



Delitos informáticos en Argentina: modalidades detectadas durante la pandemia del COVID-19

Recomendaciones preventivas
para los ciudadanos.



¿Qué es un delito informático?

Los delitos informáticos o ciberdelitos son todas aquellas conductas ilícitas o ilegales que vulneran derechos o libertades de las personas y utilizan un dispositivo informático como medio para la comisión del mismo o como fin.

Un dispositivo informático es toda aquella tecnología que procesa automáticamente datos e información, como por ejemplo, una computadora, un celular inteligente, una tablet, una televisión inteligente, una consola de videojuegos o cualquier dispositivo que tenga conexión a Internet, entre otros.

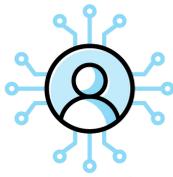
El dispositivo actúa “como medio” para la comisión de un delito, por ejemplo, cuando una persona amenaza o acosa a otra u otras y lo realiza a través de esta tecnología. Y actúa “como fin” cuando el blanco del delito es la propia tecnología, por ejemplo, cuando un malware o software malicioso, como un virus, afecta y altera el normal funcionamiento del dispositivo o los datos y la información que almacena.

En este sentido, el cibercrimen no representa un tipo de criminalidad específica en tanto que nuclea a un conjunto de delitos que adoptan esta definición por el lugar que ocupa la tecnología, más que por la naturaleza criminal del acto mismo. La definición de delitos informáticos es instrumental.

Durante los dos primeros años de la pandemia del COVID-19, en Argentina, se produjo un incremento de denuncias sobre diferentes modalidades delictivas sucedidas en Internet. El aumento de casos pudo surgir por un mayor uso de las Tecnologías de la Información y las Comunicaciones, de servicios y aplicaciones de Internet, surgidos a partir de la implementación del teletrabajo, la educación a distancia y el pago de servicios, generado por el aumento del comercio electrónico.

Una característica propia de los delitos informáticos cometidos en este contexto excepcional de pandemia **es una mayor sofisticación y complejidad en las técnicas** de comisión de estos ilícitos, tanto así como la aparición de asociaciones ilícitas y de bandas con cierto grado de organización, que toman al cibercrimen como emprendimiento delictivo.

Las modalidades detectadas más frecuentes pueden agruparse en tres tipos: *los fraudes y estafas en línea* a nivel de usuarios particulares, los ataques de *ransomware* a organizaciones y *el blanqueo ilícito de capitales por Internet*. Esto arroja como resultado la presencia de **nuevas modalidades de delitos ya existentes.**



Fraudes y estafas en línea a usuarios particulares

Para la Organización para la Cooperación del Desarrollo Económico (OCDE), “un fraude es la adquisición indebida de bienes ajenos por medio del engaño”¹. Es una acción que se comete con el objetivo de producir un perjuicio a una persona, organización o al Estado mediante un engaño o trampa en beneficio de quien lo practica. Puede realizarse a través de una ocultación, falsificación o artificio, entre otros.

El fraude económico suele ser entendido como estafa cuando el objetivo del engaño es producir a la víctima un perjuicio de tipo patrimonial –financiero o material– con un fin puramente lucrativo en beneficio del autor.

Para el Departamento de Justicia de los Estados Unidos, el fraude por Internet es “cualquier tipo de esquema de fraude que utiliza uno o más componentes de Internet, como salas de chat, correo electrónico, tableros de mensajes o sitios web, para presentar solicitudes fraudulentas a posibles víctimas, realizar transacciones fraudulentas o transmitir el producto del fraude a instituciones financieras u otras personas relacionadas”².

Phishing

En cuanto a los **fraudes y estafas en línea**, en Argentina, la mayoría de ellos se produjeron 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”. Se trata de un fraude de ingeniería social aplicado para “pescar” datos personales de una víctima. Es utilizado como una técnica para cometer el robo de identidad, el fraude más común de Internet, entendido como la obtención no autorizada de datos personales para realizar luego una suplantación o usurpación de identidad en un hecho ilícito posterior.

La ingeniería social en informática hace alusión al proceso por el que se intenta obtener información de un usuario mediante métodos y herramientas no técnicas, como por ejemplo, el proceso comunicacional. Es utilizada por los “*phishers*” para ganarse la confianza de una

¹ Organization for Economic Co-operation and Development, “Fraud definition”. En <https://stats.oecd.org/glossary/detail.asp?ID=4781#:~:text=OECD%20Statistics,severest%20form%20of%20an%20irregularity>. [consultado 23-06-2017]

² United States Department of Justice: ¿What is Internet Fraud?. En www.justice.gov [consultado 10-12-2007]

persona y así obtener los datos de ella, generalmente, para la comisión de una estafa posterior.

En los casos de phishing, el estafador se puede hacer pasar por un empleado de una institución bancaria, un organismo público, una tarjeta de crédito o una ONG, entre otras organizaciones, y envía mensajes fraudulentos a través de mails, mensajes de texto –SMS–, redes sociales, WhastApp, chats y/ o en grupos de discusión o foros de sitios web, entre otros.

Habitualmente, los motivos son un supuesto problema de seguridad, la actualización de datos, aprovechamiento de una oferta o promoción, la caducidad de un servicio o producto o la urgencia por una necesidad de la potencial víctima para obtener datos como nombre y apellido, DNI, número de tarjeta de crédito, credenciales de acceso a servicios y aplicaciones (nombre de usuario y contraseña) o número de cuenta bancaria, entre otros.

Antes de la pandemia, el fraude más común en Argentina era el *phishing bancario*. Si bien sigue existiendo, “los ganchos” o motivaciones que tratan de explotar los phishers se ampliaron y diversificaron. En el mismo, la víctima recibe un correo electrónico, supuestamente, de una institución bancaria que le solicita -por ser cliente- que valide su usuario y contraseña de acceso a *homebanking*.

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. El “*phisher*” intentará utilizar esos datos para hacer transferencias bancarias a una cuenta determinada.



The image shows a screenshot of a phishing login form. At the top, there is a red rectangular area. Below it, the form is titled "Identificación de usuarios". The instructions say "Introduzca sus datos de identificación." The form contains several input fields: "Número de DNI/NIE", "Fecha de nacimiento", "Datos de la tarjeta" (with a sub-field "Número tarjeta"), "CVV", "PIN de cajero", and "FIRMA". Below the fields, there is a link that says "Acceder con DNI electrónico". At the bottom, there is a small text block containing HTML code:

Introduzca primero el DNI electrónico en el lector:
<p>Acceder con:</p> <div class="dni">Acceder con DNI electrónico<p id="di lector"></div>

Durante la pandemia, las solicitudes fraudulentas comenzaron a ser dirigidas, personalizadas. Esta modalidad se denomina “spearphishing” y, para cometerla, 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.

