JORNADAS FEDERALES DE CIBERSEGURIDAD

MG. GUSTAVO SAIN

Director Nacional de Ciberseguridad de Jefatura de Gabinete de Ministros de la Nación

"NUEVAS MODALIDADES DE CIBERATAQUES DURANTE LA PANDEMIA DEL COVID-19: LA IMPORTANCIA DE LA PREVENCIÓN EN CIBERSEGURIDAD"

Santa Cruz Gobierno de la Provincia

UTN Facultad Regional Santa Cruz

UNPA UARG

Jefatura de Gabinete de Ministros Argentina

Dirección Nacional de Ciberseguridad

Datastar

NUTANIX

NUEVAS MODALIDADES DE CIBERATAQUES DURANTE LA PANDEMIA DEL COVID-19: LA IMPORTANCIA DE LA PREVENCIÓN EN CIBERSEGURIDAD

Gustavo Sain
Dirección Nacional de Ciberseguridad
26 de Mayo 2022

¿Qué es un ciberdelito o delito informático?

- ✓Conductas antijurídicas, ilícitas, que afectan derechos y libertades de las personas que utilizan un dispositivo informático como ***medio*** para su comisión o como ***fin,*** donde el dispositivo es el blanco del delito.
- ✓No refieren a un tipo de criminalidad específica.
- ✓Adquieren esta definición a partir del **lugar que ocupa la tecnología** mas que a la naturaleza criminal del acto mismo.
- ✓La definición de ciberdelito o delito informático es puramente **intrumental.**

Características de los delitos informáticos

- ❖Poseen una **amplia cifra oculta** a partir del bajo nivel de denuncia judicial que poseen en relación a los delitos convencionales

- ✓Algunas organizaciones no recurren a la justicia si sus sistemas informáticos fueron victimas de un ciberataque; la falta de legislación penal que tipifique este tipo de conductas; los problemas de jurisdicción y territorialidad que plantea la investigación criminal de este tipo de delitos por parte de la justicia
- ✓Las **resoluciones técnicas y administrativas** de los ciberdelitos.

INSEGURIDAD

Ciberdelito: Cómo evitar una modalidad que creció un 3000% con la cuarentena

Los delincuentes aprovechan las fallas en la seguridad y el poco interés de los bancos a la hora de extremar las medidas de prevención.

En el primer trimestre del año, la Argentina recibió 186 millones de ciberataques. Qué hacer para evitar el hackeo en épocas de pandemia. | CEDOC PERFIL

Marcos Teijeiro
Periodista de Información General.
teijeiromarcos ▶ Más notas de Marcos Teijeiro

21-05-2021 19:21

DIVISAS	COMPRA	VENTA
Dólar Oficial	97.33	103.33
Dólar blue	176.50	181.50
Dólar Solidario		170.49
Euro oficial	104.66	111.11
Euro blue	189.78	195.16

OPINIÓN

Características de los delitos informáticos

- ✓En términos criminológicos, el delito informático se explica por el **criterio de oportunidad.**

- ✓Teoría de elección racional: los individuos toman decisiones acerca de cometer un delito basándose en una serie de inputs entre los que figuran; el esfuerzo que implica, los beneficios potenciales, el apoyo con el que cuenta, el esfuerzo que implica, el riesgo de ser detenido y las necesidades particulares de la propia persona.

Características de los delitos informáticos

- ✓Teoría de la elección racional: Relación inversamente proporcional que afirma a mayores oportunidades situacionales para la comisión de un delito, menores posibilidades de riesgo para el delincuente de ser atrapado.

- ✓Internet: medio de alcance global que brinda a un usuario comunicarse con una gran cantidad de personas a la vez mediante el uso de servicios y aplicaciones gratuitos y con posibilidades de establecer comunicaciones anónimas a partir de la construcción de identidades ficticias.

Ciberdelitos en pandemia

- ✓Mayor cantidad de denuncias sobre delitos patrimoniales que afectan a las personas e instituciones.
- ✓**Mayor sofisticación y complejidad en las técnicas** en la comisión de ciberdelitos: esto arroja como resultado **nuevas modalidades de delitos informáticos ya existentes.**
- ✓Aparición de **asociaciones ilícitas, grupos criminales con cierto grado de organización** que toman al ciberdelito como emprendimiento delictivo.

Ciberdelitos en pandemia

Modalidades delictivas frecuentes:

- ❖A nivel de usuarios particulares
- ✓**Fraudes y estafas en línea**, fundamentalmente basadas en campañas de phishing

- ❖A nivel de organizaciones:
- ✓Ataques de **ransomware** o “secuestro de datos”

Fraudes y estafas en línea

- ✓**Fraude:** según la OCDE *"adquisición indebida de bienes ajenos por medio del engaño".* 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.

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

Fraudes y estafas en línea

Fraudes por Internet (Departamento de Justicia de los EEUU):

"cualquier tipo de fraude que utiliza uno o más componentes de Internet (…) para presentar solicitudes a posibles víctimas para llevar a cabo transacciones fraudulentas…"

Fraudes y estafas en línea

Phishing: *password harvesting fishing* (cosecha y pesca de contraseñas).

- ✓Consiste en obtención de datos personales de la victima mediante un mensaje fraudulento donde el “phisher” simula una comunicación de un banco, una tarjeta de crédito, una empresa de servicios, un organismo gubernamental o una ONG, entre otros, con el fin de utilizar esa información para la comisión de un delito posterior.
- ✓Técnica para el “robo de identidad”

Fraudes y estafas en línea

Phishing tradicional:

- ✓Consiste en que la víctima valide o confirme ciertos datos mediante una comunicación de correo electrónico por cuestiones vinculadas a la actualización de datos, la seguridad de los sistemas, perjuicios legales o patrimoniales, o el aprovechamiento de una oferta o promoción, entro otros motivos.
- ✓El cuerpo del mensaje contiene un enlace que deriva a un sitio web falso creado por el estafador para que la victima vuelque sus datos personales.

Fraudes y estafas en línea

- ✓El mas común es el **phishing bancario**, donde una supuesta institución bancaria solicita valide el usuario y contraseña de acceso a homebanking.

- ✓El “phisher” intentara utilizar esos datos para hacer transferencias bancarias a una cuenta.


Borradores
Enviados
Eliminados
Comentarios
PHP
Nueva carpeta
Santander
Estimado cliente:
Phishing
Notificamos que su tarjeta de Banco Santander se ha suspendido temporalmente debido a intentos fallidos de uso.
Como medida de seguridad hemos decidido desactivar su tarjeta temporalmente.
Para asegurarnos de su autenticidad rogamos reactivar su tarjeta desde el siguiente enlace el cual presentamos :
https://www.bancosantander.es/cssaSatellite?pagename=verification_cliente43287jkru43i4rhf
Spam Loco
202.91.12.181/SUPFPA_ENS/
© 2014 Microsoft
Términos
Privacidad y cookies
Desarrolladores
Español

Santander

Identificación de usuarios

Introduzca sus datos de identificación.

