talleres TI

Cibercuidados
Fraudes y Estafas

Jefatura de Gabinete de Ministros
República Argentina

Secretaría de Innovación, Ciencia y Tecnología

Cibercuidados: prevención de fraudes y estafas

INTRODUCCIÓN

a) Introducción

En muchos aspectos, el uso de Internet y de las Tecnologías de la Información y las Comunicaciones (TIC) beneficiaron la vida de los usuarios digitales, ya sea para trabajar, estudiar, hacer compras, pagar servicios o simplemente conectarse con amistades a través de redes sociales.

Pero así como existen un sinfín de ventajas, hay también peligros, amenazas y riesgos en el entorno virtual que no se deben desconocer. Un usuario o usuaria que conozca los principales delitos informáticos, como la estafa, podrá disfrutar de las TIC sin poner en riesgo sus datos personales, su patrimonio o el bienestar propio y el de su familia.

b) Riesgos y peligros que pueden suceder en el ciberespacio.

¿Qué cosas nos atemorizan con el uso de las TIC?

- Que alguien nos robe los datos de nuestra tarjeta de crédito -cuando hacemos un pago a través de Internet- y luego, los utilice para hacer compras en nuestro nombre.
- Que alguien acceda a nuestras contraseñas de redes sociales y sitios bancarios.
- Que nos roben nuestros datos bancarios para obtener préstamos a nuestro nombre, realizar compras online y/o transferencias de dinero desde nuestra cuenta hacia otra desconocida.
- Que accedan a nuestros dispositivos, tomen imágenes y las publiquen en algún sitio web en el que no nos gustaría aparecer.
- Que alguien ingrese remotamente a nuestra computadora y robe o copie información muy importante sin que nos demos cuenta.

c) Privacidad de datos personales

Los ***datos personales*** son un conjunto de información que se refiere a personas físicas o jurídicas. Pueden ser el nombre, apellido, domicilio, número de DNI, fecha de nacimiento, información sobre deudas, imágenes de fotografías o de videos, etc.

También los ***datos biométricos*** son un tipo de dato personal. Estos son los que están relacionados con las características físicas, fisiológicas o de conductas que permiten la identificación única de una persona. Por ejemplo, la huella dactilar, el rostro, el iris, la retina, la firma, la forma de la mano, la escritura, la voz, la forma de caminar, etc.

Además existe una categoría más que se denomina ***datos sensibles***, y son aquellos que se refieren al origen étnico, a las opiniones políticas, convicciones religiosas, filosóficas o morales, a la afiliación sindical o que se relacionan con la salud o la vida sexual.

Es importante tener presente que nadie puede obligarnos a informar estos datos, y que no deben estar registrados en ninguna base de datos, salvo que sea con autorización o pedido judicial.

Toda esa información es muy importante y muy requerida por los ciberdelincuentes, ya sea para robar o usurpar la identidad de sus víctimas con el fin de obtener algún beneficio económico, causar daños a la imagen o para vender la información a terceros, por ejemplo.

En Argentina, la Ley 25326 de Protección de Datos Personales protege si los datos de identidad, de salud o de crédito de una persona son usados sin su consentimiento.

d) Qué es un delito informático

Cuando hablamos de ***delitos informáticos***, nos referimos a aquellas conductas ilegales que vulneran derechos o libertades de las personas, en las cuales los cibercriminales que los cometen utilizan en su accionar un dispositivo informático, una computadora, un celular inteligente, una tablet, una televisión inteligente, una consola de videojuegos o cualquier otro artefacto electrónico que tenga conexión a Internet.

Diferencia entre fraude y estafa

Muchas veces utilizamos las palabras fraude y estafa como si fueran sinónimos. Sin embargo, refieren a conceptos distintos: ambas figuras penales, delictivas, tienen un significado propio.

El **fraude** se caracteriza por la utilización del engaño para obtener algún beneficio en perjuicio de una institución, organización o de una persona.

La **estafa** se comete también mediante un engaño, pero contra el patrimonio o la propiedad de una víctima. Se puede decir, entonces, que ***la intención final de la estafa es el lucro.***

Componentes de la estafa

La figura del delito de **estafa** fue tipificada en el Código Penal Argentino para proteger el bien patrimonial, la buena fe y las relaciones de confianza de las personas. De modo que una víctima de estafa es traicionada “en su buena fe”.

- **El engaño**

El engaño es el factor fundamental que debe elaborar un delincuente. Pensemos que debe ser lo suficientemente creíble como para que la víctima no sospeche y “caiga en el engaño”, en la mentira que le dicen.

- **La intención de estafar**

Al cometer una estafa, el delincuente sabe que está ejecutando un plan de falsedad con el propósito de cumplir su objetivo, que es obtener alguna ganancia.