También se han ampliado las modalidades de phishing hacia otro tipo de estafas que van más allá de las bancarias y utilizan “ganchos” vinculados a temas del momento y a problemáticas de actualidad. Los mismos tratan de explotar diferentes motivaciones en las potenciales víctimas, tales como la curiosidad, la ambición, el temor, la necesidad, y la solidaridad, entre otros.

Perfiles falsos de bancos en redes sociales

A partir del Aislamiento Social Preventivo y Obligatorio (ASPO), decretado por el Gobierno nacional durante marzo de 2020³, se ha notado un incremento de modalidades fraudulentas a través de cuentas falsas de bancos creadas por los phishers en redes sociales.

Ellos aprovecharon para atacar el aumento de vías de contacto web establecidas por las instituciones bancarias a partir del trabajo remoto de muchos de sus clientes y el aforo temporal en la atención personalizada de las sucursales.

En este sentido, cuentas no certificadas en Instagram -y en menor medida de Facebook- simulaban ser las oficiales del banco. A diferencia del phishing tradicional, en el que se envían comunicaciones “al voleo”, comenzaron a seguir esas cuentas o las agregaron como parte de sus contactos, clientes reales de la institución bancaria suplantada. Tal situación le permite al atacante hacer más selectivo el fraude en cuanto al universo de potenciales víctimas.

³ A partir del 19 de marzo de 2020 el gobierno de la República Argentina decretó el Aislamiento Social Preventivo y Obligatorio en todo el territorio nacional como medida de salud ante la pandemia del COVID-19.

Una vez que los clientes estaban dentro de la red social, el estafador elegía una víctima y le enviaba un mensaje directo con la misma lógica del phishing tradicional.



Fraude de servicio o aplicación informática “vulnerada”

Algunos fraudes estuvieron acompañados con técnicas de comisión similares a modalidades delictivas propias del mundo físico. En algunos de ellos, se utilizó el modus operandi parecido al de los “secuestros virtuales”. Estos se producen mediante una vía de contacto telefónico, por parte de un supuesto secuestrador que elige a una víctima y la priva de su libertad. Luego, durante la noche, llama a un familiar y le dice que la liberará tras el pago de un rescate. Generalmente, acuerdan la operación en un lugar cercano al domicilio de la persona secuestrada.

En Internet, un fraude de este tipo sucede -por ejemplo- cuando la víctima recibe un mensaje de WhatsApp en horas de la madrugada, por parte de un supuesto empleado que trabaja en una empresa que le provee servicios a ella. En la comunicación, le informa que en la cuenta de ella existen intentos de acceso ilegítimo por parte de un tercero o que la misma fue vulnerada (hackeada).

Y para que la pueda recuperar, le dice que debe validar los datos. En ese momento, para ser más convincente, el estafador le envía una imagen con datos precisos de ella, como por ejemplo, su foto o el número de pasaporte. El objetivo de esta estafa es extraer datos de una persona para suplantar su identidad y cometer un posterior hecho ilícito.

En el ejemplo que se ilustra a continuación, el contacto por escrito estuvo acompañado con videollamadas producidas dentro de la aplicación y con comunicaciones telefónicas hechas a su línea móvil.



Fraude de turno de vacunación

Durante el aislamiento preventivo, se produjeron diversos fraudes de robo de identidad basados en la sustracción de cuentas de usuario para diversos fines, principalmente, económicos.

Las técnicas utilizadas por los *phishers* estaban basadas en la obtención de datos de autenticación brindados por algunas empresas proveedoras de Internet. El factor de doble autenticación de usuario o autenticación multifactor es una medida de seguridad que poseen algunos servicios y aplicaciones. Funciona mediante la solicitud de un dato anexo que se utiliza para intentar acreditar la identidad de un titular o de un legítimo usuario.

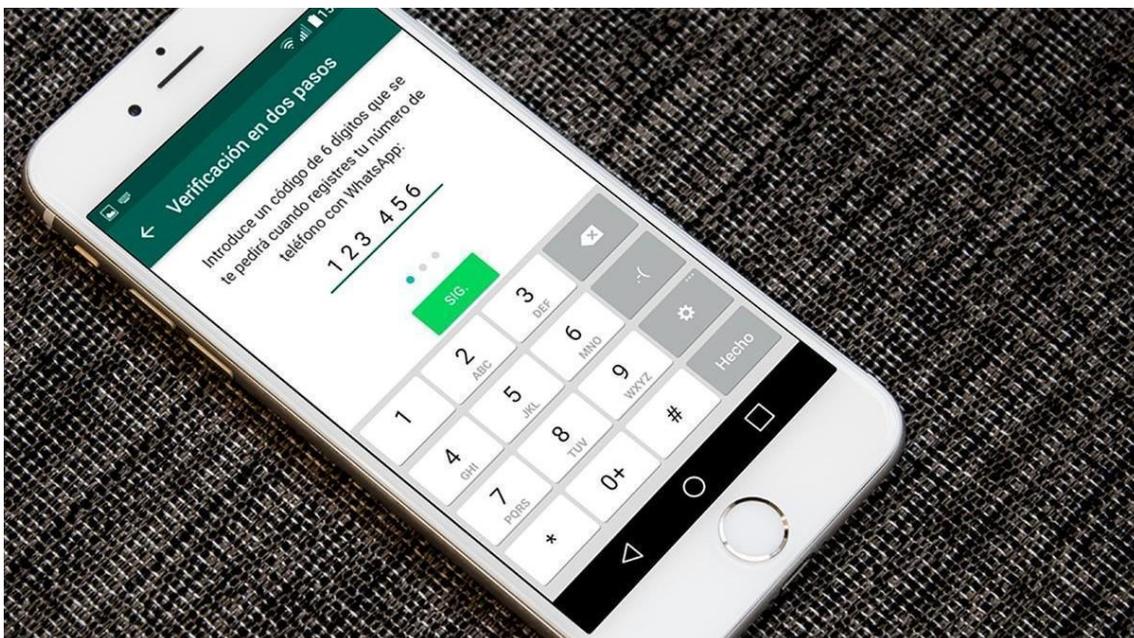
WhatsApp cuando un usuario intenta instalar el servicio de mensajería en un dispositivo nuevo o no habitual, envía mediante un mensaje de texto -SMS- un código numérico de seis dígitos. Lo manda al número de teléfono que dejó registrado el titular de esa cuenta -que se pretende abrir en el nuevo dispositivo- para verificar que efectivamente es él quien está iniciando la sesión desde otro aparato.

