PRIMERO LA VIDA
ATENTO AL RIESGO PÚBLICO

Delitos informáticos

¿Qué hacer en caso de ser víctima de un delito informático?
Cada vez son más los crímenes que se presentan en plataformas digitales, los delitos informáticos van desde la violación de datos personales, hasta la suplantación y la obstaculización de redes de telecomunicaciones y sistemas. ¿Sabe cómo denunciar un delito informático? Acá le contamos:

1. Ingrese al portal 'A Denunciar' de la Policía Nacional.
2. Seleccione la opción 'Denuncia Virtual'.
3. Seleccione 'Delitos Informáticos'.
4. Consulte la normatividad para saber qué tipo de delito informático quiere denunciar.
5. Ingrese sus datos e instale la denuncia.

Evite ser víctima de delitos cibernéticos teniendo en cuenta las siguientes recomendaciones

Busque contraseñas seguras
Entre más difíciles sean mucho mejor. Siempre que las vaya a elegir busque una clave que combine símbolos, mayúsculas, minúsculas y números. Evite utilizar la misma contraseña de sus cuentas, fechas de nacimiento, días especiales o números de teléfono, además de compartirlas con personas que no son de su confianza.

¡A la hora de navegar!
Siempre cierre su sesión de correo electrónico, así como redes sociales, WhatsApp Web, entre otros. Nadie está exento de que un amigo de lo ajeno nos robe el computador, así que también es recomendable eliminar los archivos recientes (memoria caché) que fueron vistos y el historial del navegador.

Cuidado con los archivos desconocidos
Aunque sea muy amigo de compartir cadenas y mensajes grupales, desconfíe de los correos electrónicos y SMS que provienen de fuentes desconocidas, así que evite abrir archivos y enlaces de este tipo. ¡Una clave de oro para prevenir delitos cibernéticos!

Proteja su información personal
Nunca ingrese sus datos personales ni credenciales en sitios de los que desconfíe o que no sean de su confianza. Antes de darlos es importante que se asegure que no sea una página falsa. Revise que la dirección que aparece en el navegador inicie con HTTPS.

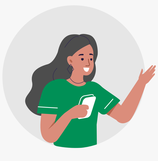
Antivirus, ¡el infaltable!
Una de las mejores formas de proteger su seguridad es utilizando un antivirus tanto para computadores como para smartphones. ¡Es una medida sencilla que le puede ahorrar muchos problemas!

¿Y qué pasa con las Wifi públicas?
Muchos lugares ofrecen acceso gratuito a Wi-Fi y aunque en ocasiones necesite conectarse a las mismas, es mejor evitarlo. Si es estrictamente necesario, nunca ingrese datos privados ni acceda a servicios bancarios, correo electrónico y redes sociales.

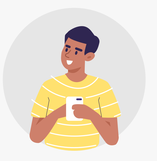
- Tener cuidado con los mensajes de correo electrónico que contienen enlaces sospechosos o archivos adjuntos que no son esperados.
- No descargar nada de fuentes desconocidas.
- Asegurarse de que se está utilizando un sitio web legítimo antes de introducir la información personal.
- Aplicar siempre las actualizaciones de software inmediatamente, ya que corrigen vulnerabilidades de seguridad.
- Emplear contraseñas seguras y exclusivas, es decir, no reutilizar la misma contraseña para varias cuentas.
- No utilizar terminales públicas de carga ni conectar dispositivos desconocidos a los equipos personales.
- Revisar los permisos de las aplicaciones antes de instalarlas.
- No enviar datos confidenciales por correo electrónico, SMS o telefónicamente.
- Limitar la información que se comparte en redes sociales.
- Mantener actualizado el sistema operativo y las aplicaciones.

Cuide de su empresa y de sus trabajadores

Las empresas deben estar atentas a diseñar estrategias que permitan ofrecer más controles de ciberseguridad, con el objetivo de proteger la empresa, sus empleados y usuarios, conozca los riesgos actuales en el mundo digital y conozca cómo enfrentarlos.



Vencer el Ransomware
Es un tipo de ciberataque que consiste en un software malicioso que infecta un dispositivo y muestra mensajes exigiendo el pago de dinero para restablecer el acceso. El Ransomware puede llegar a través de aplicaciones móviles, redes sociales, correo electrónico, compra en línea, entre otros. Por esto es importante seguir las recomendaciones de evitar abrir correos sospechosos, o aplicaciones poco confiables, no comprar en páginas que no cuenten con tecnología SSL, que es un estándar de seguridad que encripta la información de usuario.



Frenar los ataques de phishing
Esta modalidad se explica como la suplantación de sitios web, para capturar datos personales y credenciales de acceso a plataformas virtuales como bancos, redes sociales, correo, entre otros.

Para esto le recomendamos:
- No dar clic en enlaces o archivos sospechosos adjuntos en un correo electrónico.
- No ingresar usuario y contraseña en links sospechosos que lleguen vía correo electrónico.
- Cambiar contraseñas de manera periódica.
- No de información confidencial por medio telefónico.

Implementar nuevos métodos de verificación
En los últimos años los desarrollos en dispositivos electrónicos permiten tener la posibilidad de usar nuevas formas para verificar la identidad de una persona. Por ejemplo, autenticación facial, reconocimiento por voz o a través de la impresión dactilar. Esto puede generar mayor confianza para los usuarios digitales y seguridad de los datos almacenados en las empresas.

Efectos colaterales cuando se vulnera la ciberseguridad
Finalmente, las empresas deben empezar a reconocer la importancia de implementar buenas prácticas para evitar ataques cibernéticos. Esto debido a que un solo ataque puede verse reflejado en efectos como:

- La reducción de su productividad.
- Daños reputacionales.
- Retos de carácter legal por fugas de información privilegiada de datos sensibles de clientes, proveedores y asociados de negocios.