Universidad de Santander
UDES

VIGILADA MINEDUCACIÓN | SNIES 2832

ACREDITACIÓN INSTITUCIONAL ALTA CALIDAD UDES MIN EDUCACIÓN

BOLETÍN DE SEGURIDAD INFORMÁTICA

Número 16

Octubre a Diciembre 2023

Universidad de Santander
UDES
VIGILADA MINEDUCACIÓN | SNIES 2832

ACREDITACIÓN INSTITUCIONAL ALTA CALIDAD UDES MIN EDUCACIÓN

Protege tus datos, información personal e información crediticia los atacantes se encuentran al asecho.

Smishing

Engaños por SMS

Compras Online

Smishing

¿Qué es el Smishing?

El Smishing es una combinación de las palabras “SMS” (Short Message Service) y “phishing”. Se trata de una modalidad de estafa cibernética en la que los ciberdelincuentes utilizan mensajes de texto o SMS para engañar a las personas y obtener información confidencial, como datos personales, contraseñas, números de tarjetas de crédito o cualquier otro dato que puedan utilizar con fines fraudulentos.

Como Actuar

Sospecha de mensajes inesperados: Si recibes un mensaje de texto no solicitado, especialmente si te piden información personal o hacer clic en un enlace, verifica la fuente antes de actuar.

No hagas clic en enlaces sospechosos: Siempre verifica la URL antes de hacer clic en un enlace en un mensaje de texto. Si algo parece extraño o poco confiable, evita hacer clic.

Contacta directamente a la entidad: Si recibes un mensaje que supuestamente proviene de una empresa o institución, en lugar de hacer clic en el enlace proporcionado, busca su número de teléfono o sitio web oficial y contáctalos directamente para verificar la autenticidad del mensaje.

No compartas información personal: Nunca compartas información personal o financiera a través de mensajes de texto, a menos que estés seguro de que es una fuente legítima.

Tomado de: https://suind.co/cuidado-con-el-smishing-protege-tus-datos-y-evita-caer-en-esta-estafa-digital

Compras Online

En los últimos años, ha habido un aumento enorme de las compras en línea. Los principales vendedores en línea ahora ofrecen más opciones y selecciones de productos para sus consumidores, y las tiendas físicas tienen sus propios incentivos en línea para seguir siendo competitivas y lograr captar una parte del mercado en línea.

Por desgracia, como la actividad en línea de los consumidores aumentó, también aumentaron los delitos cibernéticos, lo que ha generado que víctimas desafortunadas sufran pérdidas económicas.

Riesgos de comprar en línea

Los riesgos potenciales de comprar en línea incluyen:

- **Robo de identidad**
- **Tiendas en línea falsas**
- **Datos no cifrados**
- **Filtraciones de datos**
- **Opiniones falsas**
- **Aplicaciones falsas**
- **Wi-Fi no seguro**
- **Adware**
- **Phishing**

Tomado de: https://latam.kaspersky.com/resource-center/threats/how-safe-is-online-shopping

BOLETÍN DE SEGURIDAD INFORMÁTICA N° 16

Universidad de Santander UDES
VIGILADA MINEDUCACIÓN | SNIES 2832

ALTA CALIDAD UDES

Octubre - Diciembre 2023

Compras Online

¿Es seguro comprar en línea?

SI: Comprar en línea es una actividad segura. Pueden ser las mismas personas, su Internet y sus hábitos de compra en línea los que lo hacen inseguro.

Y en eso justamente se basan los ciberdelincuentes, Esperan que utilicen contraseñas débiles o el mismo nombre de usuario y contraseña para todas las cuentas en línea.

Cuentan con que utilicen redes públicas de Wi-Fi para ingresar a sus cuentas privadas.

Básicamente, dependen de que los usuarios, es decir, los consumidores, no sigan las buenas prácticas de ciberseguridad.

Ser víctima de ciberdelincuentes podría costarle mucho más que el dinero de su cuenta bancaria: podría costarle su identidad y ocasionarle una serie de problemas financieros y personales.

Suele haber historias de hackers y estafadores en línea, pero la realidad es que es menos probable que los ciberdelincuentes se hagan con los datos de su tarjeta de crédito a través de Internet que por teléfono, por correo o en un restaurante.

