UNIVERSIDAD DE COSTA RICA

C+T

CIENCIA MÁS TECNOLOGÍA

Con una mejor cultura digital disminuyen los riesgos de una estafa informática

La mayoría de los casos de los delitos informáticos ocurren por factores humanos mediante técnicas de ingeniería social.

8 NOV 2023 Ciencia y Tecnología

En las estafas informáticas median, por lo general, factores humanos. Por esto, debemos desarrollar mucha malicia digital para no caer en el engaño de las redes dedicadas a este negocio.

Isabel se encontraba esa mañana en su casa atendiendo a unos trabajadores de la construcción cuando **sonó su teléfono celular.**

—Buenos días, señora. Le hablamos de parte del Banco Continental para informarle que **hay un problema con su cuenta**, el cual debe ser resuelto lo antes posible.

—¿Y cuál será el problema? Es que en este momento estoy ocupada y **no puedo atenderlo.**

—No le vamos a quitar mucho tiempo, es rápido y es muy importante para usted porque **su cuenta corre peligro**, en cualquier momento le podrían sustraer el dinero.

—Este... es que como le dije, en este momento estoy ocupada. ¿Podría llamarme más tarde?

—Es que **esto es urgente**, son solo un par de minutos. Usted no tiene que hacer nada, nada más **le mandamos un enlace por WhatsApp y usted le da clic**. Con solo eso nosotros corregimos de inmediato el problema técnico.

La historia de Isabel, aunque ficticia, no tuvo un final feliz. Todos los días se repite y es similar a la de muchas personas que son **víctimas de los fraudes informáticos** por medio de una llamada telefónica, un correo electrónico, el hackeo de su perfil de Facebook o de su información personal por medio de una red no segura de wifi.

Este fenómeno **está presente en todo el país**. Aunque las provincias del Área Metropolitana son las que reportan más casos, ya se presentan denuncias en Guanacaste, Puntarenas y Limón.

Todo esto ocurre **en un abrir y cerrar de ojos,** sin que nos percatemos de que estamos siendo estafados. Es, posteriormente, cuando nos damos cuenta de que **caímos en las estratagemas de los grupos de ciberdelincuentes** dedicados a dicho negocio.

El *vishing* es un tipo de fraude por medio de llamadas telefónicas, en las cuales **el atacante suplanta la identidad de una institución, empresa o persona** con el propósito de obtener

información personal de la víctima. Es lo que le ocurrió a Isabel, quien creyó que realmente la contactaban del banco en donde ella guardaba su dinero.

Al hacer ella clic en un enlace, **instalan un *softwar*e de gestión remota** para ver el contenido de una cuenta bancaria y luego capturar la información.

El artículo 217 bis del **Código Penal** costarricense establece **una pena de tres a seis años de prisión** por el delito de estafa informática. La sanción será de **cinco a diez años de prisión** si las conductas son cometidas contra **sistemas de información públicos, sistemas de información bancarios y de entidades financieras** o si el autor del fraude es una **persona encargada de administrar o dar soporte a un sistema** o red informática.

De acuerdo con el Foro Económico Mundial, el **95 % de los delitos e incidentes informáticos ocurren por factores humanos;** es decir, "el ser humano es el punto donde se focaliza toda la energía del ataque", explica el Ing. Abel Brenes Arce, oficial de seguridad de la información (CISO, por sus siglas en inglés) de la Universidad de Costa Rica (UCR).

Las diferentes **técnicas de manipulación que usan los ciberdelincuentes** para engañar a los usuarios y obtener información confidencial es lo que se conoce como **ingeniería social.**

Las personas son el blanco principal de las técnicas de manipulación (conocidas como ingeniería social) que los atacantes usan para engañar a las personas y obtener información confidencial.

Foto: Laura Rodríguez Rodríguez.

¿Por qué este acercamiento hacia el usuario? Brenes considera que **los ciudadanos no son conscientes de la cantidad de información que manejan** y de la importancia de resguardarla. Nos referimos a claves, acceso a sistemas informáticos, datos confidenciales personales o de su lugar de trabajo, por ejemplo.

