02/11/2023

Juan Carlos Galindo: “Si existe el crimen perfecto es la ciberestafa”

El autor de “Ciberestafas, la historia de nunca acabar” de 0xWord analiza en esta entrevista el panorama de las estafas digitales

Ciberestafas, la historia de nunca acabar. Este acertado título describe una situación que se lleva dando mucho tiempo. Y es que la **ciberestafa**, las estafas digitales a las que todos estamos expuestos, son en realidad una extensión de las estafas tradicionales, pero con la capacidad de tener un alcance mucho mayor. Una realidad que conoce perfectamente el autor de **la historia de nunca acabar**, Juan Carlos Galindo, título publicado por 0xWord que ha alcanzado ya su segunda edición, que amplía y actualiza el contenido de la primera.

Con **prólogo de** Chema Alonso y epílogo del **Magistrado-Juez de la Audiencia Nacional**, Eloy Velasco, el libro sumerge al lector en una historia de principio a fin del fraude online, desde su concepto, su historia, la evolución y migración al ciberespacio y por supuesto la prevención y su lucha, sin olvidar otros aspectos cruciales como son explorar quiénes son las víctimas de este tipo de estafas.

Y es que, uno de cada cinco delitos se comete en internet. ¿Los motivos? Son muchos. Pra empezar, un ciberdelincuente **«puede multiplicar por 10 sus beneficios sin apenas riesgo y reduciendo su exposición a ser detenido»** apunta Galindo, quien nos ofrece en esta entrevista a través de MyPublicInbox con una precisa panorámica de la situación actual de los fraudes y ciberestafas.

Por eso, no solamente es importante entender **cómo llevan a cabo las estafas digitales** los ciberestafadores modernos, también es necesario **bucear en cómo se ha llegado hasta aquí**, trasladando las estafas del ámbito físico al digital.

Pregunta: Dos ediciones ya, y sumando, porque el libro está teniendo un merecido éxito. ¿Por qué te lanzaste a escribir este libro, qué te llevó a ello?

Respuesta: Muchas gracias. Pues fue una deriva profesional. Te explico. Desde el año 2012 soy experto externo (inscrito ante el SEPBLAC) en prevención del blanqueo de capitales y de la financiación del terrorismo y desde el año 2015/16 empezamos a detectar un aumento imparable del mismo, producto del cibercrimen. Este hecho me llevó a formarme y a interesarme por el fenómeno. Ya que un ciberestafador, además de preparar su ataque con herramientas tecnológicas, necesita un número de cuenta para cometerlo y mover su dinero (mulas) y el movimiento de dinero (ilícito) es considerado se como blanqueo de capitales, así como de una identidad falsa (falsificación documental). Estos fueron los factores que me hicieron especializarme en este sector tan concreto. Y una vez en él, me di cuenta del abandono más absoluto de las víctimas de estafa y su falta de regulación legislativa e investigativa para poder perseguir el delito.

P: Se suele decir que somos muy inocentes en internet, y que por eso caemos en todo tipo de estafas (suplantación de identidad o phishing, fraudes pero lo cierto es que toda la vida siempre el ser humano ha sido víctima de estafas, al creernos que algo bueno puede ser verdad. ¿Cómo han evolucionado las estafas del mundo físico al digital?

R: Lo describo con precisión en el libro donde no solo recoge cómo se realizan las Ciberestafas más modernas cometidas por los estafadores, sino que también deambula por el pasado del fenómeno para entender su calado social y psicológico. Describe con precisión las decenas de tipologías de fraudes y estafas reales, para poder identificarlas en la vida cotidiana. También nos cuenta

con claridad, cuáles son las medidas más eficaces para su mitigación, tanto en el entorno de la empresa como el particular, así como los sistemas de prevención más eficaces.

En definitiva, es una evolución del ser humano como sociedad (conducta desviada) y la evolución del crimen organizado, como parte de ella. Te imaginas cuando al capo tradicional de la delincuencia organizada, le comentas que **puede multiplicar por 10 sus beneficios sin apenas riesgo y reduciendo su exposición a ser detenido en casi un 90%** ☀ pues eso, en cuanto lo probó y vio el resultado, migró de inmediato al cibercrimen.