A partir de ese dato, se produjo en la pandemia el “fraude de turno de asignación de vacunación”. Para esta modalidad, el *phisher* contaba con el número de celular, el documento, el nombre y el apellido de la potencial víctima. Luego establecía una comunicación fraudulenta por WhatsApp haciéndose pasar por un organismo de Salud determinado, que le informaba la fecha, hora y lugar donde debía asistir para la aplicación de la dosis de la vacuna contra el COVID-19.

El fraude consistía en que la víctima debía confirmar el supuesto turno mediante el envío del código numérico de seis dígitos, que le había llegado a su casilla de mensajes de texto del móvil.

Una vez que lo enviaba, el estafador lo utilizaba para iniciar una sesión de Whatsapp en otro dispositivo, es decir, que utilizaba los datos de la víctima y el doble factor de autenticación para hacerse pasar por ella en un celular que él tenía en su poder.

Una vez apoderado de la cuenta, la estafa posterior consistía en enviar mensajes a los contactos de la víctima solicitándoles dinero por un problema personal⁴.



⁴ “Tenés turno para la segunda dosis contra el Covid: alertan sobre estafas por Whatsapp”. -Clarín edición online- 13/07/2021 [consultado 22-07-21]

Fraude de DEBIN

Otra estafa relacionada con fondos bancarios es el “Fraude de Débito Inmediato (DEBIN)”. Este débito automático es un sistema de pago electrónico autorizado por el Banco Central de la República Argentina en 2017. La operación se realiza cuando un vendedor de un producto o servicio o una persona física, en acuerdo con otra, envía una solicitud de débito automático de fondos de una cuenta bancaria a su titular. Con el objetivo de agilizar el intercambio de activos financieros, los sistemas de *homebanking* cuentan con esta modalidad en el país.

Durante la pandemia, circularon engaños mediante el uso de esta transacción bancaria. La modalidad se realizaba cuando los estafadores enviaban a la víctima mensajes fraudulentos solicitando autorizar una transferencia de fondos en calidad de pago. Y cuando el titular de la cuenta hacía la autorización -desconociendo esta modalidad-, lo que realmente estaba haciendo era dar el visto bueno a la sustracción de dinero de su cuenta bancaria. Antes de llegar a esa instancia, el estafador le había solicitado mediante un engaño el número de cuenta, el alias o el CBU.



Estafas piramidales o de esquema Ponzi

La estafa piramidal o de esquema Ponzi lleva esa denominación por el italiano Carlo Ponzi, quien la ideó en 1919. El engaño comienza con la oferta realizada por una supuesta persona física o jurídica que ofrece altas rentabilidades por ingresar dinero a un esquema piramidal de inversión. El mismo busca atraer plata prometiendo ganancias basadas en intereses elevados a medida que ingresan más “inversionistas” a la pirámide, motivando a cada participante a captar gente para que también aporte fondos.

Y en un momento determinado, la cadena se corta, los fundadores se quedan con la mayor parte de los ingresos, y los últimos en llegar nunca recuperan lo invertido.

Ya desde antes de la pandemia se vieron estafas así bajo nombres como la “*Flor de la Abundancia*”, “*Mandala de la Prosperidad*”, “*Telar de los Sueños*”, “*Ruedas de amistad*” entre otros, que prometen ingresos rápidos y elevados a cambio de un aporte inicial.

Muchos de ellas buscan captar mujeres con mensajes feministas, basados en un discurso que genera una mística de empoderamiento apoyados en testimonios de violencia doméstica e intercambio de mantras.

La “*Flor de la abundancia*”, por ejemplo, es una estafa que se compone de 15 “pétalos” y un “centro”, que representan 15 personas en total divididas en cuatro niveles.

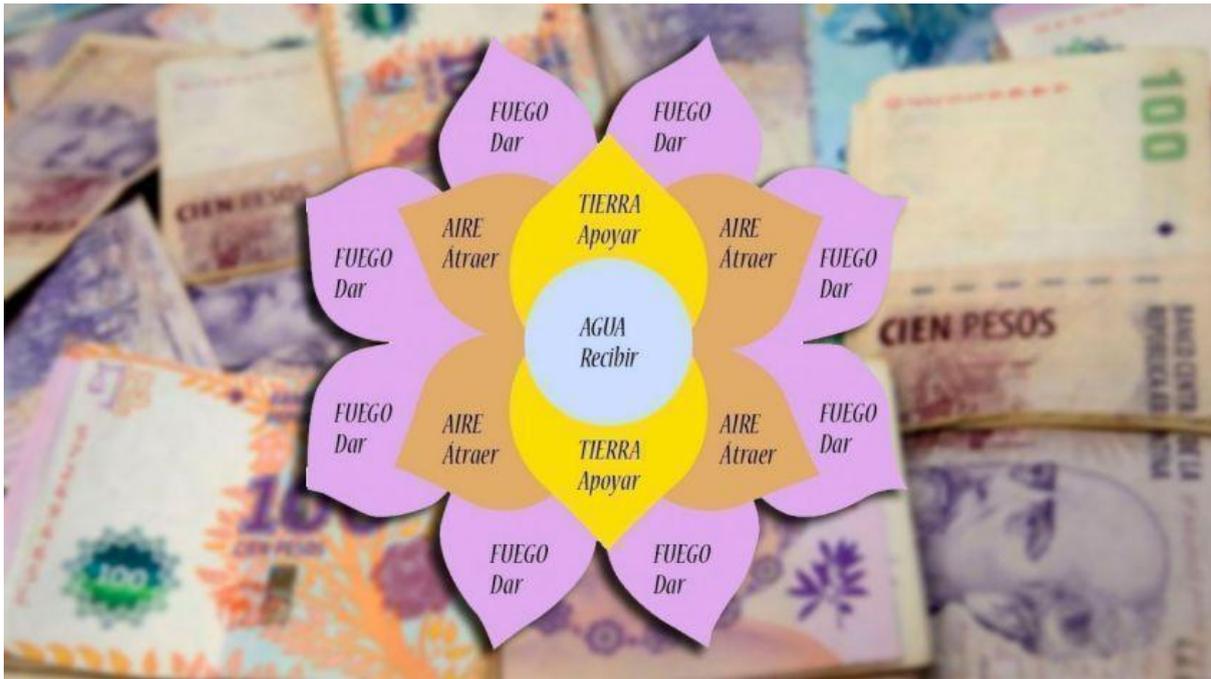
En el nivel 4, que lleva el nombre del elemento del *Fuego*, se ubican ocho personas que pretenden ingresar en la flor. Para hacerlo, deben depositar en la cuenta de alguien -conocido o no- una determinada cantidad de dinero.