- **El error de la víctima**

Cuando el agresor planea la estafa, espera que la víctima elegida cometa un error, que crea en el engaño para que realice una acción que beneficiará al delincuente, pero que la perjudicará patrimonialmente.

e) La ingeniería social

La navegación por Internet, así como el uso del correo electrónico o de las redes sociales, se ha transformado en un hábito cotidiano para la mayoría de las personas. La familiaridad y comodidad con las que usamos estas herramientas nos hacen sentir confiados y protegidos. Sin embargo, estos entornos digitales son compartidos con personas malintencionadas que intentan obtener un beneficio a costa de los demás. Y para ello utilizan técnicas y mecanismos denominados “ingeniería social”.

La ingeniería social se basa en el arte de la persuasión, es decir, en convencer a las personas para que revelen datos confidenciales o realicen alguna acción. Este tipo de engaño no es nuevo y ya venía registrándose fuera del ciberespacio, bajo otras modalidades conocidas como “el cuento del tío”.

A continuación, describimos algunos ejemplos de ingeniería social:

- Pretender estar vinculado a un alto funcionario o a una persona reconocida en el ámbito de la víctima, usando tal vez un tono de voz intimidante, amenazante o urgente, para robar información.
- Usar la adulación, modales amistosos o conversar sobre intereses comunes.
- Establecer una relación o contacto repetido durante un cierto período de tiempo para provocar familiaridad con la “identidad” del atacante y probar su confiabilidad.
- Imitar el comportamiento habitual de ciertas personas, actuando como un compañero/a de trabajo o un amigo/a que necesita información, contraseñas o documentos para su trabajo.

f) Modalidades delictivas

1) Phishing

En Argentina, los fraudes y estafas sucedidos en línea se produjeron mayormente a través de campañas de ***phishing***, término derivado de las palabras en inglés ***"password harvesting fishing", que pueden traducirse como "cosecha y pesca de contraseñas"***.

En los casos de phishing, el estafador o "phisher" se puede hacer pasar por un empleado bancario, un trabajador estatal, un representante de una ONG, etc., para enviar mensajes fraudulentos. Lo hace a través de mails, mensajes de texto (SMS), redes sociales, WhatsApp, chats y/o en grupos de discusión o foros de sitios web, entre otros.

- **Phishing bancario:** consiste en que la víctima reciba un correo electrónico de un supuesto banco, que le solicita -por el hecho de ser cliente- que valide su usuario y contraseña de acceso a homebanking. Usualmente, el cuerpo del mensaje contiene un enlace que deriva a un sitio web falso creado por el estafador para que la víctima coloque sus credenciales de acceso a homebanking o banca electrónica. Luego, el "phisher" utilizará esos datos para hacer transferencias bancarias a una cuenta determinada.
- **Spearphishing**: el estafador cuenta de antemano con información personal de la víctima, como el número de celular, el nombre, el apellido, la foto y el número del DNI, entre otros.

2) Perfiles falsos de bancos en redes sociales

Al poco tiempo de haberse decretado el aislamiento por aumento de casos de COVID -19, se detectaron varios fraudes provenientes de cuentas de bancos falsas, creadas por los ciberdelincuentes en redes sociales. Así, cuentas no certificadas en Instagram y X (ex Twitter) simulaban ser las vías de comunicación oficiales de bancos conocidos, que operan en el país.

A diferencia del phishing tradicional, en el que el atacante envía comunicaciones "al voleo", en este caso los clientes fueron quienes comenzaron a seguir esas cuentas falsas o las agregaron como parte de sus contactos al verlas en las redes, sin sospechar que la institución bancaria había sido suplantada.

3) Fraudes de compraventa en redes sociales

Para atraer a las víctimas, los estafadores dicen vender productos baratos o importados libres de impuestos. Asimismo, ofrecen garantías y muestran imágenes ficticias (tomadas de la web) de clientes satisfechos, que hacen comentarios positivos por las compras realizadas. La estafa consiste en comprar un producto y realizar el pago, en efectivo o con depósito bancario, para después no recibirlo.

4) Estafas por WhatsApp

Las estafas por WhatsApp consisten en dos etapas:

- **Suplantación de identidad**: el ciberdelincuente busca obtener el código de verificación de WhatsApp de la víctima, usando las técnicas de ingeniería social vistas anteriormente, para clonar la línea.
- **Pedido de dinero**: una vez que logró clonar la línea, suele escribirle a los contactos de esa cuenta pidiendo una transferencia de dinero, haciéndose pasar por el propietario original.

g) Medidas preventivas de ciberseguridad

Es importante recordar que nunca una organización, ya sea pública o privada (como un organismo de gobierno, un banco, una empresa, una tarjeta de crédito o una ONG, entre otras), va a solicitar datos personales de un cliente o usuario por vías alternativas de contacto tales como el correo electrónico, los servicios de mensajería del celular, SMS, redes sociales o sitios web. Por lo general, estos datos se piden cuando es el cliente quien se comunica con alguna de esas organizaciones.