P:¿Y cómo hemos evolucionado los usuarios como víctimas de los fraudes?

R: Sin lugar a duda, **hemos involucionado**. En la parte física ya conocíamos los riesgos y habíamos tomado medidas contra los posibles delitos que pudiéramos sufrir. Estafas, fraudes, secuestros, extorsiones, amenazas, etc. Pero en la red somos unos recién nacidos. Como te comentaba desde el año 16 notamos el repunte de este delito, pero lo que lo ha catapultado al estrellato de la delincuencia organizada fue el COVID y la crisis bancaria, que obliga a sus usuarios a trabajar desde internet, tenga la edad que tengan y el propio estado que obliga a relacionarse con ellos de manera telemática. Estos factores han hecho que de repente millones de personas estén navegando (o, mejor dicho, naufragando) en internet desconociendo los riesgos altísimos que eso conlleva.

P: ¿Somos más proclives a caer en ciberestafas? ¿Por qué, cuál es el motivo sociológico, o psicológico?

R: Sí, sin dudarlo. Los motivos son los mismos, siempre han sido los mismos. El ser humano siempre ha buscado la ganga, el chollo, lo barato, inclusive, en ocasiones aprovecharse del prójimo y eso no ha cambiado. Pero ahora es en un entorno que desconoce y donde el chollo y la ganga es el objetivo.

Existen cuatro (cinco) grandes agentes socializadores: La familia, el colegio, los amigos y los medios de comunicación y yo añadiría internet y ahí, empiezan nuestros problemas. Hasta la fecha, en mayor o menor medida, los cuatro grandes agentes socializadores se podían calificar por etapas de vida, por edades, escalas sociales, etc. Pero llegó internet y lo cambió todo. De ahí que exista una gran brecha entre los nativos digitales y los que no. También tenemos que contar con el tiempo de exposición en internet que se ha multiplicado por diez en pocos años y el número de usuarios, que hace que aumenten exponencialmente las víctimas de estos delitos.

P:Como especialista en conducta criminal en la web y en ingeniería social, ¿observas diferencias entre los criminales "tradicionales" y los ciber estafadores, ¿qué caracteriza a estos últimos?

R: Por supuesto que existen diferencias. Sobre todo, en el modus operandi. Ten en cuenta que en la parte física se necesita tener ciertas cualidades para poder llevar a cabo la estafa. Me vienen a la memoria, desde los trileros, los del timo de la estampita o los del timo del nazareno. Se necesita para su comisión personas con ciertas aptitudes y actitudes que no tiene cualquiera. Si pasamos a la extorsión, a la amenaza o al secuestro, ni te cuento. Se necesitan personas con sangre fría, psicopatía, etc. Pero muy valientes para estar cara a cara con la víctima. Además, de una organización jerarquizada con mucho riesgo de fuga de información y muy cara de mantener.

En cambio, en el ciberespacio no hace falta nada de eso. No hay contacto físico, no hace falta ser muy ducho con el don de la palabra, ni siquiera hay que tener buen parecido. **En el ciberespacio soy cualquiera**. En cuanto a su comisión, es sencilla, muy automatizada y cómoda. Casi lo puede hacer cualquiera. Nadie te ve y no hay prisa (porque gestionan decenas de estafas a la vez) El ransomware ha sustituido con éxito al secuestro físico. Los mails y las redes sociales son utilizadas para amenazar, coaccionar y extorsionar, sin riesgos de ser puestos a disposición judicial, gracias a la internacionalización de este tipo de delito, ya que lo cometen desde fuera del país del estafado. Dificultando así su seguimiento, su averiguación de identidad y, por ende, su detención. **Si existe el crimen perfecto es la ciberestafa.estos delitos.**

P: ¿Cuáles son los fraudes online más populares en la actualidad?

