets**
- **Phishing**
- **Adware y Spyware**



Boletín N° 20

Octubre - Diciembre 2024

Impacto del crimeware



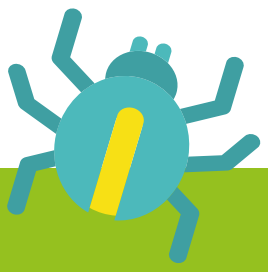
El crimeware puede tener consecuencias devastadoras tanto para las personas como para las organizaciones. Algunos de los impactos incluyen:

- **Pérdida financiera:** A través del robo de información financiera, fraudes o la interrupción de las operaciones comerciales.

- **Robo de datos personales:** Puede incluir la exposición de datos sensibles como números de tarjetas de crédito, identidades personales y detalles bancarios.

- **Daño a la reputación:** Las organizaciones que sufren un ataque de crimeware pueden perder la confianza de sus clientes o socios comerciales.

- **Interrupción de servicios:** Como los ataques DDoS o la extorsión a través de ransomware, que pueden interrumpir las operaciones de una organización.



Prevención y Mitigación

Para protegerse contra el crimeware, es importante seguir algunas buenas prácticas de seguridad informática:

- **Mantener actualizado el software:** Los parches de seguridad son cruciales para reducir la vulnerabilidad de los sistemas.

- **Uso de antivirus y herramientas de seguridad:** Mantener un software antivirus actualizado puede ayudar a detectar y bloquear el crimeware.

- **Educación sobre phishing:** Asegúrate de que los usuarios estén bien informados sobre las técnicas de phishing y cómo identificarlas.

- **Backup de datos:** Realizar copias de seguridad de manera regular para mitigar el impacto de ataques como el ransomware.

- **Autenticación de múltiples factores (MFA)**: Implementar MFA ayuda a proteger las cuentas aunque las credenciales se vean comprometidas.

Boletín N° 20

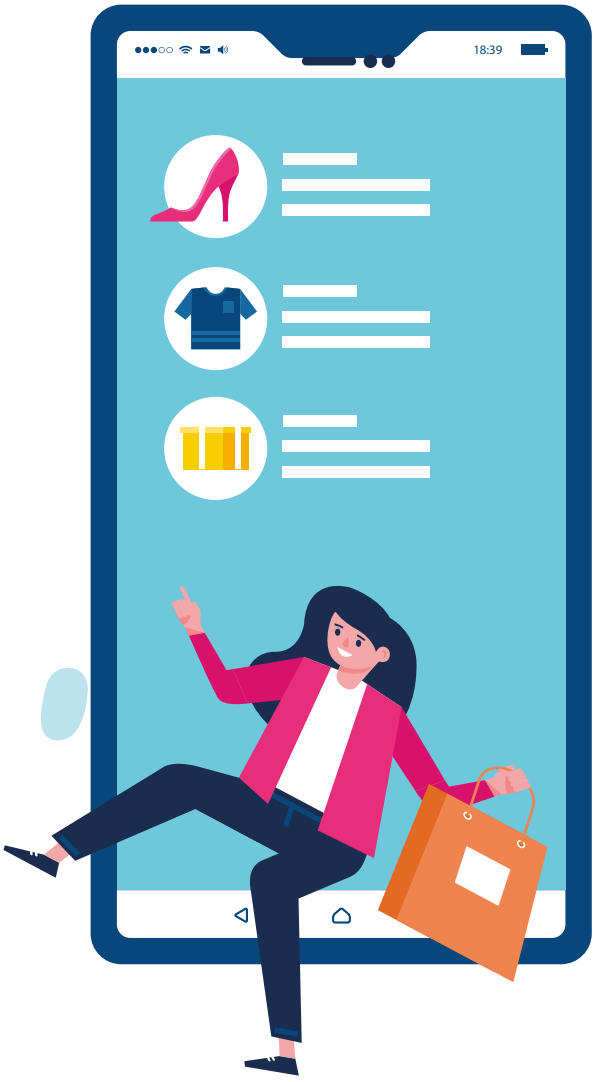
Octubre - Diciembre 2024

Cibercriminales, listos para la temporada navideña

La temporada navideña es una época de grandes compras y ofertas, pero también se convierte en una ventana de oportunidad para los cibercriminales.

Durante este período, las tiendas en línea falsas y las ofertas engañosas aumentan considerablemente, buscando aprovecharse de la prisa y la emoción de los consumidores.

Aquí te explicamos cómo puedes identificar estas amenazas y protegerte de caer en sus trampas.