Número de DNI/NIE	
Fecha de nacimiento	
Datos de la tarjeta	
Número tarjeta	
CVV	
PIN de cajero	
FIRMA	

Acceder con DNI electrónico

Introduzca primero el DNI electrónico en el lector
Acceder con: Acceder con DNI electrónico<p id="dr
lector

Fraudes y estafas en línea durante pandemia

- ✓A partir del Aislamiento Social Preventivo y Obligatorio (ASPO) decretado por el gobierno durante marzo de 2020, se ha notado un incremento de modalidades fraudulentas a través de cuentas falsas de bancos creadas en redes sociales.
- ✓El consecuente incremento de vías de contacto web para la realización de tramites en línea a partir de servicios digitales brindó la oportunidad a los phishers de explotar nuevas formas de obtención de las claves de homebanking
- ✓Perfiles falsos en Instagram -y en menor medida Facebook- simulaban ser las cuentas oficiales del banco.

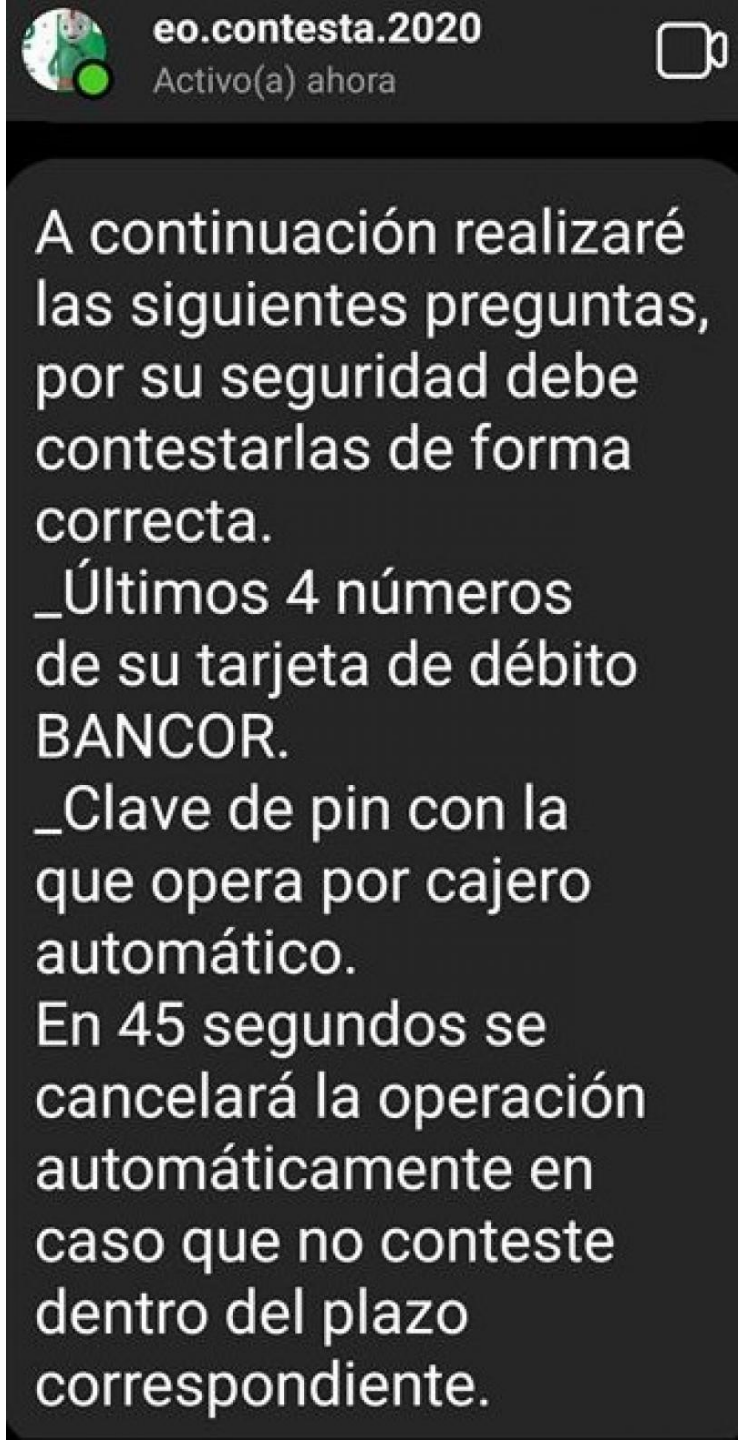
Fraudes y estafas en línea durante pandemia

- ✓A diferencia del phishing tradicional donde se envían comunicaciones generales a partir de un listado de direcciones de correos electrónicos -mailist-, los usuarios que comenzaron a seguir dichas cuentas eran en su mayoría clientes de la institución bancaria, lo que hace más selectivo el fraude en cuanto al universo de víctimas.
- ✓De esta manera, el estafador establecía comunicación con la victima vía mensaje directo con la misma lógica del phishing general.

La Voz

Por Instagram, el cuento del tío a clientes de Bancor

Foto ilustrativa.

