PROTECCIÓN DE DATOS PERSONALES Y PREVENCIÓN DE ESTAFAS DIGITALES

En la era digital, la protección de datos personales se ha convertido en un tema de suma importancia. Los avances tecnológicos han facilitado la recopilación, almacenamiento y procesamiento de grandes cantidades de información personal, lo que ha aumentado el riesgo de exposición a estafas y fraudes. En este ensayo, se abordarán los conceptos básicos de la protección de datos personales, qué son los datos personales, las estafas digitales, los tipos de estafas digitales y cómo prevenir las estafas telefónicas.

La delincuencia informática y el Abuso Informático la define Gómez Perals como *"El conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos"*. [1]

Protección de datos personales

La protección de datos personales se refiere a las medidas y prácticas destinadas a garantizar que la información personal de los individuos sea tratada de manera segura, confidencial y respetuosa de sus derechos. Esto incluye la recopilación, almacenamiento, uso y divulgación de datos personales.

¿Qué son los datos personales?

Los datos personales son cualquier información que pueda utilizarse para identificar a una persona, como el nombre, la dirección, el número de teléfono, la dirección de correo electrónico, la fecha de nacimiento, entre otros. También pueden incluir información más sensible, como la salud o la orientación sexual.

Es importante proteger los datos personales para evitar su mal uso, como la suplantación de identidad, el fraude financiero o la invasión de la privacidad.

Estafas digitales

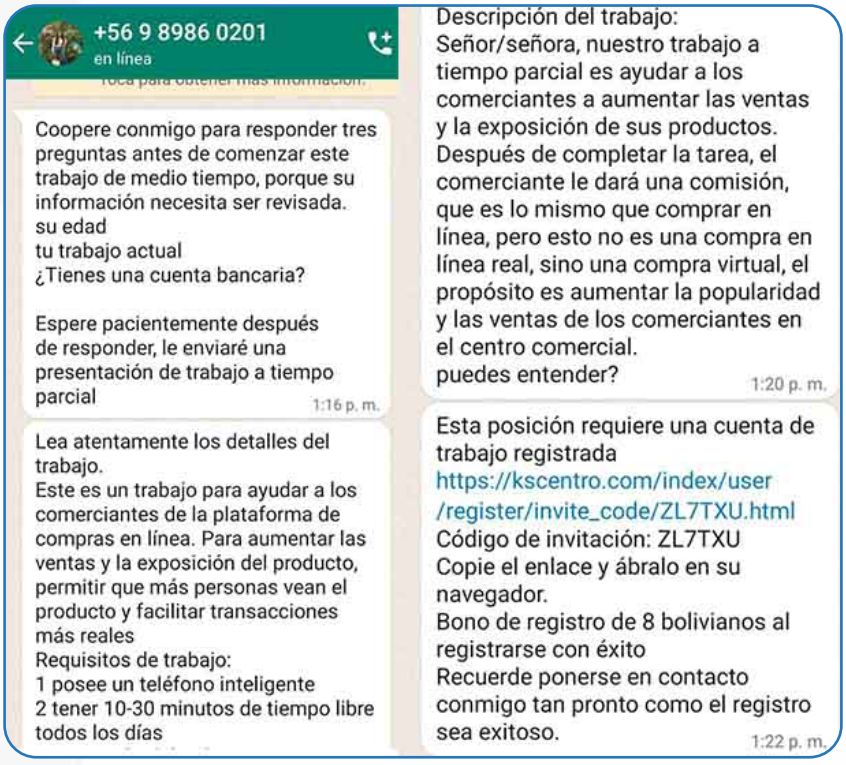
Las estafas digitales son engaños o fraudes realizados a través de medios electrónicos, como correos electrónicos, mensajes de texto, redes sociales o páginas web falsas. Estas estafas suelen tener como objetivo robar información personal o financiera de las víctimas.