R: Los ataques de ingeniería social, sin duda. Déjame antes de continuar con mi explicación que defina que es la ingeniería social para que el lector sepa de qué hablamos. Las técnicas de ingeniería social se basan en **la ciencia de la motivación humana**.

Manipulan las emociones y los instintos de las víctimas de maneras que se sabe que impulsan a las personas a realizar acciones que no les favorecen. La ingeniería social manipula a las personas para que compartan información que no deberían compartir, descarguen software que no deberían descargar, visiten sitios web que no deberían visitar, envíen dinero a delincuentes o bien cometan otros errores que comprometan sus activos o seguridad personal o empresarial.

Por un lado, **el phishing**. Los ataques de phishing son mensajes digitales o de voz que intentan manipular a los destinatarios para que compartan información confidencial, descarguen software malicioso, transfieran dinero o activos a las personas equivocadas o realicen alguna otra acción dañina. Los estafadores diseñan los mensajes de phishing de tal manera que parezca que provienen de una organización o persona fiable o creíble, a veces incluso una persona que el destinatario conoce personalmente.

Hay muchos tipos de estafas de phishing: **los correos electrónicos de phishing en masa** se envían a millones de destinatarios al mismo tiempo. Parecen enviados por una gran empresa u organización reconocida y realizan una solicitud genérica como «estamos teniendo problemas para procesar su compra; por favor, actualice su información de crédito».

El **spear phishing** se dirige a una persona específica, normalmente alguien con acceso con privilegios a la información del usuario, la red de sistemas o fondos corporativos.

El **whaling** es un tipo de spear phishing dirigido a una persona de alta visibilidad, como un director ejecutivo o una figura política. En el Business Email Compromise (BEC), el hacker utiliza credenciales comprometidas para enviar mensajes de correo electrónico desde la cuenta de correo electrónico real de una figura de autoridad, lo que hace que la estafa sea mucho más difícil de detectar.

El **phishing de voz o vishing**, es un phishing realizado a través de llamadas telefónicas.

El **phishing por SMS, o smishing**, es phishing a través de mensajes de texto.

El **angler phishing** es phishing a través de cuentas falsas en redes sociales que se hacen pasar por la cuenta oficial del servicio al cliente o de equipos de soporte al cliente de empresas fiables.

De acuerdo con el informe sobre el coste de una brecha de seguridad en los datos de 2021 de IBM, el phishing es el método de envío de malware más común y la segunda causa más común de filtraciones de datos.

En cuanto al **baiting**, la estafa nigeriana es probablemente el ejemplo más conocido de esta técnica de ingeniería social. Más ejemplos actuales incluyen las descargas de software, música o juegos gratuitos pero infectados con malware.

En el **pretexting**, el estafador crea una situación falsa para la víctima y se hace pasar por la persona adecuada para resolverla. Muy a menudo (e irónicamente), el estafador afirma que la víctima se ha visto afectada por una brecha de seguridad y le ofrece solucionarla si esta le proporciona información de cuenta importante o control sobre su sistema o dispositivo (técnicamente hablando, casi todos los ataques de ingeniería social implican algún nivel de pretexting).

Te podría contar muchas más, pero estaríamos todo el día y con las que te he comentado, cubrimos prácticamente el 85% de las ciberestafas. Pero déjame que te cuente cual es el lema de los ingenieros sociales. No existe nada más seguro, que una máquina (ordenador, Tablet o móvil) esté desconectada de internet y/o de la red eléctrica. Para un ingeniero social no es ningún problema ya que “encontraremos a una persona que lo encienda y lo conecte a internet”

«Muchas víctimas no denuncian por miedo o vergüenza»

P:Los usuarios ciertamente somos aún □□□□□□□A en el mundo digital, y necesitamos un poco de guía y de luz para discernir lo que es un fraude de lo que no. ¿Cuáles son los consejos básicos que sueles dar en este sentido?

R: Así es. En primer lugar y no me cansaré de repetirlo, los bancos, financieras, empresas telefónicas, eléctricas, gasísticas, agua, agencia tributaria, ayuntamiento, etc. nunca te van a pedir datos que ya tienen, ¡¡nuncaii por lo tanto si piden datos es la primera alerta temprana de que es una estafa y sobre todo si te piden tu número PIN de la tarjeta de débito o crédito.