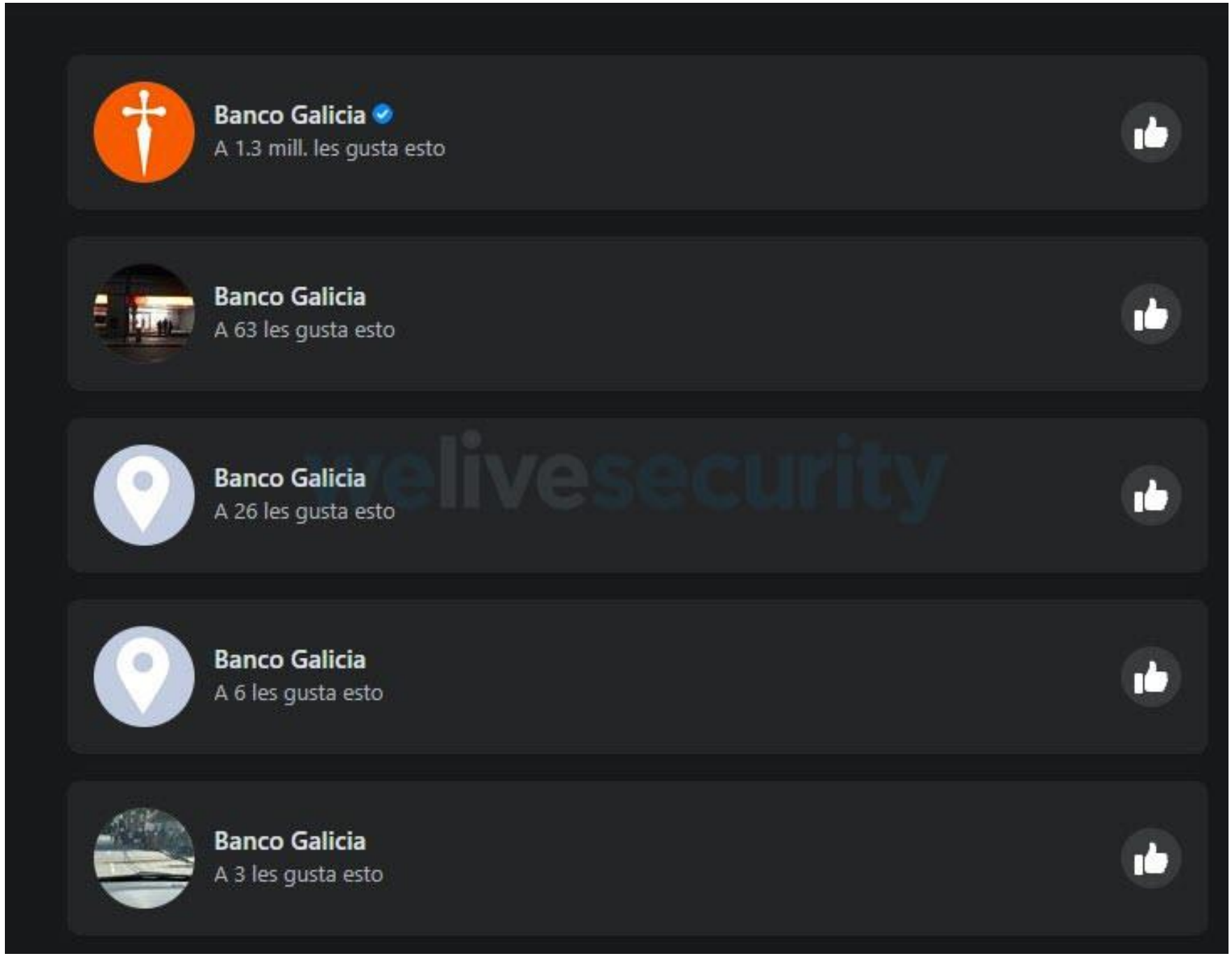

eo.contesta.2020
Activo(a) ahora
A continuación realizaré las siguientes preguntas, por su seguridad debe contestarlas de forma correcta.
_Últimos 4 números de su tarjeta de débito BANCOR.
_Clave de pin con la que opera por cajero automático.
En 45 segundos se cancelará la operación automáticamente en caso que no conteste dentro del plazo correspondiente.

banco_galicia_11 Seguir también

1 publicación **31** seguidores **263** seguidos

Banco Galicia
Atención al cliente

PUBLICACIONES ETIQUETADAS


Banco Galicia
A 1.3 mill. les gusta esto
Banco Galicia
A 63 les gusta esto
Banco Galicia
A 26 les gusta esto
Banco Galicia
A 6 les gusta esto
Banco Galicia
A 3 les gusta esto

Fraudes y estafas en línea durante pandemia

✓Los phishers explotan tres vulnerabilidades:

1. Tanto en Instagram, Facebook o WhatsApp, las cuentas que aparecen con un tilde son **cuentas verificadas o certificadas** por la empresa META. Las mismas acreditan la identidad de la persona o la organización que se encuentra detrás de la cuenta. No todos los usuarios conocen esta medida de seguridad
2. No existe el impedimento técnico de **creación de cuentas duplicadas**, sin ningún tipo de alerta o verificación por parte de la empresa. Estos dos factores lo que facilita la comisión de este fraude por parte de los ciberdelincuentes.
3. El **factor temor** de los clientes, a ver poder ver afectada su solvencia económica en pleno ASPO.

Fraudes y estafas en línea durante pandemia

- ✓En relación a los fraudes y estafas, durante la pandemia, estas solicitudes comenzaron a ser dirigidas, personalizadas; inclusive con datos previos de la víctima. Esta modalidad se denomina ***spearphishing.***
- ✓Dicha información previa de la victima puede ser obtenida mediante fuentes digitales abiertas en Internet en un proceso de búsqueda que establece el estafador.
- ✓**Tambien de archivos o bases de datos personales digitalizadas de las organizaciones que administran información de terceros.**

Fraudes y estafas en línea durante pandemia

Fuentes:

- ✓La sustracción de información mediante el acceso remoto por parte de ciberdelincuentes a un sistema informático (hackeo).
- ✓La filtración publica de las bases de datos por una falla en las políticas de seguridad de la información de la organización.
- ✓***Robo de información de las bases de datos personales de las organizaciones del "empleado Infiel".***

- ❖Compra y adquisición de bases de datos personales de terceros en la Dark Web.

Deep y Dark Web

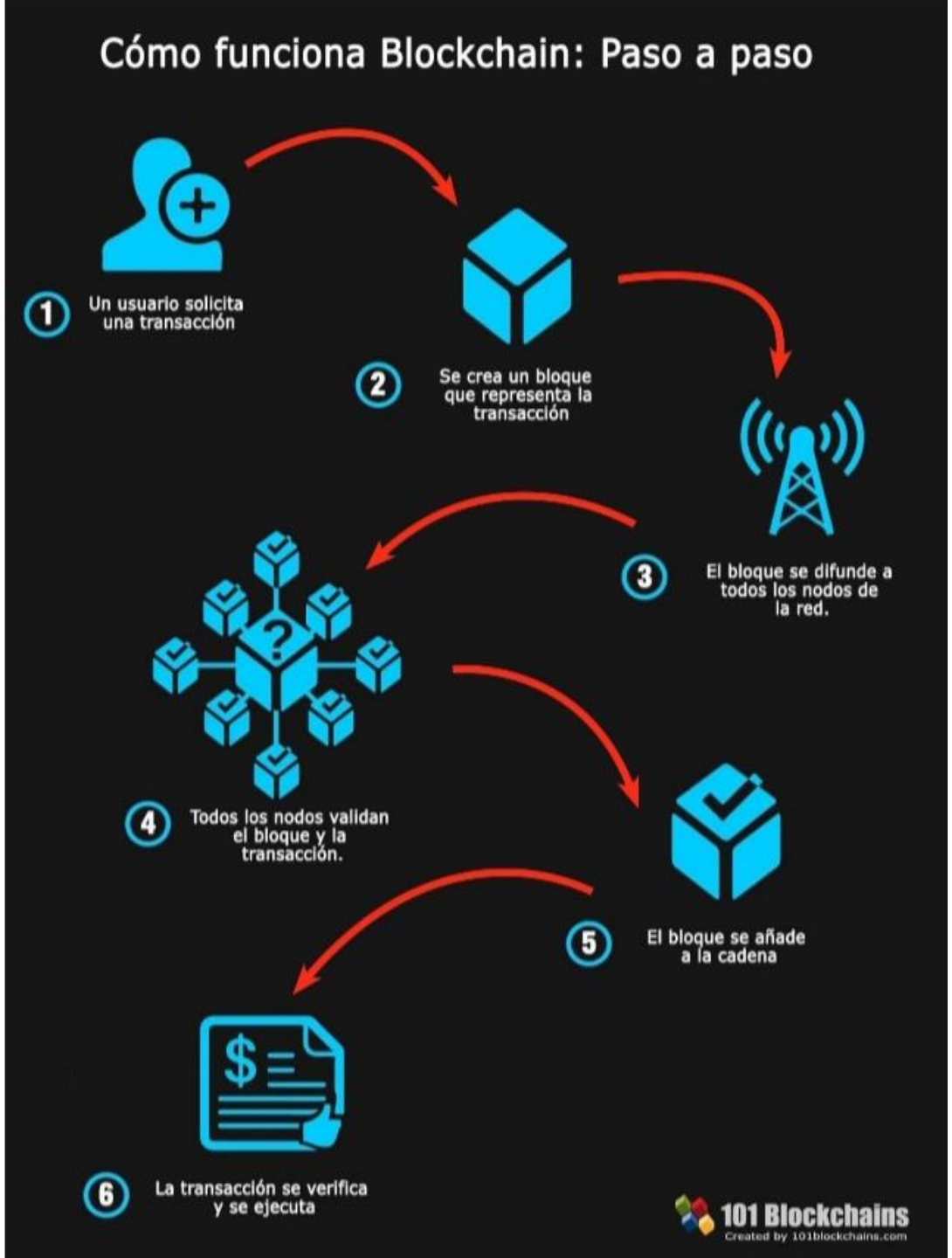
Deep Web” o “Internet profunda”:

