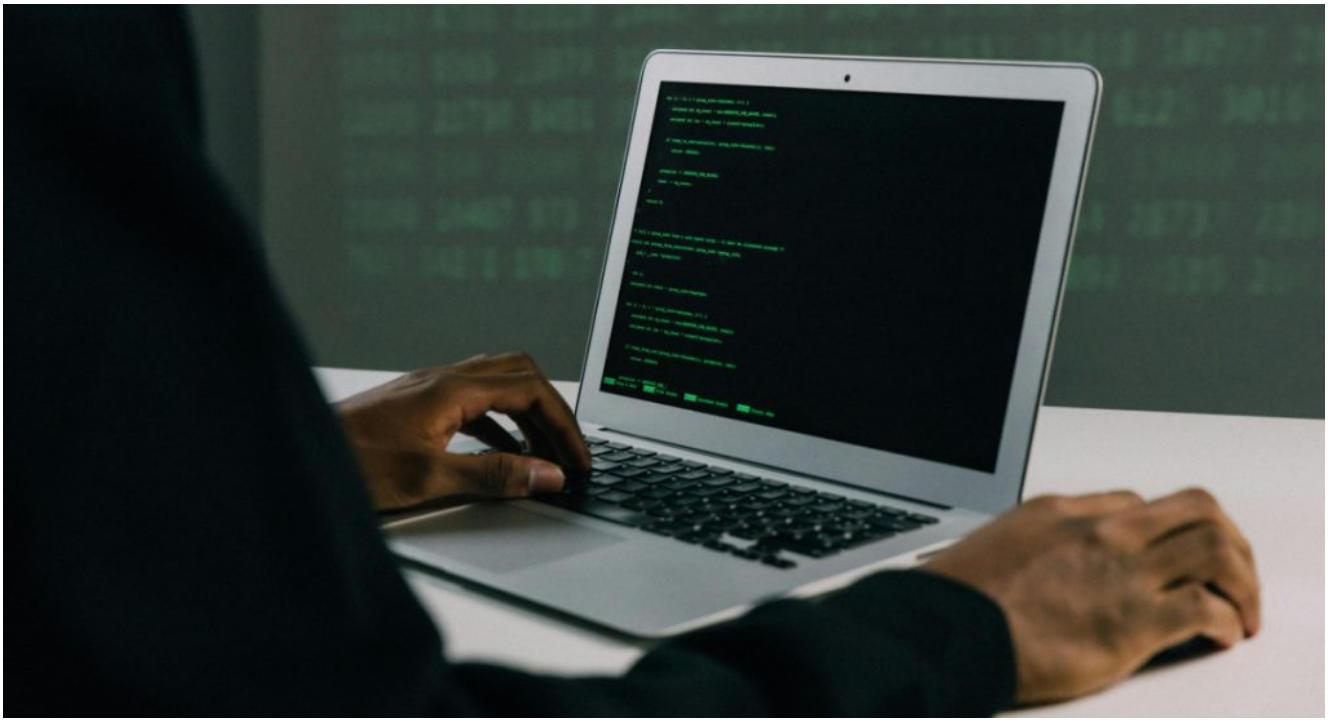
Ciberdelincuentes al acecho: cada vez más argentinos sufren estafas virtuales

29/06/2024



Un ciberataque es cualquier intento de obtener acceso no autorizado a un sistema de computación, red o dispositivo con la intención de robar datos, interrumpir operaciones o realizar otras actividades maliciosas.

Los ciberataques pueden ser llevados a cabo por individuos, grupos organizados o estados-nación con diferentes motivaciones, como **el lucro económico, el espionaje o el activismo**.

Según un estudio realizado, en 2022 un 9% de los argentinos habían sufrido una estafa virtual. **Esta cifra escaló hasta el 31% en 2024**, por lo que muestra el aumento de estos delitos.

Ciberdelito. Foto: Unsplash.

Se trata de un problema significativo en una **actualidad marcada por la creciente digitalización, que incrementó la dependencia de las personas a la tecnología**. Esta situación crea una extensa y variada superficie de ataque, ya que la proliferación de dispositivos conectados añade múltiples puntos de entrada potenciales para los ciberdelincuentes.

Desde el punto de vista económico, los ciberataques tienen un impacto severo. **Las pérdidas financieras directas pueden ser considerables debido a fraudes, robos y extorsiones**, como es el caso del ransomware.

Los distintos tipos de ciberataques existentes

La comprensión de los **diferentes tipos de ciberataques** y sus mecanismos de propagación es esencial para implementar estrategias efectivas de ciberseguridad y minimizar el riesgo de infecciones que puedan comprometer la integridad y seguridad de los sistemas de información.

- **Malware**: es cualquier tipo de software diseñado específicamente para infiltrarse en, dañar o causar un comportamiento no deseado en un sistema de computación sin el consentimiento del usuario. El objetivo del malware puede variar, desde robar información confidencial y espiar las actividades del usuario, hasta tomar el control del sistema o dañar los datos almacenados.
- **Phishing**: los atacantes intentan engañar a las víctimas para que revelen información personal y confidencial, como nombres de usuario, contraseñas, números de tarjetas de crédito y otros datos sensibles. Los atacantes suelen hacerse pasar por entidades legítimas y confiables, como bancos, servicios en línea, o incluso compañeros de trabajo, para ganarse la confianza de las

víctimas.

Los hackers tienen técnicas cada vez más innovadoras. Foto: Unsplash.

- **Ransomware**: un tipo de malware que cifra los archivos de un usuario o de una organización, haciendo que los datos sean inaccesibles hasta que se pague un rescate para obtener la clave de descifrado. Este tipo de ataque creció significativamente en frecuencia y sofisticación, afectando a individuos y empresas.
- **Ataque de diccionario o por fuerza bruta**: busca robar las contraseñas mediante un programa automático que prueba diferentes combinaciones de claves. Por eso, es recomendable poner contraseñas únicas, que alternan mayúsculas y minúsculas, números, letras, símbolos y que sean bastante largas.
- **Ataque de denegación de servicio**: una forma de ciberataque diseñada para inundar un sistema, red o servicio en línea con múltiples solicitudes inmediatas para incapacitar el acceso a una página web.
- **Ataque de Man-in-the-middle**: un ataque mediante el cual se busca interceptar una conversación, navegación o subida de archivos sin que este sepa en ningún momento que está siendo espiado.

5 consejos para evitar las estafas virtuales

Con los avances tecnológicos y las nuevas técnicas empleadas por los ciberdelincuentes es muy fácil ser víctima de un hackeo. **Con estos trucos podrás prevenirlo:**

1. **No entrar a la cuenta bancaria desde Google**, es mejor

aprender la dirección/URL y tipearla en la barra de direcciones de tu navegador o desde la app oficial.
2. **No compartir información personal o financiera por teléfono, email, redes sociales o WhatsApp**, ya que los bancos nunca solicitan estos datos a los clientes.
3. **No entrar en enlaces sospechosos** ni descargar archivos de correos electrónicos y mensajes de redes sociales.
4. **Descargar apps solo desde las tiendas oficiales**, como la App Store o Google Play.
5. **Cambiar periódicamente las contraseñas de tu homebanking**.

Fuente: Canal 26