En el tercer nivel, llamado *Aire*, hay cuatro personas que ya depositaron la suma inicial y ahora deben traer dos nuevos interesados para escalar al siguiente nivel.

En el nivel 2, denominado *Tierra*, se sitúan dos personas que están a la espera de que el individuo del escalafón superior cobre para ocupar su lugar.

Por último, en el nivel Agua, se centra la persona que recibe el dinero de los primeros ocho interesados. De este modo, cobra el 800% de su inversión inicial, es decir, que si su depósito fue de \$2000 se llevará \$16000.

La estafa consiste en que se promete ganancias en base a un capital invertido, pero éstas se obtienen por la plata que otras personas invirtieron. Así se genera una estructura que se agranda de manera cuadrática hasta el punto que colapsa y deja a varios inversores con pérdidas totales. En definitiva, una persona debe convertirse en estafadora para no perder dinero.



Fraude de donaciones por el COVID-19

En cuanto al fraude de donaciones por el COVID-19, la Organización Mundial de la Salud advirtió sobre una serie de mails engañosos referidos a supuestas donaciones en nombre del organismo, surgidos a partir de los efectos económicos generados por el Coronavirus. Los mismos no solo tienen como finalidad robar dinero a las víctimas sino también datos personales de los estafados.



REQUEST FOR DONATION TION TO HELP COMBAT THE DEADLY COVID-19 VIRUS

ie Covid-19 Solidarity Response Fund is a secure way for individuals, philanthropies and businesses to contribute to the WHO-led effort to respond to the pandemic.

ie United Nations Foundation and the Swiss Philanthropy Foundation have created the solidarity fund to support WHO and partners in a massive effort to help countries prevent, detect, and manage the novel coronavirus – particularly those where the needs are the greatest.

ie fund will enable us to:

Send essential supplies such as personal protective equipment to frontline health workers
 Enable all countries to track and detect the disease by boosting laboratory capacity through training and equipment.
 Ensure health workers and communities everywhere have access to the latest science-based information to protect themselves, prevent infection and care for those in need.
 Accelerate efforts to fast-track the discovery and development of lifesaving vaccines, diagnostics and treatments

The Strategic Preparedness and Response Plan outlines a funding need of at least US\$675 million for critical response efforts in countries most in need of help through April 2020. As this outbreak evolves, funding needs are likely to increase.

Donations can be made through the below bitcoin wallet address : 36gFxmLf9dxu1SxD8qEYW1Eem6CrGrAv

Fraudes de inmunización del Coronavirus

En diferentes sitios web, empezó a circular la venta de productos que ofrecen remedios o curas falsas contra el coronavirus. Algunos de los supuestos tratamientos antivirales que se venden por la red son tés, aceites esenciales y terapias intravenosas con vitamina C.

También ha habido venta online de supuestos remanentes de vacunas como Sputnik V y Oxford/AstraZeneca, entre otras.

Y en Argentina, se ofrecieron productos como suero equino, para aliviar la enfermedad de aquellos que se contagiaron el virus, sin autorización de las autoridades sanitarias.

Fraudes relacionados con programas o beneficios gubernamentales.

A través de anuncios en sitios web, mensajes de texto móviles (SMS) o por WhatsApp, se informa a la víctima sobre un bono o beneficio excepcional, como por ejemplo, el Ingreso Familiar de Emergencia (IFE), lanzado por el Gobierno nacional para asistencia familiar.

Los estafadores crean sitios web o perfiles de redes sociales falsos simulando ser la autoridad gubernamental competente. En algunas oportunidades, falsos gestores de la Administración Nacional de la Seguridad Social (ANSES) contactaron por teléfono a los supuestos beneficiarios pidiéndoles sus nombres, fechas de nacimiento y otras informaciones para otorgarles el subsidio. Hubo casos en los que hicieron además ir a las víctimas hasta un cajero para que tramitaran una clave de seguridad, con la que luego podían acceder a las cuentas de ellas.



Fraudes de compraventa en redes sociales

Durante la pandemia, se incrementó mucho la venta online de productos por redes sociales. La empresa Facebook, por ejemplo, creó *Facebook Marketplace*, un sitio dentro de la red social para que los usuarios puedan comprar y vender productos y servicios. En este caso, la empresa solo brinda el lugar para realizar la actividad, no cobra comisiones ni brinda seguros ni sistemas de pago, como posee la mayoría de las tiendas en línea.

En estos casos, las transacciones las realizan los propios usuarios usando el servicio de mensajería directa que está dentro de estos entornos digitales, para comunicarse entre sí o por otra vía alternativa fuera de la red social.

Y al ver el crecimiento de estas operaciones comerciales, los estafadores no perdieron la oportunidad y se instalaron también en estos entornos digitales, como Instagram, donde sucedieron muchas estafas.

Para atraer a las víctimas, los estafadores venden productos a bajo precio del promedio de mercado y libres de impuestos en aquellos importados, por tratarse de “zona franca” de compraventa. Asimismo, ofrecen garantías y muestran imágenes ficticias de clientes satisfechos, que están acompañados de comentarios positivos por las transacciones realizadas, todas tomadas de forma pública de la web. Los pagos deben ser siempre en efectivo o con depósito bancario. La estafa consiste en comprar un producto, realizar el pago para después no recibirlo.



Ataques de *ransomware* a organizaciones

El *ransomware* (conjunción de “ransom” -rescate- y software) es un programa malicioso, un malware que encripta determinados archivos de un dispositivo o sistema o el acceso a los mismos. El “secuestrador” de los datos solicita un “rescate”, un pago de criptomonedas, generalmente, para liberar la información.

Los primeros tipos de *ransomware* bloqueaban el acceso al equipo de un usuario haciéndoles llegar un supuesto mensaje de agencias de seguridad que los acusaba de infringir la ley. Los argumentos eran el de visitar sitios webs de pornografía y por descarga de archivos protegidos por los derechos de autor (música, películas, etc.).

En este caso las bases de datos almacenadas en los dispositivos no se cifraban mediante técnicas criptográficas, sino que se alteraban los archivos de inicio de una computadora para impedir su acceso a los mismos.