- ✓Son redes descentralizadas que alojan sitios web no públicos, -no localizados por los motores de búsqueda- para mantenerlos inaccesibles.
- ✓Para su uso se requiere de un navegador específico.
- ✓El objetivo es mantener la privacidad de las comunicaciones y el anonimato de sus usuarios.

Deep y Dark Web

- ✓Funcionan a través de una cadena de bloques (blockchain).

- ✓Se basan en **redes TOR** (The Onion Router, el router cebolla) donde se enruta el tráfico a través de múltiples servidores y se cifra en cada paso del camino, ocultando la dirección de origen para mantener el anonimato.


Cómo funciona Blockchain: Paso a paso
1
Un usuario solicita una transacción
2
Se crea un bloque que representa la transacción
3
El bloque se difunde a todos los nodos de la red.
4
Todos los nodos validan el bloque y la transacción.
5
El bloque se añade a la cadena
6
La transacción se verifica y se ejecuta
101 Blockchains
Created by 101blockchains.com

Deep y Dark Web

- ✓También se utilizan las redes TOR para el desarrollo de actividades delictivas:

- ✓Para establecer una diferenciación con los usos lícitos, aquellas redes TOR utilizadas para emprendimientos delictivos se las denomina como parte de la **Dark Web o Internet oscura**


Surface Web
10% de Internet
Internet Indexado
Deep Web
90% de Internet
Internet no Indexado
Dark Web (Darknet)
Servicios Ocultos
I2P
Tor
freenet

Fraudes y estafas en línea durante pandemia

❖***Fraude de la cuenta vulnerada***

✓La víctima recibe un mensaje de WhatsApp entrada la madrugada donde un supuesto empleado de Twitter le informa que su cuenta ha sido hackeada y para recuperarla, debe validar ciertos datos personales para acreditar que el la legitima usuaria.

✓El estafador comparte una imagen verdadera de la víctima, en este caso, su foto u número de pasaporte para que acredite que es la legitima propietaria de la cuenta.

✓La comunicación escrita estuvo acompañada con videollamadas realizadas dentro de la aplicación tanto así como comunicaciones telefónicas a su línea móvil.

+1 (435) 224-5240

Este chat es con una cuenta de empresa. Toca para obtener más información.

Hola buenos días [redacted]
ANDREA FABIANA ([redacted]), soy Marcelo Soporte de Twitter, me contacto con vos ya que hemos detectado unos inicios de sesion sospechosos en tu cuenta de Twitter y para corroborar y dejar asentado de que esta todo en orden le quiero hacer unas preguntas. Se detectaron +3 inicios de sesion desde "Santa Fe, Argentina", le voy a pedir que se ponga en contacto conmigo cuanto antes, le adjunto una imagen con su estado de cuenta de Twitter.
Usuario: [redacted] 00:12

Este chat es con una cuenta de empresa. Toca para obtener más información.

Llamada perdida a las 00:14

Llamada perdida a las 00:16

2 MENSAJES NO LEÍDOS Y 2 LLAMADAS PERDIDAS

Le parece si le hago las preguntas de seguridad asi comenzamos el protocolo de seguridad?, son unas preguntas faciles 00:18

Llamada perdida a las 00:25

1- Es usted la dueña de la cuenta? 00:33

Llamada perdida a las 00:33

Esta cuenta de empresa ahora se ha registrado como una cuenta estándar. Toca para más información.

Escribe un mensaje

Fraudes y estafas en línea durante pandemia

- ✓El engaño a su vez utiliza una técnica delictiva frecuente del mundo físico, en este caso utilizando el modus operandi utilizados en los “secuestros virtuales” estableciendo una comunicación durante la madrugada.
- ✓Los secuestros virtuales se producen mediante la vía de contacto telefónico por parte del supuesto secuestrador donde un llamado alerta a un familiar durante la noche del secuestro del mismo y del lugar de pago de un rescate para su pronta liberación, generalmente un lugar cercano al domicilio.

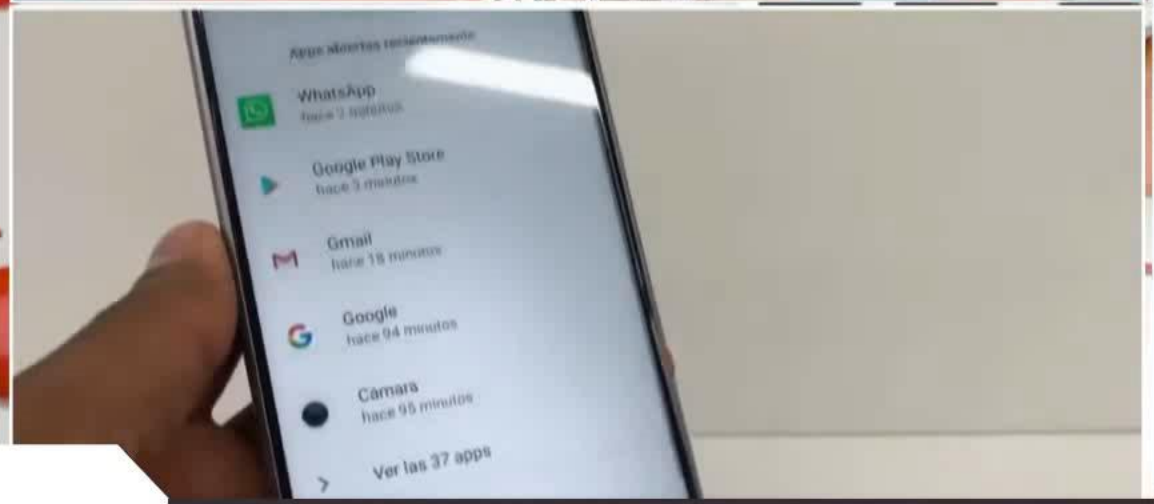
Fraudes y estafas en línea durante pandemia