Se busca atacar a las personas que usan los sistemas informáticos para **obtener información valiosa de ellos.** Por tanto, no hay en primera instancia un ataque directo a las máquinas, sino que este se efectúa de forma indirecta.

En palabras del ingeniero informático y abogado especialista en ciberseguridad Roberto Lemaitre Picado, profesor de la Escuela de Ciencias de la Computación e Informática de la UCR, **"nuestro sistema operativo humano es muy vulnerable".**

Los cibercriminales **se aprovechan de la condición humana**, desde quienes quieren ayudar a otros o creen mediante engaño que ganaron un premio sin haber participado en ninguna actividad, hasta las personas que dan por cierta una herencia que no esperaban.

"Los atacantes son **depredadores del comportamiento y de las emociones humanas**", complementa Brenes.

Métodos sofisticados

Lemaitre confirma que el cibercrimen no ha dejado de avanzar. **La pandemia por el COVID-19 marcó un antes y un después en este tipo de acciones**, ya que muchos criminales tradicionales evolucionaron hacia actividades más sofisticadas.

De hecho, durante ese período de emergencia sanitaria disminuyeron los asaltos físicos a las personas y **aumentaron los ataques por medios informáticos.**

Con la **inteligencia artificial,** los ciberataques han aumentado y las capacidades de los delincuentes también se han fortalecido para acceder a dichos recursos tecnológicos.

Este campo de la informática **permite mejorar los mensajes para que parezcan más reales** y cada vez es más difícil identificar las fuentes de la estafa, puntualizan los expertos.

"El ***phishing*** —indica Lemaitre —, que se usa mucho para estafas informáticas, inicialmente era muy difundido, mal redactado y con temas poco precisos. Ahora **ha mejorado y se ha venido especializando".**

Esta técnica de ingeniería social se dirige a **ciertos segmentos de la población**, entre estos los adultos mayores, pues se aprovechan del desconocimiento del uso de la tecnología debido a la brecha digital.

También buscan **información en las redes sociales y en internet de ciertas personas de su interés**, ya sea por las características de su perfil, su trabajo o su condición económica.

Brenes detalla que existen **tres fases en la estrategia de los fraudes informáticos**. La primera fase es la recolección de la información de la víctima.

Denuncias de estafas informáticas en el Organismo de Investigación Judicial (OIJ)

A octubre del **2023**: **3 846** denuncias

2022: **5 318** denuncias

"Los ciberdelincuentes **hacen previamente una investigación de la persona**, principalmente en las redes sociales, y empiezan así a planificar el ataque. Entonces disponen de mucha información, lo que lleva a pensar que el mensaje es legítimo", afirma.

Luego viene la fase de **adquirir confianza con la persona** a través de llamadas telefónicas, mensajes por las redes sociales y correos electrónicos, con el fin de construir una relación armoniosa.

En la tercera fase empieza **la manipulación que al ciberdelincuente le interesa** para obtener cierta información más específica y así llegar al dinero.

"La salida consiste en **irse sin dejar pruebas y con el objetivo satisfecho.** Es tratar de que no les den seguimiento", finaliza.