Al igual que el *phishing*, en un principio, las víctimas eran generales y se utilizaban direcciones web que aparecían públicamente en sitios de Internet y se enviaban como SPAM (correo no deseado). En los últimos años, se ha segmentado el público y se han ampliado los objetivos de usuarios particulares a empresas y organismos gubernamentales con ataques dirigidos, mediante la explotación de vulnerabilidades de los sistemas, campañas de *phishing* y/o cifrando los archivos.

El caso más conocido sobre este tipo de *malware* es el del emblemático *ransomware* Wannacry de 2017 por afectar a más de 150 países en todo el mundo. Dicho código malicioso no fue justamente noticia por la filtración de datos privados de las organizaciones afectadas, sino por la sensibilidad que generó en un comienzo al afectar la información de un hospital de Gran Bretaña, una semana después del ataque al puente de Westminster, a metros del Parlamento Británico.



Meses antes de que la Organización Mundial de la Salud decretara la pandemia del COVID-19, los atacantes comenzaron a realizar copias de información en forma remota antes de encriptarla para luego amenazar a la organización víctima con hacerla pública en Internet en caso de no pagar el rescate, lo que constituye una doble extorsión.

Asimismo, aumentaron los ataques mediante la explotación de vulnerabilidades de los sistemas, y comenzaron los de “fuerza bruta” contra los empleados de las organizaciones, que se conectaban a las redes corporativas a partir de la expansión del trabajo remoto o teletrabajo. Un ataque de fuerza bruta sucede cuando un atacante intenta ingresar a un sistema informático probando diferentes combinaciones de caracteres hasta que logra descubrir la contraseña buscada. De esa forma obtiene las credenciales de acceso para ingresar a la cuenta de un legítimo usuario.

Por otro lado, se incrementó notablemente en la Internet profunda o Deep Web la cantidad de sitios donde se ofrece el ransomware como servicio por parte de hackers maliciosos. La misma consta de una serie de sitios webs no públicos -no localizados por los motores de búsqueda-, que son inaccesibles para mantener la privacidad de las comunicaciones y el anonimato de sus usuarios.

Y para su uso se requiere de un navegador específico (Navegador TOR, The Onion Router) y redes distribuidas descentralizadas (Cadena de Bloques o Blockchain).

El modelo de negocios de *ransomware* como servicio (RaaS, por sus siglas en inglés) incluye la descarga del software malicioso, el soporte, la venta de vulnerabilidades *Zero Day* y la de credenciales robadas, adquiridas en mercados negros que funcionan en línea.

Y es así como, durante el transcurso de la pandemia, se produjo un notable incremento de estos ataques, que tuvieron como objetivo fundamental al sector privado, donde los blancos principales fueron grandes empresas, debido a la capacidad adquisitiva de las mismas para pagar las millonarias sumas demandadas.

Otra característica que se observó durante este período, a nivel global, fue el incremento de ataques de *ransomware* contra las Infraestructuras Críticas de Información (ICI). Estas Infraestructuras son sistemas y redes informáticas que hacen a la operatividad y suministro de servicios esenciales para las personas. Algunas de ellas pueden ser las pertenecientes al sector bancario, al energético, a la provisión de combustible, a los medios de transporte, al gas, etc.

Un ejemplo de estos ataques ocurrió en la empresa de transporte de petróleo y gas de los Estados Unidos “Colonial Pipeline”, produciendo demoras en los servicios a toda la Costa Este del país durante casi una semana. De manera preventiva, la firma decidió suspender la provisión de ambos insumos desde la ciudad de Houston hasta New York ante la posibilidad de que los ciberdelincuentes dañaran físicamente el oleoducto.



Si bien el ataque solo comprometió información corporativa sensible, la empresa pagó 5 millones de dólares para la liberación (o no publicación) de la información cifrada.

Para la Agencia Federal de Investigación de los Estados Unidos (FBI por sus siglas en inglés), se trató de un grupo organizado que produjo el ataque a partir de una vulnerabilidad del sistema de energía.

La empresa reconoció haber pagado el rescate de los archivos por motivos que aún no fueron esclarecidos, pese a las recomendaciones habituales de los especialistas de no efectivizar el pago.

Blanqueo ilícito de capitales

El blanqueo ilícito de capitales consiste en legitimar fondos provenientes de actividades ilegales. También es comúnmente conocido como “lavado de dinero”. Es un delito difícil de descubrir por el uso de testaferros o “prestanombres” que hacen los delincuentes, para la realización de operaciones ejecutadas por debajo del umbral permitido por las autoridades de control financiero, establecidas por el Grupo de Acción Financiera Internacional (GAFI). Esta última es una modalidad conocida como “técnica de *smurfing*”.

A partir del surgimiento de la Internet comercial a mediados de la década de 1990, *la nueva economía digital* ofrece una serie de servicios económico-financieros mediados por tecnologías de la información y la comunicación en Internet, tales como la compraventa de bienes y servicios, el desarrollo de pagos electrónico, las transferencias de fondos en línea y el uso de prestaciones bancarias en forma electrónica, entre otros.

En los últimos años, en Argentina, se produjo el surgimiento de bancos digitales, que tienen existencia únicamente en el ciberespacio, es decir, sin sedes físicas. A diferencia de los bancos tradicionales, donde la apertura de una cuenta bancaria es de forma personalizada mediante acreditación de identidad, en la versión en línea se permite comenzar a operar mediante métodos digitales de identificación que están en la web.

Durante la pandemia, se han incrementado los casos de **intento de apertura de cuentas bancarias en esos bancos digitales mediante la sustitución de identidad**, tanto así como la apertura de varias cuentas hechas por clientes para legitimar fondos ilícitos provenientes de fraudes y estafas en línea.

Para los casos de *ransomware*, los atacantes utilizaron como método de pago de rescate las criptomonedas, que operan por fuera del sistema bancario tradicional, pero para los casos de transferencia de fondos de un sistema de *homebanking* -por parte de un *phishers*- se necesitan cuentas bancarias convencionales.

Una de las formas de obtener estas cuentas es mediante **fraudes de empleo por Internet**. En este caso, tras el ofrecimiento formal de ser parte de una empresa, se solicita a la víctima

autorización para ingresar fondos a su cuenta bancaria como parte de los movimientos financieros de la firma.

Una vez realizado el depósito, se le solicita al “empleado” entregarla a un “corresponsal” de la empresa. Así, en la operatoria ilícita, el único registro final electrónico es la cuenta bancaria de la víctima, quien en este caso está actuando de “mula”, como se conoce en la jerga.