En segundo lugar, navegar en páginas confiables que ya hayas usado antes. En tercer lugar, paga sólo a través de PayPal o en la

red redsys o similar y nunca salgas de la página web que estés comprando para pagar fuera de la misma y mucho menos en criptomonedas.

En cuarto lugar, no tengas prisa, compra con calma. No compartas nada rápidamente dedícale unos segundos. Las prisas son malas consejeras.

En quinto lugar, activa el doble factor de autenticación en todas tus RRSS, cuentas corrientes, correos-e y en otras aplicaciones.

En sexto lugar, aprende a decir NO y sobre todo no des información a nadie.

En séptimo lugar, no pinches en enlaces desconocidos y no abras correos electrónicos o SMS que te informen de algún problema. Jamás lo hacen por ese medio. Es preferible pecar de incrédulo a que te roben todo tu dinero.

En octavo lugar, mantén tu equipo actualizado, instala antivirus, ten contraseñas robustas y cambiarlas por lo menos una vez al año. No te descargues programas gratuitos o sin licencia.

Pero, sobre todo, antes de clicar un enlace o iniciar una descarga …piensa, no tengas prisa.

P:Como bien se titula tu libro, este es el cuento de □□□□□ acabar A□ ahora además llegan nuevas técnicas impulsadas por IA y otras tecnologías que están haciendo más fácil a los estafadores desarrollar fraudes, y será todavía más difícil a los usuarios diferenciar algo real de una estafa. ¿Cómo vislumbras este futuro? ¿Y cómo podremos los usuarios defendernos de estas técnicas?

R: El futuro no es bueno, nada bueno. Los legisladores españoles están a otra cosa, por desgracia. Parece que nos les importe el millón de víctimas anuales que sufren este tipo de delitos y que se sienten solas, abandonadas, sin que nadie les haga caso, ni tan siquiera son escuchadas. Es más, en ocasiones son tratadas como tontas, de ahí, que **muchas víctimas no denuncien por miedo o vergüenza.**

La parte investigativa es también muy compleja, donde nuestra LECRIM necesita de adaptaciones al siglo XXI tal y como ha hecho recientemente nuestro código penal con la reforma del delito de estafa. Aunque a posteriori se encuentren con la problemática del principio de soberanía nacional, ya que estos delitos se cometen en su inmensa mayoría fuere del territorio nacional. Y muchos países se han convertido en países refugio o □□□□□□ atacantes A que en un porcentaje muy elevado coinciden con los paraísos fiscales. Y que junto al uso de internet que permite el anonimato casi absoluto hace que la identificación fehaciente de las personas que están detrás sea prácticamente imposible. En cuanto a la recuperación del dinero y casi por los mismos motivos, es prácticamente imposible su recuperación.

Con formación e información y con mucha cautela. El ámbito represivo no es eficaz, a fecha de hoy, en esta tipología de delitos. Vamos siempre por detrás del malote y la recuperación de nuestro dinero y la encausación de la persona que cometió el delito es casi improbable. No existe la justicia restaurativa.

Solo nos queda la prevención de este tipo de delitos y tampoco existe nada al respecto. No existen leyes de obligado cumplimiento, ni oficinas, ni agencias y las que hay, no van en la misma dirección. Prácticamente están enfocadas en el ámbito de lo público. Nada de nada para los ciudadanos. Necesitamos políticos valientes que no miren su cortoplacismo y su silla, y estén orientados, de verdad, a la ciudadanía. En estos momentos y es triste decirlo, una persona que sufra una ciberestafa está sola, nadie la va a ayudar. Depende de sus recursos, para intentar recuperar su dinero y poner de patitas en prisión a los malotes que le robaron su dinero.

Puedes encontrar su libro y contactar con Juan Carlos Galindo a través de MyPublicIbox

Fuente: Bit Life media

LINK DE LA NOTICIA