Más cultura digital

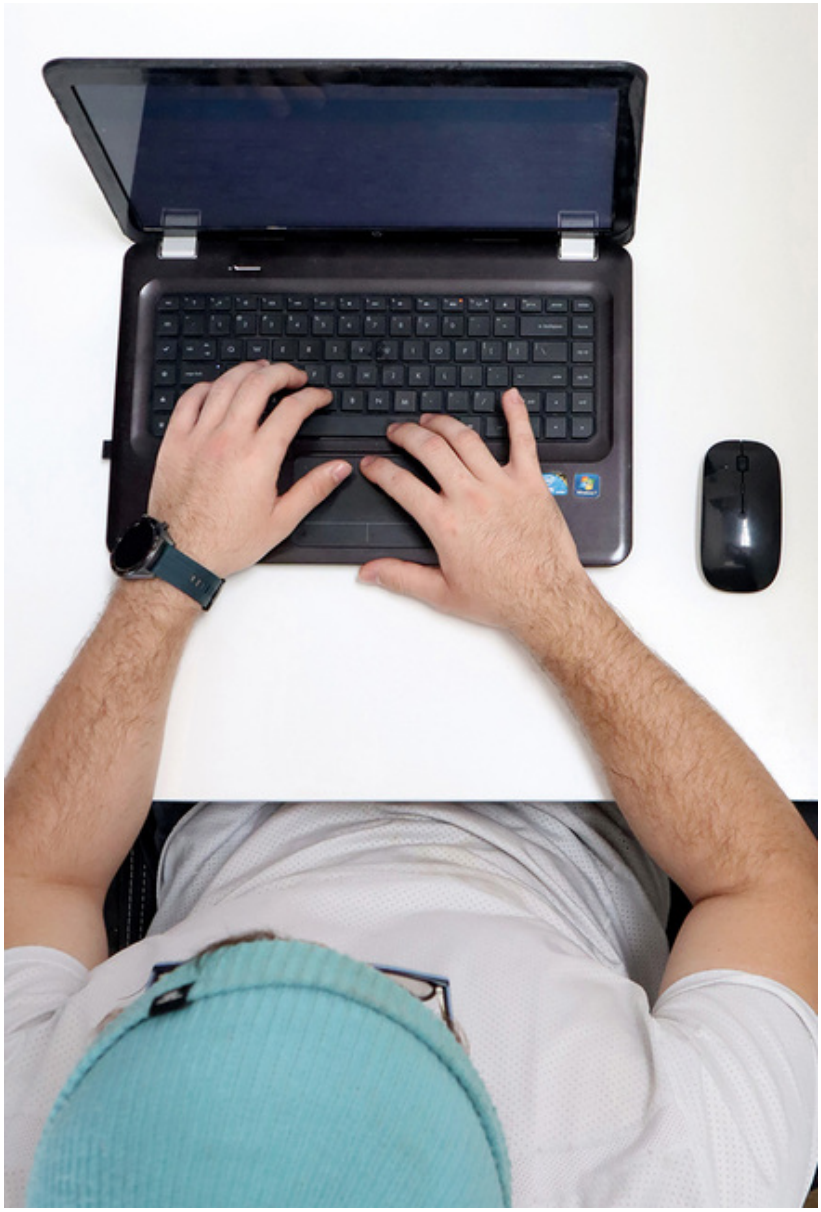
El director del Organismo de Investigación Judicial (OIJ), Randall Zúñiga López, reveló al periódico *La República* que, del 2017 al año en curso, el **monto de las estafas informáticas se triplicó** en el país, al pasar de **4 000 millones de colones a 12 000 millones de colones.**

Los expertos de la UCR enfatizan en la necesidad de que haya **mayor responsabilidad y cultura digital por parte de la ciudadanía**, para que esta adquiera conciencia sobre el valor de la información que maneja y cómo protegerse de los cibercriminales.

Brenes recuerda que uno como ciudadano digital debe ser responsable y cuidar la huella. "**Todo lo que hacemos en internet no es privado,** la información sobre nuestros movimientos en la red es recolectada por los sistemas de trazabilidad", aclara.

Para Lemaitre, se debe apostar a una **formación sobre cultura digital** muy fuerte en todos los niveles etarios, desde la niñez, para que los usuarios estén mejor preparados sobre el uso y funcionamiento de la tecnología y el accionar de estos grupos criminales.

Las **estrategias nacionales de ciberseguridad** deben incluir la creación de programas de formación con énfasis en las poblaciones más vulnerables, manifiesta. En este momento, Costa Rica tiene dicha estrategia en período de consulta.



Como usuaria de la tecnología, la ciudadanía debe ser más responsable y consciente del valor de la información que maneja y cómo protegerse de los ciberdelincuentes.