1) Qué hacer para no morder un anzuelo de phishing

- Nunca abras correos electrónicos o ingreses a enlaces que te resulten sospechosos o que no esperabas recibir. Revisá detalladamente la dirección del mail y chequeá cada letra para ver si es la original que ya conocés, es decir, la que figura en la página oficial de tu banco u organización conocida. Los cibercriminales suelen cambiar en una letra, número o símbolo a la dirección web para engañarte.
- Otro factor a tener en cuenta son los errores gramaticales. Tené presente que ninguna empresa seria enviará un correo electrónico que esté mal redactado, no sea claro o tenga faltas de ortografía.
- Tampoco realices ninguna acción si recibís un correo que te indica actuar de forma inmediata, con límite de tiempo o te cause miedo.
- Si recibís un mail desde una casilla general (como Gmail, Outlook o Yahoo) en el que dicen ser una empresa determinada, desconfiá al instante. Por lo general, las empresas o instituciones suelen tener sus propios dominios para las direcciones de correo electrónico

2) Uso de contraseñas robustas

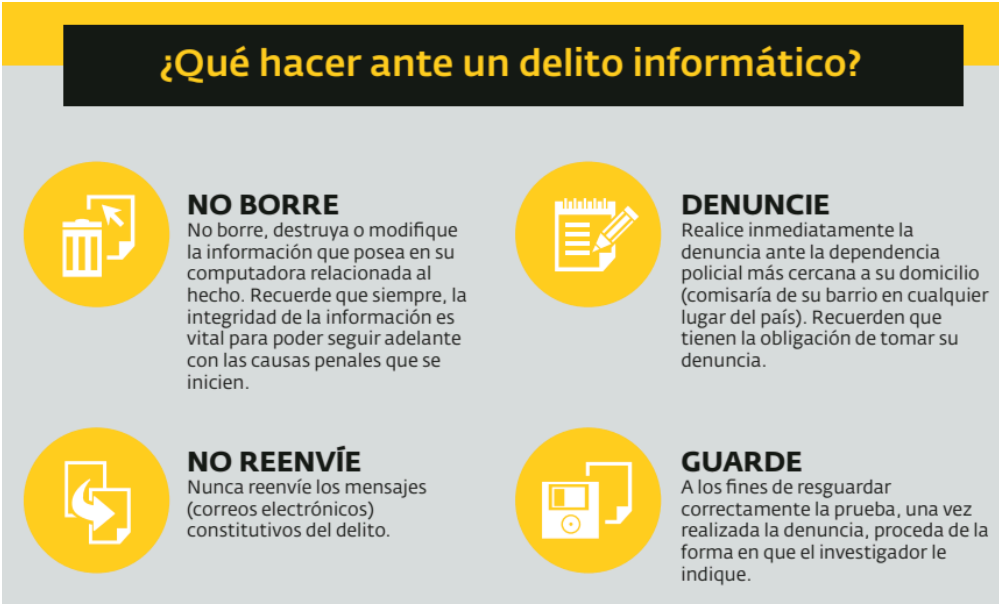
- Debido a la importancia que tienen como medida de protección para la información, deben ser elaboradas de forma robusta, es decir, difíciles de adivinar y fáciles de recordar.
- Es recomendable generar una de más de ocho (8) caracteres utilizando mayúsculas, números y algún carácter especial. También se sugiere no utilizar fechas específicas como día, mes y año de nacimiento, número de dirección postal ni nada que te identifique o puedan asociar con vos.
- Establece un código para el dispositivo y presta atención a quiénes tienen acceso físico a tu teléfono

3) Configuración de WhatsApp

- Nunca compartas tu código de registro ni el PIN de la verificación con otras personas.
- Para evitar el clonado: activá la verificación de dos pasos y proporciona una dirección de correo electrónico en caso de que olvides tu PIN.

h) Dónde y cómo denunciar

- Si sos víctima de una estafa o fraude online, lo primero que tenés que hacer es la denuncia en la comisaría o en la oficina receptora de denuncias que corresponda a tu domicilio.
- Además, podés reportar el caso a la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) enviando un correo a denunciasufeci@mpf.gov.ar.
- Otra oficina que recibe las denuncias es la División Delitos Tecnológicos de la Policía Federal Argentina.
  Correo electrónico: delitostecnologicos@policiafederal.gov.ar



talleres TI

Jefatura de Gabinete de Ministros
República Argentina

Secretaría de Innovación, Ciencia y Tecnología