Oferta del trabajo

¡Un trabajo bien retribuido!

Te ofrecemos una posibilidad de ganar dinero fácilmente. Puedes simultanear este trabajo con el que tienes ya. Solo hay que encontrar 2-3 horas libres al día 1 - 2 veces a la semana.

Te explicamos como funciona:

1. Realizamos el ingreso de 3000 EUR en tu cuenta.
2. Una vez llegado retiras el dinero.
3. **Ya has ganado 20 % del ingreso - te queda 600 EUR!**
4. Luego nos entregas el resto 2400 EUR.

Los montos transferidos y su frecuencia pueden ser diferentes, todo depende únicamente de tus preferencias y posibilidades! La actividad está absolutamente legal y no viola ninguna ley de UE o de España.

Si te interesa la propuesta y quieres probar, mándanos un mail a la dirección: es@nix-finance.com. Te contactaremos lo más pronto posible para contestar tus preguntas.

¡Ten prisa! La cantidad de vacancias está limitada!

Le pedimos perdón si este mensaje le ha molestado. En caso que este e-mail le ha llegado por error y si desea dar de baja su dirección electrónica de nuestra base de datos - nueva enviar un mensale sin texto a la dirección siguiente: del@nix-finance.com Muchas gracias.



Recomendaciones para evitar fraudes y estafas

Recomendación general

Nunca una organización, 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.

Recomendaciones particulares

Para no caer en un engaño de *phishing*, nunca abras correos electrónicos o ingreses a enlaces que te resulten sospechoso o que no esperabas recibir. En el caso de los correos, revisá detalladamente la dirección del mail y chequeá cada letra para ver si es la original que ya conoces, es decir, la que figura en la página oficial de tu banco u organización conocida. Los cibercriminales suelen cambiar a la dirección una letra, número o símbolo para engañarte, de la misma forma que lo hacen con el enlace de los sitios web, es decir, con la dirección de la ubicación de las páginas.

Podés chequear la dirección de correo o el enlace colocando el puntero del mouse sobre el enlace recibido y, de esa forma, verás en la parte inferior izquierda del navegador el enlace o la cuenta de mail verdadera. Si esa opción no resulta efectiva, la mejor práctica es escribir en tu navegador la dirección que ya conoces, es decir, la que usaste anteriormente.

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. Por eso, no accedas a los enlaces de un mensaje así, ni descargues archivos adjuntos porque podrían contener un programa malicioso.

Tampoco realices ninguna acción si recibís un correo que te indica actuar de forma inmediata, con límite de tiempo o te cause miedo. Lo primero que debés hacer es comunicarte por teléfono o personalmente con esa organización que supuestamente te ha enviado el mensaje para corroborar la veracidad del contenido.

La revelación de tus claves personales o bancarias son un tesoro muy preciado que los ciberdelincuentes buscarán también obtener mediante la técnica de phishing. Por eso, nunca debes revelarlas, ya que ninguna institución financiera ni de otra naturaleza, que se precia de ser seria, te las pedirá por teléfono o por mail, ni a través de empleados que vayan a tu casa o trabajo.

Si recibís un mail desde una casilla general (como Gmail, Outlook o Yahoo) en el que dicen ser una empresa determinada, desconfía al instante. Por lo general, las empresas o instituciones prestigiosas suelen tener sus propios dominios para las direcciones de correo electrónico, salvo algunos comercios pequeños. Por lo tanto, antes de responder o realizar alguna acción solicitada, verifica todo y así evitarás caer en los fraudes. Lo mejor es mantener una actitud de desconfianza y cuidado.

Presta atención a los encabezados genéricos de los correos, como aquellos que dicen: "Estimado, cliente"; "Hola"; "Buenas tardes, amigo o amiga", etc.", porque de esa forma se suelen expresar los estafadores que envían de forma simultánea el mismo mail a un número importante de personas. Cuando una organización quiere dirigirse a un cliente o usuario, lo hace escribiendo el nombre del destinatario en el texto y no de forma general.

Si el sistema no te exige claves con ciertos requisitos de seguridad, generará una de más de ocho caracteres utilizando mayúsculas, números y algún carácter especial. No utilices fechas específicas como día, mes y año de nacimiento, número de dirección postal ni nada que te identifique o puedan asociar con vos. Tampoco repitas letras en secuencia.

Si el sistema de homebanking desde donde accedes a tu cuenta bancaria permite una contraseña sencilla, comunicate con el banco para solicitar que no permita esa opción y que configure sus sistemas con credenciales de acceso que contengan un cierto nivel de seguridad, tal como lo exige la normativa del Banco Central de la República Argentina

Si caíste en un fraude online, lo primero que debes hacer es la denuncia en la comisaría de tu barrio o fiscalía más cercana. Asimismo debes avisar en la entidad bancaria que usaron para engañarte o en la organización en cuestión. Por ese motivo, no debes eliminar el correo recibido ni los enviados, ni los diálogos que hayas tenido con alguna persona que se hizo pasar por un empleado bancario, por ejemplo. No borres nada porque todo podrá ser usado como prueba para intentar descubrir a los ciberdelincuentes.

Luego debes cambiar de inmediato la contraseña que te solicitaron para cometer el fraude, en todos los sitios y redes sociales en los que la estés utilizando, para evitar que los cibercriminales ingresen, ya que es probable que intenten hacerlo para obtener la mayor cantidad de datos posibles.

Para identificar **perfiles falsos**, verificar siempre que junto al nombre de la cuenta esté el ícono azul, que sirve para confirmar si la misma es auténtica.

También podés leer la cantidad de seguidores que tiene la cuenta, los posts realizados y la fecha de creación para saber qué antigüedad tiene. Si es reciente, debes elevar aún más el nivel de sospecha y ser sumamente cuidadoso para avanzar.

También observa si figura la página web de la sucursal que dice ser y si tiene un teléfono y un domicilio para que puedas comprobar la veracidad de su existencia.

Siempre evita comunicarte con cualquier organización o entidad que te escriba desde un perfil personal, ya que puede ser falso y utilizado para robarte los datos personales o bancarios.

Tené presente que las empresas serias no te pedirán por redes sociales tus datos personales ni los bancarios, como claves de acceso o números de tarjeta de créditos.

Si llegás a comprobar o detectar algún perfil falso, podés reportar la cuenta como spam directamente desde la aplicación para alertar sobre posibles estafas.

Para evitar el **robo de cuentas por suplantación de identidad**, no compartas ningún código o archivo recibido en dispositivos informáticos, y ten presente que ninguna empresa te pedirá datos personales por mensajes o llamadas telefónicas.