Foto: Laura Rodríguez Rodríguez.

Las instituciones también deben tener **mecanismos de seguridad tecnológica** y toda una infraestructura que dé garantía de protección de sus sistemas informáticos y de la información que resguardan.

De acuerdo con Brenes, son muy importantes las **campañas de educación y sensibilización** en este sentido, para que las personas aprendan que la información es estratégica y tiene un gran valor institucional. “Es un proceso de recordación permanente”, recalca.

Reto global

Los grupos de cibercriminales **actúan globalmente**, como lo hace el crimen organizado en otros campos.

El internet no tiene límites, razón por la cual los países se enfrentan al reto de definir cuál debe ser la respuesta jurídica y técnica ante los fraudes informáticos.

En Latinoamérica, **algunas naciones han venido avanzando en la atención de los delitos informáticos** y en la creación de **grupos especializados de atención de esta materia en los órganos de investigación judicial y policial.**

El Convenio sobre Ciberdelincuencia, conocido como el **Convenio de Budapest**, fue firmado en 2001 y tiene como objetivo proteger a la sociedad contra el cibercrimen. Costa Rica es uno de los países firmantes de tal documento.

Lemaitre destaca la importancia de este instrumento para que **los países miembros puedan colaborar en la investigación y persecución de estas faltas,** las **incorporen a sus marcos jurídicos** y dispongan de equipos especializados que atiendan esta problemática.

Al ser un tema que trasciende las fronteras, se necesita **mucha colaboración para poder investigar y conseguir en otro territorio la información** que se requiere para entender cómo se cometió un delito y buscar a las personas responsables.

Sin embargo, aunque las normativas jurídicas son importantes, se deben tener establecidas las **buenas prácticas y estándares** para el buen funcionamiento de la parte operativa. En esta materia, señala Lemaitre, **nuestro país tiene una calificación baja.**

"Esto implica que los marcos de seguridad nos permitan tener buenas prácticas en las organizaciones e instituciones, con protocolos adecuados y con formación para que los funcionarios tengan claro qué hacer. **Esto baja el riesgo**", concluye el especialista.

Patrones que se repiten en las denuncias sobre la forma en que los delincuentes abordan a las personas para estafarlas:

-Falso funcionario o funcionaria bancaria

-Falso funcionario gubernamental

-Falso funcionario municipal

-Falso empleador

-Página falsa en los buscadores de internet

-*Phishing* (envío de correos electrónicos que suplantan la identidad de instituciones o empresas y solicitan información personal y bancaria al usuario).

-Venta o alquiler falso

Fuente: Organismo de Investigación Judicial (OIJ).

Consejos de ciberseguridad

-Desarrollar la malicia y la alerta digital para no caer en engaños.

-Nunca atender una llamada telefónica cuando le dicen que procede de un banco. Cuelgue y llame usted al banco.

-No brindar datos personales a desconocidos.

-Evitar conectarse a una red desconocida. Y si lo hace, se recomienda tener en el teléfono o en la computadora un *software* antivirus y anti *malware* que le permita crear una red privada virtual (VPN).

-No abrir correos de usuarios desconocidos y revisar la procedencia del mensaje.

-Verificar la seguridad de los sitios web.

-No compartir contraseñas.

-Verificar la identidad de la persona con quien se está hablando.

-Mantener el equipo informático actualizado.

-Tener doble autenticación en las cuentas personales.

-Conectarse desde la casa por medio de una VPN.

-No apresurarse a darle clic a los enlaces. Tener precaución y revisar primero el enlace. Se debe copiar a mano para validar el mensaje.

-Capacitarse para entender cómo funciona la tecnología, por ejemplo, un teléfono celular o una computadora y sobre cuáles medidas de seguridad debo tomar.

Fuentes: Roberto Lemaitre y Abel Brenes, expertos en ciberseguridad de la UCR.

Patricia Blanco Picado
Periodista Oficina de Comunicación Institucional
Área de cobertura: ciencias básicas
patricia.blancopicado@ucr.ac.cr