Boletín N° 20

Octubre - Diciembre 2024

Tiendas falsas: El engaño al alcance de un clic

Las tiendas falsas son una de las formas más comunes de fraude en línea durante la temporada navideña.

Los cibercriminales crean sitios web que imitan a tiendas legítimas, pero que en realidad son diseñados solo para robar tu dinero y tus datos personales.

¿Cómo funcionan?

- **Sitios web falsos:** Estos sitios pueden tener un aspecto similar a los de marcas reconocidas o incluso replicar páginas populares de compras. A menudo, las URL parecen legítimas pero tienen ligeras variaciones (por ejemplo, un ".com" en lugar de ".es" o una letra cambiada).

- **Precios irresistibles**: Las ofertas son demasiado buenas para ser ciertas, como descuentos altísimos en productos populares como electrónicos, juguetes o ropa de marca.

- **Pago inseguro:** Muchas veces, estos sitios ofrecen métodos de pago poco seguros o directamente piden transferencias bancarias, lo que dificulta recuperar el dinero en caso de fraude.

Boletín N° 20

Octubre - Diciembre 2024

Tiendas falsas: El engaño al alcance de un clic

¿Cómo protegerse?

1. **Verificar la URL:** Antes de realizar una compra, asegúrate de que la dirección del sitio sea segura, es decir, que comience con “https://” y tenga un candado verde en la barra de direcciones.

2. **Investiga la tienda:** Busca opiniones y reseñas de otros usuarios en línea, consulta redes sociales y verifica la existencia de la tienda en foros de seguridad.

3. **Desconfía de precios extremadamente bajos:** Si una oferta suena demasiado buena para ser cierta, probablemente lo sea. Los cibercriminales usan precios bajos para atraer a las víctimas.

4. **Revisa las políticas de devolución y contacto:** Las tiendas legítimas suelen tener políticas claras de devolución y formas de contacto visibles. Si no encuentras esta información, es una bandera roja.

Boletín N° 20

Octubre - Diciembre 2024

Quishing llega a los códigos QR

El quishing es un tipo de fraude que utiliza códigos QR maliciosos para engañar a los usuarios y redirigirlos a sitios web falsos o peligrosos.

El término "quishing" proviene de la combinación de QR (código de respuesta rápida) y phishing, que hace referencia a las tácticas de engaño utilizadas para obtener información confidencial, como contraseñas, datos bancarios o información personal.

¿Cómo funciona el quishing?

Los atacantes crean códigos QR maliciosos que parecen legítimos, pero que, cuando son escaneados por un usuario, lo redirigen a un sitio web peligroso. Este sitio web puede ser:

Un sitio de phishing: Que intenta robar información personal o financiera del usuario (por ejemplo, una página que imita un banco, una tienda en línea o un servicio popular, solicitando datos sensibles).

Un sitio que descarga malware: El código QR puede iniciar la descarga de un virus, troyano o ransomware en el dispositivo móvil, lo que comprometería la seguridad de los datos y la privacidad del usuario.
Un sitio de pago falso: Los delincuentes pueden crear páginas que imitan servicios de pago o transferencias, engañando a las víctimas para que introduzcan detalles de tarjetas de crédito o contraseñas.

¿Cómo protegerse?

No hagas clic en enlaces sospechosos: Si recibes correos electrónicos con ofertas demasiado buenas, verifica siempre el remitente antes de hacer clic en cualquier enlace. Si tienes dudas, visita directamente el sitio web de la marca para comprobar la oferta.

Cuidado con los anuncios no solicitados: Desconfía de los anuncios de marcas que no has solicitado o que no parecen tener una conexión legítima con tu perfil.

Usa métodos de pago seguros: Siempre que sea posible, utiliza plataformas de pago seguras, como tarjetas de crédito o servicios como legítimos, que ofrecen protecciones en caso de fraude.

Boletín N° 20

Octubre - Diciembre 2024

CONTÁCTANOS

Si presentas dudas o detectas alguna situación sospechosa puedes comunicarte con el subproceso de seguridad informática UDES:

Bucaramanga
seguridadinformatica@udes.edu.co
Teléfono (607) 6516500 ext. 1005-1001

Valledupar
lortiz@valledupar.udes.edu.co
Teléfono: (605) 5730073 ext. 129

Cúcuta
wpena@udes.edu.co
Teléfono: (607) 5748717 ext. 4196

Universidad de Santander UDES
VIGILADA MINEDUCACIÓN | SNIES 2832
ACREDITACIÓN INSTITUCIONAL ALTA CALIDAD UDES MIN EDUCACIÓN