Recuerda que configurar bien las opciones de seguridad, te brindará mayores niveles de protección. Para ello, y desde “Ajustes” o “Configuración” de Whatsapp, activá el doble factor de autenticación que te aportará una mayor seguridad.

Esta práctica debes llevarla a cabo en todos los servicios que lo permitan, como por ejemplo, en portales de compra, pago de servicios, etc. Y nunca compartas tu código de verificación en dos pasos con otras personas.

Si recibiste un correo electrónico para restablecer el PIN de la verificación en dos pasos de Whatsapp y no hiciste esa solicitud, no hagas clic en el enlace recibido, ya que es posible que alguien esté intentando acceder a tu cuenta.

Para elegir quién puede ver tus fotos, perfil, datos y estados, configurá la privacidad de las aplicaciones.

Si una persona desconocida te envía un mensaje a través de Whatsapp, se aconseja ignorarlo y, si es necesario, bloquearla y reportarla.

Si llegás a ser víctima de alguna estafa, además de hacer la denuncia, avisales rápido a tus contactos para que estén atentos en caso de que reciban algún pedido en tu nombre.

Protegé tu teléfono de la mano de cualquier extraño. Pensá que si alguien accede físicamente a tu celular, puede usar tus perfiles abiertos y robar tus datos. Se recomienda siempre bloquearlo con una contraseña, un patrón o la huella dactilar.

Si no querés caer en estafas de vacunación o de cualquier otro tema que a vos te interese, es importante que siempre te informes antes de hacer cualquier acción que se te solicita realizar sin que lo hayas requerido.

Para no caer en una estafa de **DEBIN**, tener presente que el mismo será enviado por la persona que necesite cobrar, o sea, un comerciante con el que realizamos alguna operación de compra. Si no fuera el caso, desestimá el pedido de modo de no autorizar ningún débito.

También debes evitar ingresar en un enlace contenido en un mensaje llegado por mail o SMS solicitándonos autorización para realizar el pago a un vendedor desde nuestra cuenta bancaria. Siempre debemos chequear la procedencia de ese emisor y corroborar que hayamos hecho la compra indicada.

Si tenés alguna duda o estás ante una situación sospechosa, comunicate urgente con tu banco antes de concretar cualquier transferencia. Tené en cuenta que el DEBIN lo autoriza la persona que actúa como compradora y pagadora.

Además, infórmate siempre -y en forma previa- sobre cómo funcionan las herramientas bancarias, ya que de esa forma disminuirán las posibilidades de ser engañado.

Nunca facilites información confidencial como nombres de usuarios, claves, números de tarjeta por teléfono, correo o SMS. Recordar siempre que son personales e intransferibles.

Para evitar las **estafas piramidales o de esquema Ponzi**, tené presente que en Argentina toda captación de dinero con fines de inversión está regulada por organismos públicos como el Banco Central o la Comisión Nacional de Valores. En la web de cada organismo, se pueden buscar las empresas que están reguladas para operar.

Y en este tipo de conducta, cuando te llegue la invitación por un medio electrónico, tené en cuenta las mismas precauciones que tendrías en el mundo físico. Entre estas recomendaciones se encuentran las siguientes.

No olvides que las compañías administradoras de inversiones de mercado no pueden asegurar un rendimiento determinado a futuro debido a que los instrumentos del mercado cotizan libremente y se mueven por una variedad de factores que pueden ser locales, internacionales y/o de resultados. Por tal motivo, hay que sospechar de cualquier “tasa segura”.

Si se presenta una oportunidad que ofrece grandes ganancias, investiga bien cómo funciona el negocio y compara los retornos ofrecidos con los de otros instrumentos de inversión. Desconfía de inmediato si la diferencia entre ambas es muy amplia.

No confíes en un sistema de inversión o de venta que te exija permanentemente atraer a más personas para ser integrante del mismo.

Antes de realizar cualquier tipo de negocio, debemos hacer todas las preguntas necesarias. Los y las estafadoras especulan con que no se investigue antes de invertir y presionan para que la inversión se realice rápidamente. Por ese motivo, es fundamental investigar a quién le entregamos nuestro dinero.

Nunca utilices los correos electrónicos no solicitados, los anuncios y los comunicados de prensa de las empresas como única base para tomar decisiones de inversión. Siempre debemos ampliar y chequear la información recibida.

Averigua siempre si los asesores de valores que nos están contactando para realizar alguna operación financiera, son empleados reales que están autorizados a negociar en el país. También busca información sobre si ellos o sus empresas tuvieron problemas con otros inversores.

Desconfiá siempre y toma medidas de prevención si alguien recomienda hacer inversiones en el extranjero u off-shore. No olvides que si algo sale mal, será más difícil averiguar lo sucedido y localizar el dinero enviado al exterior.

Recomendaciones para evitar el *ransomware*

Para evitar el código malicioso, instala un sistema operativo original para que pueda ser actualizado permanentemente. Las compañías proveedoras sacan actualizaciones para corregir problemas que puedan ser aprovechados por los atacantes si no se toman precauciones.

Tené siempre instalado un antivirus en los dispositivos, y descargalo siempre de una tienda y/o sitio web oficial que te lo permita hacer.

También es importante que mantengas el antivirus actualizado, ya que todos los días salen nuevos códigos maliciosos y variantes de los ya existentes. Por tal motivo, no dejes de realizar periódicamente un análisis de control en todos los dispositivos que utilizas, al igual que en los correos electrónicos y sus archivos adjuntos.

No abras archivos adjuntos o mensajes de mail si no conocés su procedencia o si aún conociéndola, el mensaje te llega de un modo inesperado. Se recomienda ser desconfiado, verificar si es un correo confiable y si proviene de un emisor conocido o confiable.

Evita hacer click en fotos que aparezcan mensajes de emails, aún cuando prometan la última noticia de actualidad o algo que despierte mucho interés. Los atacantes utilizan temas candentes para atraer la atención de sus víctimas y bajar el umbral de peligro o la sensación de riesgo, así como también para distraer tu atención. Algunos de estos ataques pueden ser dirigidos a una persona específica a sabiendas de sus intereses.

No accedas a sitios desconocidos ni hagas clic en enlaces dudosos y si detectas algún código malicioso, debes eliminarlo enseguida.

Es muy importante también hacer copias periódicas de los datos, archivos y programas, incluyendo las fotos que guardes en tu computadora o en tu celular, para proteger y tener siempre la información disponible en caso de sufrir algún ataque informático.