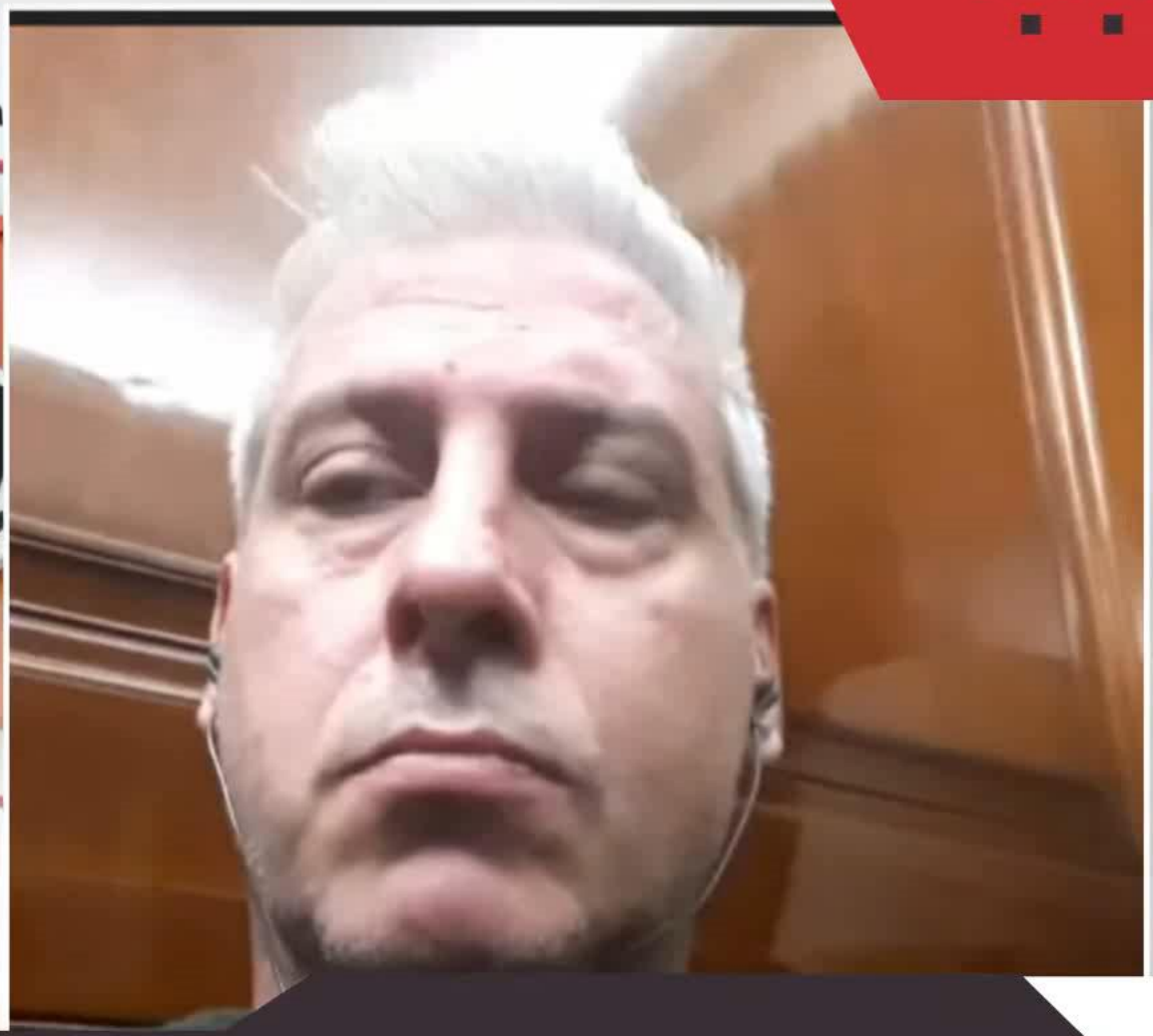
- ✓Durante la pandemia, los phishers no sólo aprovecharon las oportunidades generadas por las empresas proveedoras de servicio de Internet sino que también alguna “vulnerabilidad de las victimas”.
- ✓Los fraudes siempre refieren a temáticas actuales, intentando generar un interés en la persona.
- ✓Los mensajes intentan llamar la atención de la victima intentan explotar factores como la *curiosidad, el temor, la necesidad, la ambición, el sentimiento de caridad, entre otras.*

Fraudes y estafas en línea durante pandemia

El phisher explota tres vulnerabilidades:

1. El **servicio de alerta** utilizado por algunas empresas proveedoras de servicio cuando detecta un **acceso inusual** a una cuenta donde a través de un mensaje alerta al titular de la misma.
2. Apela **la confusión** de la victima al establecer la comunicación a altas horas de la noche, donde habitualmente una persona se encuentra cansada física y mentalmente y/o dormida.
3. Se vale del **factor miedo**, ante la posibilidad de que el usuario pierda el manejo de su cuenta, sus contactos y/o pueda ser utilizada para fines ilícitos.





C5N

ESTAFADORES VIRTUALES ROBAN DATOS POR WHATSAPP

Fraudes y estafas en línea durante pandemia

❖***Fraude de turno de vacunación***

✓El phisher contaba con el número de celular, nombre, apellido y documento de la potencial víctima y establecía una comunicación fraudulenta por WhatsApp haciéndose pasar por personal del Ministerio de Salud del Gobierno de la Ciudad Autónoma de Buenos Aires

✓En la comunicación se le informaba que se le va a comunicar fecha, hora y lugar de aplicación de la segunda dosis de la vacuna contra el COVID-19 siempre y cuando le brinde un el código numérico de seis dígitos que llegaría por mensaje de texto al celular (SMS).

Fraudes y estafas en línea durante pandemia

Aquí el phisher explota tres vulnerabilidades:

- ✓El gobierno de CABA notificaba los turnos de vacunación mediante el servicio de mensajería WhatsApp, **no poseía aplicación oficial.**
- ✓El phisher se vale del **factor de doble autenticación**, una medida de seguridad que brindan algunas empresas proveedoras de servicio de Internet cada vez que un usuario se inicia una nueva sesión en un dispositivo que no es habitual para acreditar su identidad.
- ✓El factor **necesidad** de la victima, cuestión vinculada a aumentar las defensas de salud ante la posibilidad de contagio de una enfermedad en el marco de una pandemia


13:11
Mensajes de texto con 34000 (SMS/MMS)
Codigo de WhatsApp: 820-677
O sigue este enlace
para verificar tu numero:
v.whatsapp.com/820677

Fraudes y estafas en línea durante pandemia

- ✓Una vez que el phisher obtiene el código de seis dígitos, se sincronizan los contactos de la víctima en su dispositivo.
- ✓Suplantando su identidad, la estafa consiste en solicitar ayuda económica a partir de una urgencia o el ofrecimiento de dólares a bajo precio de mercado.
- ✓El fraude también puede realizarse usurpando la identidad de la victima con un numero telefónico distinto aduciendo haber perdido el anterior mediante el acceso a los contactos a través de gmail.

Roberto Lavagna ✓
@RLavagna

CUIDADO: en épocas de estafas bancarias y pishing también hay estafas mediante WhatsApp. En esta oportunidad me tocó a mi. Desde un tel envían mensajes a contactos diciendo que cambié el número de teléfono y que actualicen el mismo (falso) ->

7:01 p. m. · 7 sept. 2021 · Twitter for Android

19 Retweets **9** Tweets citados **36** Me gusta

Gustavo Sylvestre ✓ @Gatosylvestre · 2h
Me paso lo mismo con este falso Lavagna.Denunciar de inmediato a cncrimcorr@pjn.gov.ar
Nueva modalidad de estafas!