De todas formas, hacer compras en línea requiere una medida extra de precaución.

Tomado de: https://latam.kaspersky.com/resource-center/threats/how-safe-is-online-shopping

Compras Online

Cómo saber si un sitio web es seguro para comprar

¿Cómo distinguir entre los sitios de compra en línea seguros y los fraudulentos? Aquí hay algunos datos para tener en cuenta:

Corrobore el certificado SSL

SSL significa “Secure Sockets Layer” (capa de sockets seguros) y es un indicador de que un sitio web es seguro para comprar. Básicamente, es un método de cifrado que deben tener los sitios web que solicitan información personal o confidencial, como los datos de la tarjeta de crédito. Para comprobar que un sitio de compras en línea tiene un certificado SSL actualizado, busque el ícono del candado en la barra de direcciones del navegador web o verifique que la URL comienza con HTTPS y no con HTTP (la S significa “seguro”).

Busque una declaración de privacidad

La política de privacidad explica la forma en que una empresa recopila, utiliza y guarda datos confidenciales de sus clientes. Si bien las leyes y las regulaciones varían en todo el mundo, los comercios en línea respetables deberían tener una declaración de privacidad clara. Si no la tienen, considérelo como una alerta.

Evite las ofertas que parecen demasiado buenas para ser verdad

Si un sitio web parece estar vendiendo ropa de diseño, joyas o aparatos electrónicos por bastante menos que el precio de venta habitual, analice si no es demasiado bueno para ser verdad. Puede ser que termine pagando por réplicas o productos falsos.

Tomado de: https://latam.kaspersky.com/resource-center/threats/how-safe-is-online-shopping

Compras Online

Compruebe si hay errores ortográficos y gramaticales

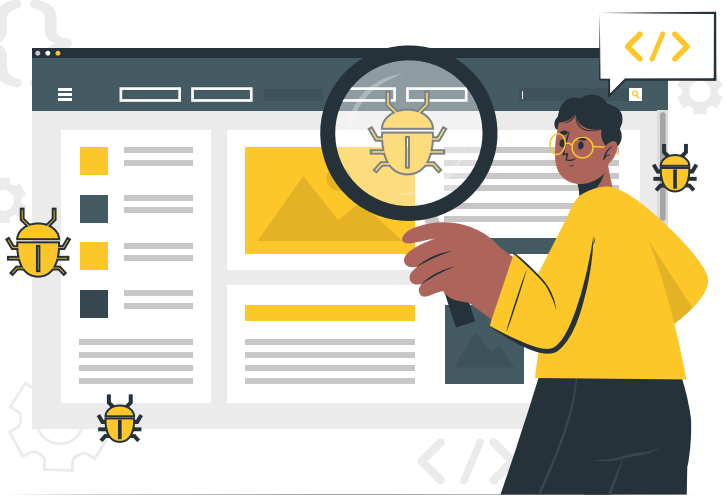
Las marcas respetables en general se aseguran de que los textos y las imágenes en sus sitios web sean de buena calidad. Si un sitio web está mal escrito y tiene muchos errores ortográficos o gramaticales, puede ser una señal de que no es real. Otros signos de alerta pueden ser las imágenes de mala calidad, que no tenga una directiva de devolución y que no se puedan dejar opiniones.

Verifique si el sitio web acepta tarjetas de crédito

Las tarjetas de crédito son uno de los métodos más seguros para hacer transacciones en línea, ya que es más fácil para los emisores de las tarjetas reembolsar el dinero perdido en una estafa. Que un sitio web no acepte pagos con tarjeta de crédito podría ser un motivo de sospecha, porque es más difícil que un sitio web fraudulento sea certificado por empresas de tarjetas de crédito.

Lea las opiniones en línea

Si bien pueden ser falsas, es útil mirar el patrón general de las opiniones de otros clientes al comprar en línea. Los sitios con opiniones confiables pueden darle una idea de la autenticidad de un comercio y de lo que piensan otros clientes antes de comprar.



Tomado de: https://latam.kaspersky.com/resource-center/threats/how-safe-is-online-shopping

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