¿Cómo proceder después de ser víctima de un ciberdelito?

Los ciberdelitos son un problema creciente en México. De acuerdo con el Instituto Nacional de Estadística y Geografía (INEGI), en 2022 se registraron más de 5 millones de ciberdelitos en el país, un aumento del 20% con respecto al año anterior.

Los ciberdelitos pueden ser de diversos tipos, como el phishing, el robo de identidad, el fraude cibernético y el ciberacoso. Estos delitos pueden tener consecuencias graves para las víctimas, como pérdidas financieras, daños a la reputación y la violación de la privacidad.

Si cree que ha sido víctima de un ciberdelito, debe seguir estos pasos:

1. **Recopile toda la información posible sobre el incidente.** Esto incluye la dirección del correo electrónico o el número de teléfono del remitente, el contenido del mensaje o la llamada, y cualquier otra información que pueda ayudar a las autoridades a investigar el caso.
2. **Cambie sus contraseñas.** Esto incluye las contraseñas de su correo electrónico, redes sociales, cuentas bancarias y cualquier otra cuenta en línea que haya utilizado.
3. **Reporte el incidente a las autoridades.** Puede hacerlo en la página web de la Fiscalía General de la República (FGR).
4. **Póngase en contacto con su banco o institución financiera.** Ellos pueden ayudar a proteger su cuenta bancaria y evitar que los delincuentes accedan a sus fondos.

¿Cuáles son los ciberdelitos más comunes en México?

De acuerdo con el Instituto Nacional de Estadística y Geografía (INEGI), los ciberdelitos más comunes en México son:

1. **Phishing:** Este tipo de ciberdelito consiste en engañar a las víctimas para que revelen información personal confidencial, como contraseñas, números de tarjetas de crédito o direcciones. Los delincuentes suelen utilizar correos electrónicos o mensajes de texto falsos que parecen haber sido enviados por una fuente legítima, como un banco o una empresa de comercio electrónico.

2. **Robo de identidad:** Este tipo de ciberdelito consiste en utilizar la información personal de otra persona para cometer fraudes o delitos. Los delincuentes pueden obtener esta información a través del phishing, la suplantación de identidad o el robo de datos.

3. **Fraude cibernético:** Este tipo de ciberdelito consiste en engañar a las víctimas para que entreguen dinero o bienes. Los delincuentes pueden hacerlo a través de estafas telefónicas, sitios web falsos o anuncios engañosos.

4. **Ciberacoso:** Este tipo de ciberdelito consiste en acosar, amenazar o intimidar a otra persona a través de Internet. El ciberacoso puede causar daños psicológicos graves a las víctimas.

¿Cómo puedo actuar ante un escenario de phishing?

En México, el ciberdelito de phishing es un delito grave que puede ser castigado con hasta seis años de prisión. Si usted es víctima de phishing, debe seguir estos pasos:

1. **Cambie sus contraseñas.** Esto incluye las contraseñas de su correo electrónico, redes sociales, cuentas bancarias y cualquier otra cuenta en línea que haya utilizado.
2. **Reporte el incidente a las autoridades.** Puede hacerlo en la página web de la Fiscalía General de la República (FGR).
3. **Póngase en contacto con su banco o institución financiera.** Ellos pueden ayudar a proteger su cuenta bancaria y evitar que los delincuentes accedan a sus fondos.

Además de estos pasos, también puede tomar medidas para prevenir el phishing en el futuro. Aquí hay algunos consejos:

1. **Sea cauteloso con los correos electrónicos** y los mensajes de texto que recibe. Si un correo electrónico o mensaje de texto parece sospechoso, no lo abra ni haga clic en ningún enlace.
2. **No comparta su información personal con nadie que no conozca.** Esto incluye su contraseña, número de tarjeta de crédito y dirección.
3. **Use un software de seguridad cibernética actualizado.** Este software puede ayudar a proteger su computadora y dispositivos móviles de los ataques de phishing.

Aquí hay algunos ejemplos de correos electrónicos de phishing que puede recibir:

1. Un correo electrónico que le pide que actualice su información de cuenta.
2. Un correo electrónico que le informa que ha ganado un premio.
3. Un correo electrónico que le advierte de una amenaza a su computadora o dispositivo móvil.

Si recibe uno de estos correos electrónicos, no lo abra ni haga clic en ningún enlace. En su lugar, bórrelo inmediatamente.

Si cree que ha sido víctima de phishing, puede tomar medidas para proteger su información y prevenir que los delincuentes accedan a sus cuentas.

¿Qué autoridades pueden ayudarme?

En México, las principales autoridades que pueden ayudar a las víctimas de ciberdelitos son:

La Fiscalía General de la República (FGR): La FGR es la autoridad encargada de investigar y perseguir los delitos federales, incluidos los ciberdelitos. Puede contactar a la FGR a través de su sitio web o llamando al número **088**.

El Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX): El CERT-MX es una unidad de la Secretaría de Seguridad y Protección Ciudadana (SSPC) que se encarga de coordinar la respuesta ante incidentes cibernéticos. Puede contactar al CERT-MX a través de su sitio web o llamando al número **800-227-2000**.

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF): La CONDUSEF es una autoridad que se encarga de proteger los derechos de los usuarios de servicios financieros. Puede contactar a la CONDUSEF a través de su sitio web o llamando al número **55-5340-0999**.