Tipos de estafas digitales

a. **Estafas vía WhatsApp:** Los estafadores envían mensajes falsos por WhatsApp u otras aplicaciones de mensajería, haciéndose pasar por amigos o familiares en situaciones de emergencia y pidiendo dinero prestado, venta de datos, suplantación de identidades de personas o instituciones.

1. Libro "Delitos Informáticos" Dr. Santiago Acurio Del Pino Profesor de Derecho Informático de la PUCE página 9

b. **Estafas con ofertas de trabajo:** Los estafadores publican ofertas de trabajo falsas en sitios web de empleo, aplicaciones de mensajería o redes sociales, solicitando información personal o dinero para cubrir supuestos gastos administrativos o de entrenamiento.



c. **Bienes raíces falsos:** Los estafadores publican anuncios de propiedades en alquiler o venta a precios muy bajos para atraer a las víctimas. Solicitan un depósito o pago por adelantado y luego desaparecen sin entregar la propiedad.

d. **Venta falsa de motorizados:** Los estafadores ofrecen vehículos a la venta a precios muy bajos en sitios de clasificados en línea. Solicitan un pago por adelantado y desaparecen sin entregar el vehículo.

e. **Compras en línea:** Los estafadores crean tiendas en línea falsas que ofrecen productos a precios muy bajos. Después de recibir el pago, no envían los productos o envían productos falsificados o de baja calidad.

f. **Estafas en redes sociales:** Los estafadores utilizan perfiles falsos en redes sociales para engañar a las personas para que revelen información personal o financiera, o para vender productos falsificados o de baja calidad, o podrán realizar delitos de trata y tráfico.

En todos estos casos, es importante estar alerta y verificar la autenticidad de las ofertas antes de realizar cualquier pago o proporcionar información personal.

Tipos de estafas en teléfonos móviles

a. **Falsas alertas de virus en tu teléfono.**

Mientras navegabas por la web en tu teléfono, puede que hayas visto aparecer una página con este tipo de alerta. Dirá que un escaneo de tu teléfono ha revelado una infección de virus y te instará a tomar medidas inmediatas.

La estafa hace que descargues una aplicación "antivirus" que en realidad es malware o spyware. Una vez que el código malicioso está en tu teléfono inteligente, los estafadores pueden infectar otros dispositivos o secuestrar el tuyo. La forma más fácil de protegerte de este tipo de ataques es asegurarte de tener seguridad cibernética en el teléfono, como el Antivirus para Android.

b. **Suplantación de identidad por correo de voz**

El phishing por correo de voz o "Vishing" implica llamadas de estafa por teléfono móvil que te incitan a tomar algún tipo de acción. En resumen: los estafadores se harán pasar por una persona u organización auténtica para ganarse tu confianza. Pueden hacerse pasar por una empresa oficial o un servicio del gobierno y te convencen de que debes proporcionar información personal o dinero.

Estas estafas intentan que actúes durante la llamada telefónica. Confían en la urgencia y esperan que el "pánico" te haga reaccionar para que les des lo que quieren. Por este motivo, los estafadores te presionarán para que pagues o compartas información en la llamada, en lugar de pedirte que realices una acción de seguimiento (una vez que hayan colgado).

c. **Suplantación de identidad por SMS**

La suplantación de identidad por SMS o "smishing" implica que un estafador te hace actuar a través de un mensaje de texto.

En estos mensajes pueden enviar enlaces de SMS con contenido malicioso, como malware o spyware y, si abres el enlace, tu dispositivo puede infectarse. Sin embargo, a veces el delincuente te engañará para que ejecutes otro tipo de acción. Ésta puede incluir llamar a un número de teléfono de pago por minuto, engañarte para que te suscribas o coaccionarte para que proporciones información personal.

d. **Estafas de llamadas que solo suenan una vez**

Las estafas de llamadas que solo suenan una vez son llamadas de un número desconocido que solo suena una vez, con la intención de que devuelvas la llamada. Esta estafa funciona porque los estafadores suelen apostar a que la curiosidad anulará tu juicio crítico. Sin embargo, esta es la estafa: te cobran cuando haces la llamada y el estafador se beneficia. Estas llamadas tienden a ser de un código de área internacional, que es parte de como cobran las tarifas. En ocasiones, se dejará un mensaje de voz para aumentar la posibilidad de que actúes. Así que ten cuidado si recibes una llamada o un mensaje de voz de un número que no reconoces o del que no esperas una llamada.