> **Federico Pinedo** ✓ @PinedoFederico · 7 sept.
> Cuidado estafas!! Este se hace pasar por @RLavagna Lavagna y te pide comprar dólares
>
> 1 MENSAJE NO LEÍDO
>
> hola sabes quien me pueda comprar unos dolares que tengo de ahorros a buen precio !!
> Yo tengo problemas con mi cuenta bancaria y necesito

8 32 51

Fraudes y estafas en línea durante pandemia

❖***Fraude de compraventa de productos en redes sociales***

✓Durante la Pandemia se incremento mucho la venta online de productos por redes sociales. La empresa META, por ejemplo, creo Facebook Marketplace, un espacio dentro de la red social para que los usuarios puedan comprar y vender productos y servicios.

✓En este caso la empresa solo brinda el espacio para la actividad, no cobra comisiones, ni brinda seguros ni sistemas de pago, las transacciones las realizan los propios usuarios usando el servicio de Messenger para comunicarse u otra vía.

✓

Fraudes y estafas en línea durante pandemia

- ✓En este sentido se incrementaros las estafas, muchas de ellas en Instagram.
- ✓Los estafadores ofrecen productos siempre a bajo precio promedio de mercado, libre de impuestos en caso de productos importados por tratarse de “zona franca” de compraventa
- ✓Ofrecen garantías y muestras imágenes ficticias de clientes satisfechos acompañados de comentarios positivos de las transacciones realizadas, todas tomadas de forma publica de la web
- ✓Siempre los pagos deben ser en efectivo o deposito bancario.
- ✓La estafa consiste en comprar un producto, realizar el pago para después no recibirlo.

uno_gameer

24 Publicacio...
2,066 Seguidores
201 Seguidos

unogameer
Compras
Medios de pago. Debito u efectivo
Envios a todo el pais 📱🇦🇷
Compra protegida
Galería las América local 12. info whatsapp
Ver traducción
wa.me/message/KRW2UL4INAT5H1

Seguir | Mensaje

Reenvió un mensaje

Buenas te comunicaste con UNOGAMER. 🎮📱
Importamos productos desde Estados Unidos. En el estado de Florida 🇺🇸.
Costo a dolar oficial, Nos encon-tramos en Puerto iguazu Misiones. Zona franca libre de impuestos.
* Compra protegida de Mercado pago.
* Formas de pago. Tarjeta de credito. Debito y efectivo. Por Link de compra.
Envios a todo el pais por andreani demora maxima de 3 a 5 dias dependiendo la distancia. Para mas info comunicarse.
Lista de **precio.OFERTA** DEL MES.
PS5 DIGITAL 🛋️ 80.000$
PS5 BLURAY. 🛋️ 110.000$
XBOX SERIE X 🛋️ 90.000$
SAMUSUNG A71 📱 40.000$.
SAMSUNG A51 📱 32.000$
SAMSUNG A01 X 2 UNIDADES 📱 18.000$
XIAOMI NOTE 10 45.000$ 📱
PS4 PRO . 40.000$
PS4 SLIM 30.000$ para mas info
https://wa.me/message/WLAGSXUKAL5MB1

uno_gameer

67 Me gusta
uno_gameer Gracias a cada uno de ustdes, seguimos trabajando para vos!... más
28 de julio • Ver traducción

paseogames

12 Me gusta

paseogames Gracias por su confianza siempre 🙏🤩

16 de julio · Ver traducción

paseogames

14 Me gusta

paseogames Gracias por la confianza #paseogames... más

19 de julio · Ver traducción

Lavado de dinero por Internet

- ✓El dinero de los fraudes van a parar a determinadas cuentas bancarias, sobre todo a aquellos que se les solicita transferencia de fondos o los phishers se hacen con las credenciales de acceso al sistema de homebanking de las victimas para vaciarles la cuenta y transferirlas a una “propia”.
- ✓¿Quienes son los titulares de dichas cuentas?
- ✓Se utilizan las llamadas “mulas digitales” que ofician como intermediarios en la operatoria ilícita.

Lavado de dinero por Internet

- ✓Desde hace algunos años surgieron dentro del sistema financiero los bancos digitales.
- ✓Son parte de las llamadas *fintech* (conjunción de las palabras financial technology, tecnologías digitales aplicadas a las finanzas)
- ✓Son institucionales bancarias 100% digitales, sin sucursales físicas que operan en Internet ni operatorias con dinero físico.
- ✓Se encuentran regulados por la normativa del BCRA.

Lavado de dinero por Internet

❖ Bancos digitales o billeteras electrónicas

Servicios que ofrecen:

✓ Apertura de cajas de ahorro (pesos y dólares), posibilidad de trasferencias de fondos, plazos fijos, tarjetas de crédito plásticas y/o virtuales (en oportunidades a clientes no bancarizados), prestamos.

Lavado de dinero por Internet

- ✓A diferencia de los bancos tradicionales, para la apertura de cuentas el titular no necesita acreditar concurrir personalmente a una sucursal física, el proceso es 100% online.
- ✓Los mecanismos de acreditación de identidad de estos bancos pasan por el uso de programas de inteligencia artificial donde se el exige al interesado enviar fotos de su rostro en diferentes posiciones, videos, para luego cotejarlos con la base de datos del Registro Nacional de las Personas del Ministerio del Interior (RENAPER).
- ✓Asimismo, algunos de estos bancos permiten la apertura de varias cuentas a la vez de parte de un mismo titular.

Lavado de dinero por Internet

- ✓Algunas asociaciones ilícitas ofrecen a personas oficiar como intermediario de los fraudes a cambio de un porcentaje de dinero mediante la apertura de la cuenta, el retiro de dinero y la entrega a un “cadete”.

- ✓En este caso esta persona pasa a ser parte de la operatoria ilícita como “mula digital”.

infobae

ARGENTINA AMÉRICA MÉXICO COLOMBIA DEPORTES TENDENCIAS

Martes 24 de Mayo de 2022

Dólar Banco Nación Dólar Bolsa Euro Real Libra Peso Uruguayo Real State

INFOBAE

Para evitar el lavado de dinero, las empresas de cuentas digitales deberán informar los movimientos de sus clientes

La Unidad de Información Financiera emitió una resolución que brinda un nuevo marco regulatorio para las empresas del sector con el objetivo de prevenir el lavado de activos

5 de Agosto de 2019

Las cuentas virtuales o billeteras electrónicas deberán informar movimiento de sus clientes

El BCRA reforzó las medidas para mejorar la seguridad de las billeteras digitales

Con el objetivo de reforzar las medidas para mitigar el fraude en las operaciones con billeteras digitales, el Directorio del Banco Central de la República Argentina (BCRA) estableció nuevos requisitos técnicos para los Prestadores de Servicios de Pago (PSP) y las entidades financieras que ofrecen el servicio de billetera digital, las que además deberán obtener una certificación del Registro de Billeteras Digitales Interoperables para poder dar el servicio de pago con transferencia (PCT).