Para mantener una mayor protección, utiliza una red privada virtual o VPN segura, y evitá usar una red Wi-Fi pública, especialmente, para realizar transacciones sensibles, como las bancarias o los trámites que involucren información personal.

No uses nunca memorias USB desconocidas, sobre todo las encontradas en lugares públicos, ya que es posible que los ciberdelincuentes la hayan infectado y dejado allí para incitar a que alguien la use.

Recomendaciones para evitar el blanqueo ilícito de capitales

A la hora de buscar empleo, Internet se ha transformado actualmente en la primera herramienta utilizada para encontrar el puesto buscado. Y si bien es sabido que su uso es muy útil, también, es conocido que los ciberdelincuentes no pierden oportunidad para capturar presas con ofertas falsas de trabajo.

Si estás buscando un puesto, tené presente que las estafas de “mulas de dinero” se disfrazan generalmente como grandes oportunidades laborales. Por ese motivo, sospechá si te prometen una forma rápida y fácil de ganar plata, y averiguá -por todos los medios que puedas- quién es la persona o empresa que ofrece el empleo.

Bajo ningún concepto aceptes dar tus datos personales para un supuesto trabajo que consiste en la apertura de una cuenta a tu nombre para que allí te depositen dinero, que luego deberás sacar por ventanilla o cajero automático, para entregarlo a algún representante de una determinada organización a cambio de una interesante comisión o bien realizar una transferencia de los fondos recibidos a otra cuenta a una cuenta que te provean. Si aceptás, estarás siendo parte de un blanqueo ilegal de capitales y podrías terminar inclusive en la cárcel. También podrías pasar a formar parte de “la lista negra” de las personas que no podrán acceder a tener tarjetas ni cuentas bancarias por antecedentes fraudulentos.

Recordá también que si te piden transferir dinero a tu cuenta bancaria de siempre y que luego lo extraigas o transfieras a cambio de esa comisión interesante, tampoco es un empleo formal, sino que se trata de un trabajo falso, porque solo se pretende reclutar en línea “mulas de dinero”.

Tené presente que esos supuestos empleadores buscan usarte a vos, tus datos y tu cuenta bancaria para no ser rastreados y mover fondos obtenidos ilegalmente a través de distintos tipos de estafas que pueden ser comerciales, de phishing y/o de malware, por nombrar algunos ejemplos. Por ese motivo, desconfiá de aquel o aquella persona que te pida usar tu cuenta bancaria o abrir una nueva a tu nombre sin una clara explicación.

Si caíste en una de esas trampas y luego te diste cuenta del engaño, interrumpí inmediatamente las transferencias recibidas, avisá a tu banco y hacé la denuncia en la policía. Y si el contacto con los estafadores se produjo a través de las redes sociales, informá rápido al proveedor de la plataforma para que intenten localizarlos y les cierren sus perfiles para evitar más víctimas.

A continuación te dejamos recomendaciones generales para la búsqueda de trabajo

Lo primero que debes asegurarte al ver una oferta de empleo es que se ajuste a tu formación y si la empresa que ofrece la vacante es conocida o si existe realmente. Si tiene un sitio web, llámalo por teléfono o envíale un mail a su página oficial y consultá si es real la oferta laboral que recibiste o encontraste. Si después de haberla googleado no aparece en web y tampoco hay referencias o no recibís respuestas creíbles, lo más seguro es que todo sea una mentira, es decir, un fraude.

Lo segundo que debes evaluar es si el salario que pagarán supuestamente es acorde a las tareas a desarrollar. Si no sabés de qué se trata el trabajo, averiguá si es una actividad legítima y dónde se realizará tu labor.

Otro factor a tener en cuenta es si la propuesta te llegó por Internet sin haberte postulado o postulada en ningún sitio. Si eso te sucede, desconfiá de la veracidad del empleo y buscá más información antes de realizar alguna acción.

Si por el contrario, enviaste una solicitud de empleo por mail y recibiste una respuesta en la que te indican que debes abonar dinero por algún motivo en particular, no lo hagas porque las empresas confiables no hacen ese tipo de peticiones.

Otra alerta que debés tener presente es respecto a quien envió el mensaje de correo que utilizaron para hacerte llegar la oferta laboral. Si es de un servicio gratuito podría ser otra mentira, salvo que te hayas anotado en algún comercio o firma que no tenga su propio correo con su nombre, situación que no es una práctica habitual.

Tené también presente que si ves un anuncio con faltas de ortografía o mal redactado, puede que estés ante un posible fraude, ya que -por lo general- las empresas serias suelen ser claras y escribir sin errores porque cuidan su imagen y reputación.

Las ofertas de trabajo en el exterior o desde casa suelen ser muy tentadoras y los ciberdelincuentes lo saben muy bien. Por eso, sospechá de anuncios de ese estilo, que ofrecen salarios muy altos y sin ningún tipo de experiencia previa. Pensá que nadie paga mucho dinero por poco tiempo de trabajo.

Tampoco creas en la propuesta si la empresa te solicita -tras un supuesto proceso de selección- que compres los materiales para el trabajo que vas a realizar desde tu hogar. Con estos tipos de engaños, los delincuentes buscan por lo general obtener información personal o un beneficio económico directo.

El primer objetivo es un recurso muy cotizado por ellos, ya que les significa una primera puerta que se les abre para generar otro tipo de fraude. Además, los datos personales tienen el plus de poder ser vendidos a organizaciones que los pueden usar también para otros hechos delictivos.

La variante económica suele ser el objetivo de la mayoría de las ofertas falsas de empleo, porque planean obtener ingresos directos mediante el envío de dinero efectuado por alguna plataforma que se dedique a eso. Como ya se dijo en este artículo, tratá de estar siempre alerta y sé desconfiado como postura permanente.

Referencias

Diario Clarín, Página 12, La Nación, iProfesional, Perfil.

Informes anuales de incidentes de seguridad informática registrados en el 2020 y 2021 por el CERT.ar de la Dirección Nacional de Ciberseguridad

Incidentes Informáticos: Informe anual de incidentes de seguridad informática registrados en el 2021 por el CERT.ar de la Dirección Nacional de Ciberseguridad

Sain, Gustavo: "NUEVAS MODALIDADES DE DELICTIVAS EN MATERIA DE CIBERCRIMEN DURANTE LA PANDEMIA DEL COVID-19". En Revista *Temas de Derecho Penal y Procesal Penal*. Buenos Aires, ERREIUS, Vol. 12, Diciembre de 2021.