Prevención de estafas telefónicas y digitales

a. **Mantén tus dispositivos seguros:** Instala y actualiza regularmente software antivirus y antimalware de sitios oficiales o con asesoramiento. Mantén actualizado el sistema operativo y las aplicaciones para proteger tu dispositivo contra vulnerabilidades.

b. **Utiliza contraseñas seguras:** Crea contraseñas fuertes y únicas para cada cuenta. Considera utilizar un administrador de contraseñas para gestionarlas de forma segura.

c. **Verifica la autenticidad de las fuentes:** Antes de hacer clic en enlaces o descargar archivos adjuntos, verifica la autenticidad del remitente y la URL. Evita abrir correos electrónicos sospechosos o enlaces de fuentes desconocidas.

d. **Ten cuidado con las ofertas *"demasiado buenas para ser verdad"*:** Si una oferta parece demasiado buena para ser verdad, probablemente lo sea. Sé escéptico ante ofertas de productos o servicios a precios extremadamente bajos.

e. **Protege tu información personal:** Nunca compartas información personal o financiera a través de correos electrónicos, mensajes de texto o llamadas no solicitadas. Verifica la autenticidad de la empresa o persona antes de proporcionar información sensible.

f. **Usa redes Wi-Fi seguras:** Evita conectarte a redes Wi-Fi públicas no seguras. Utiliza una red privada virtual (VPN) si necesitas acceder a información sensible mientras estás en una red Wi-Fi pública.

g. **Mantente informado:** Mantente al día con las formas de estafas y fraudes en línea más recientes para poder reconocer posibles amenazas. Presta atención a las alertas de seguridad y consejos de organizaciones confiables.

h. **Verificar si los números son oficiales:** No ingreses a links remitidos por números sospechosos.

Prácticas a seguir para prevenir el robo de información

a. **Mantener el software actualizado:** Mantén actualizados todos los programas y sistemas operativos para protegerse de vulnerabilidades conocidas.

b. **Cifrar los datos sensibles:** Utiliza herramientas de cifrado para proteger los datos sensibles tanto en reposo como en tránsito.

c. **Utilizar autenticación de dos factores:** Habilita la autenticación de dos factores siempre que sea posible para agregar una capa adicional de seguridad.

d. **Realizar copias de seguridad:** Realiza copias de seguridad de forma regular y asegúrate de que estén almacenadas de forma segura.

Siguiendo estas prácticas, puedes reducir significativamente el riesgo de robo de información y proteger mejor tus datos en un mundo digital cada vez más peligroso.

Bibliografía

- Ley N° 303 de Protección de Datos Personales de Bolivia
- Agencia de Protección de Datos de la Unión Europea. “Qué son los datos personales y cómo protegerlos”. Disponible en: https://edps.europa.eu/data-protection/our-work/subjects/data-protection_es
- Comisión Federal de Comercio de Estados Unidos. “Cómo evitar las estafas telefónicas”. Disponible en: https://www.consumer.ftc.gov/es/articles/0208-como-evitar-las-estafas-telefonicas
- Store Adam. Ciberseguridad: La protección de la información en un mundo digital.
- https://latam.kaspersky.com/resource-center/threats/how-to-avoid-mobile-phone-scams
- Libro “Delitos Informáticos” Dr. Santiago Acurio Del Pino Profesor de Derecho Informático de la PUCE