Los requisitos técnicos complementan y refuerzan las medidas de seguridad previamente adoptadas por esta Institución y se basan en la necesidad de interacción entre las billeteras y los proveedores de cuentas (bancarias o de pagos), con el fin de gestionar el consentimiento del cliente para vincular su cuenta a la billetera donde desee operar.

De esta manera, se agrega un proceso técnico de seguridad a la ya implementada autenticación del cliente y autorización ante instrucción de pago.

Lavado de dinero por Internet

- ✓En oportunidades, algunos usuarios pueden oficiar como mula digital, ser parte de una asociación ilícita, sin tener conocimiento de ello mediante un engaño.

- ✓Se han registrado casos producidos mediante ***fraudes de empleo desde el hogar***.

Lavado de dinero por Internet

- ✓Mediante correos electrónicos, mensajes en redes sociales, chats o publicidades en línea se publican avisos invitando a las personas a trabajar desde el hogar sin ningún antecedente profesional ni experiencia previa bajo promesa de una buena remuneración invirtiendo pocas horas de trabajo.
- ✓En este caso, tras el ofrecimiento formal de formar 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.

Lavado de dinero por Internet

- ✓Una vez realizado el depósito, se le solicita al "empleado" entregar el dinero a un "corresponsal" de la firma. Así, en la operatoria ilícita, el único registro final electrónico es la cuenta bancaria de la víctima.
- ✓Durante el último tiempo se ha incrementado esta modalidad solicitando el uso de cuentas de Mercado Pago -el sistema de pago electrónico de la empresa Mercado Libre- fundamentalmente para el cobro de dinero obtenido de fraudes.

Trabajar en Internet Llenando Encuestas

¡Por Favor Compártelo!

Las encuestas en Internet son posiblemente el método más popular de hacer dinero extra sin mucho esfuerzo. Existen muchas compañías en Estados Unidos, Canadá y Europa que pagan por completar encuestas acerca de productos o marcas de productos conocidos, con el objeto de poder mejorar y ser más competitivas. En el mundo globalizado en el que vivimos, las empresas grandes fabricantes de productos o proveedores de servicios, no pueden permitirse el lujo de cometer errores de marketing, diseño de productos, logística, etc. Es por eso, que les resulta más económico pagar a gente por Internet para obtener buenas opiniones e ideas o sugerencias y mejorar la forma de hacer negocios. Al fin de cuentas, eso les resultará más económico que las pérdidas por haber fabricado miles o millones de productos con fallas o propaganda que no vende.

Ransomware

- ✓Conjunción de “*ransom*” -rescate- y software.
- ✓Programa malicioso (malware) orientado a “secuestrar” datos e información de un dispositivo impidiendo el acceso a los archivos del mismo salvo que se pague un “rescate” para liberarlos.

Ransomware

- ✓Los primeros tipos de ransomware sólo bloqueaban el acceso al equipo de un usuario haciéndoles llegar un supuesto mensaje proveniente de agencias de seguridad acusándolos de infligir la ley.
- ✓Los argumentos eran los de visitar sitios web de pornografía y descarga de archivos protegidos por los derechos de autor (música, películas, etc.).

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through MoneyPak:
To pay the fine, you should enter the digits resulting code, which is located on the back of your Moneypak, in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

OK

Ransomware

- ✓En un principio las víctimas eran generales y se utilizaban direcciones de mail que aparecían en la web para el envío de phishing mediante correo electrónico no deseado (SPAM), donde el extorsionador iba a tratar de hacerse con las credenciales de acceso de un empleado de una organización para ingresar a los sistemas informáticos de la misma e instalar el malware.

Ransomware

Abril de 2017:

- ✓El ransomware WannaCry afectó a aproximadamente 200.000 usuarios de más de 150 países.
- ✓Mas allá de la dimensión global del ciberataque el caso tomo repercusión porque afectó a las computadoras de hospitales en Gran Bretaña, días después del atentado en el Puente del Westminster a metros del Parlamento Británico donde un automóvil atropelló a las de 40 personas.

Ransomware

- ✓El mismo se produjo mediante la ejecucion de un programa de cifrado que encriptaba los archivos impidiendo su acceso a los legítimos usuarios de la organización.

- ✓Así, el/los extorsionadores solicitaban rescate a partir del pago de criptomonedas para “liberar” las bases de datos.

Ransomware

❖Desde poco antes de la pandemia, los atacantes de ransomware comenzaron a implementar una nueva modalidad delictiva:

✓Una vez vulnerada de la red corporativa -antes de plantar el software malicioso- los extorsionadores realizan en forma remota copias de información sensible de la base de datos de la organización.

✓Finalizada esta acción, cifran la información y comienza una doble extorsión, por un lado solicitan rescate para desencriptar los archivos mientras que por otro, piden dinero a cambio de para no hacer publica dicha información en la web.

HOW_TO_DECRYPT.txt - Notepad

File Edit Format View Help

Your network has been breached and all data is encrypted.

To decrypt all the data you will need to purchase our decryption software.
Please contact our sales department at:

http://hivecust6vhekztbqgdnkks64ucehqacge3dij3gyrrpdp57zoq3ooqd.onion/
Login: EQA9oydTxwXS
Password: vNtgAgb3kMFmCooANNQr

Follow the guidelines below to avoid losing your data:

- Do not shutdown or reboot your computers, unmount external storages.
- Do not try to decrypt data using third party software. It may cause irreversible damage.
- Do not fool yourself. Encryption has perfect secrecy and it's impossible to decrypt without knowing the key.
- Do not modify, rename or delete *.key.hive files. Your data will be undecryptable.
- Do not modify or rename encrypted files. You will lose them.
- Do not report to authorities. The negotiation process will be terminated immediately and the key will be erased.
- Do not reject to purchase. Your sensitive data will be publicly disclosed at http://hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd.onion/

Ransomware

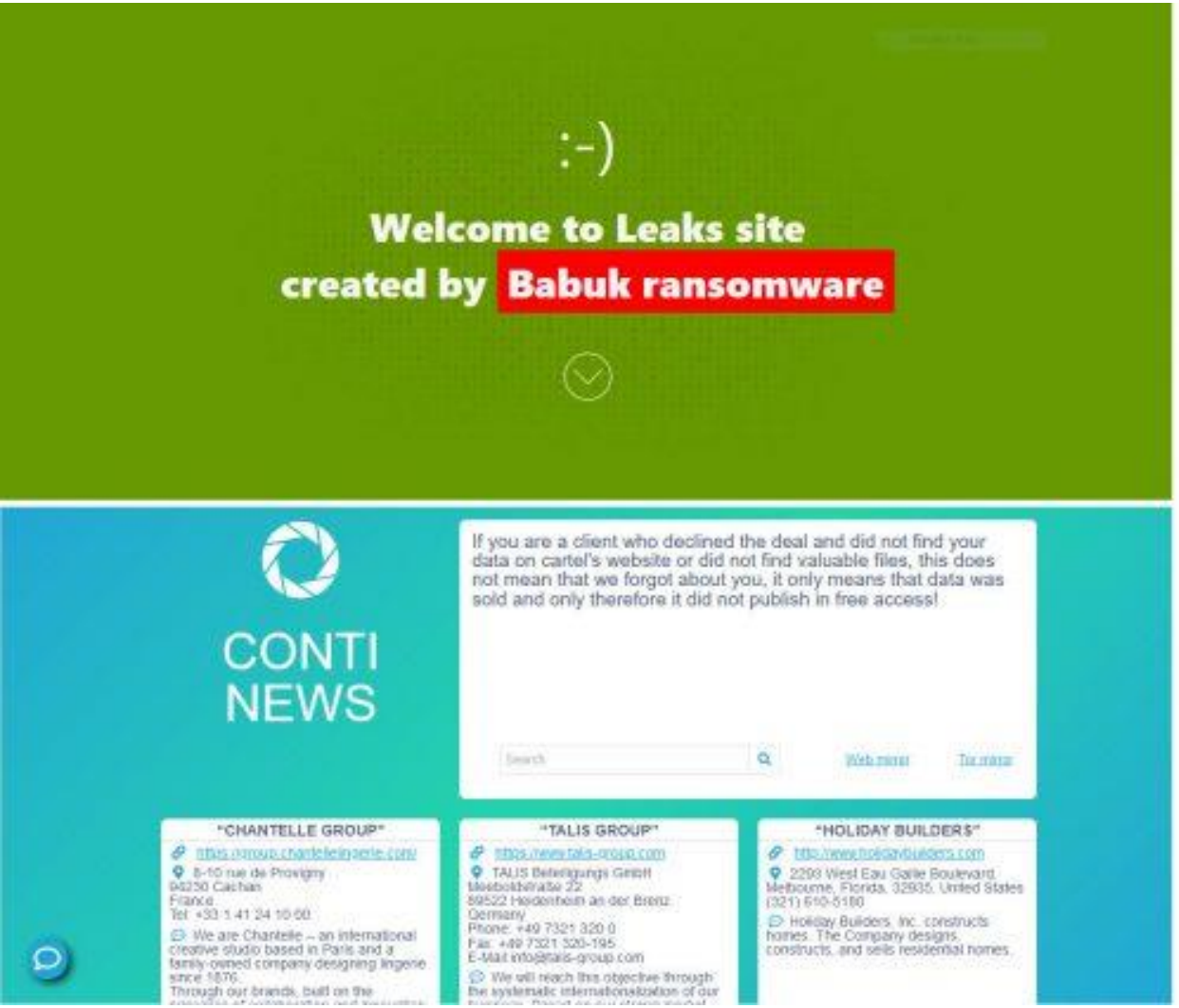
- ✓Asimismo aumentaron los ataques mediante la explotación de vulnerabilidades de los sistemas a partir del uso de exploits” -software que intentan detectar los fallos de seguridad de los programas y aplicaciones- para generar “puertas traseras”

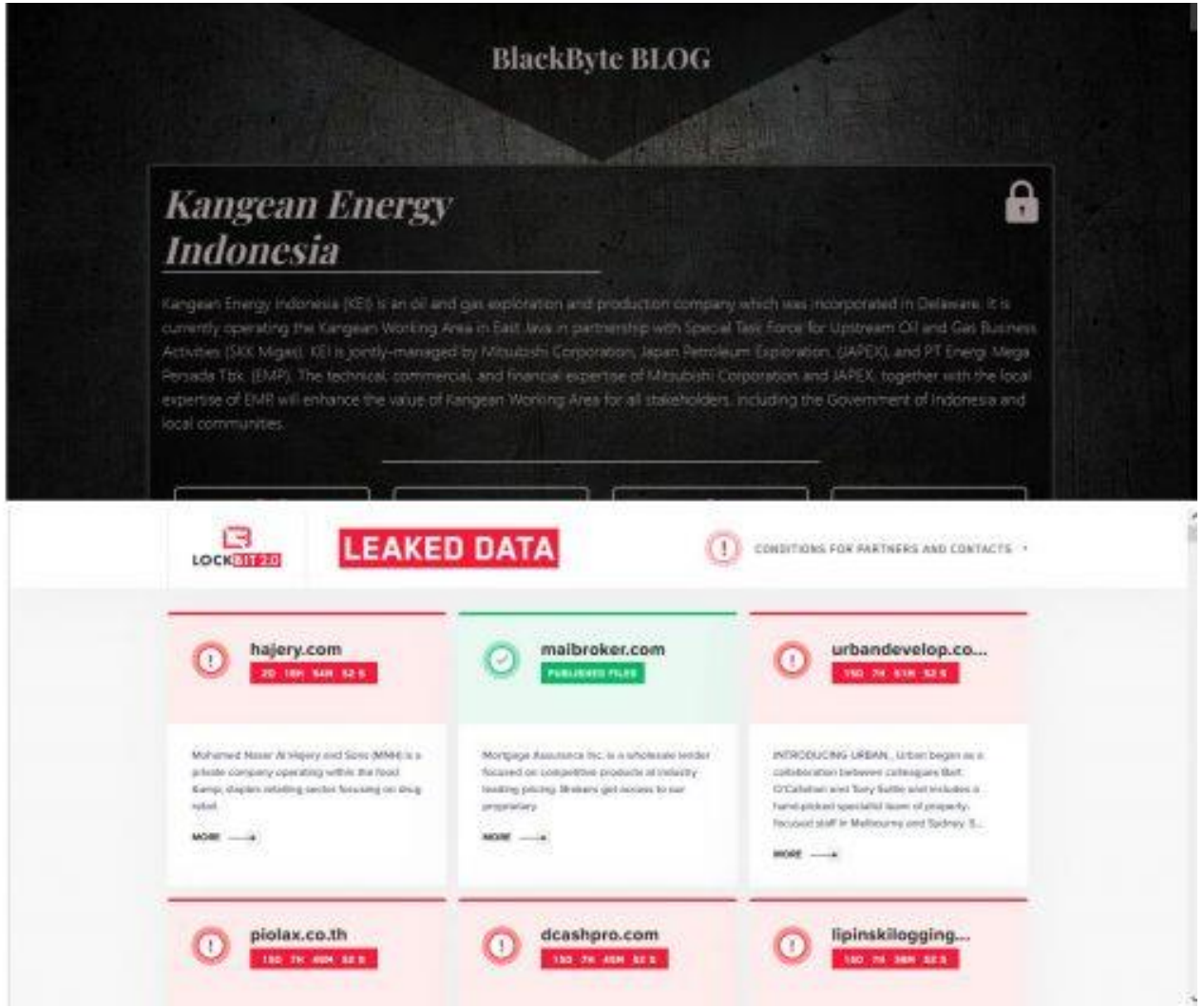
- ✓Comenzaron los ataques de fuerza bruta a los empleados de las organizaciones que se conectaban a las redes corporativas a partir de la expansión del trabajo remoto o teletrabajo.

Ransomware

- ✓Asimismo se incrementó notablemente la cantidad de sitios donde se ofrecimiento del ransomware como servicio por parte de ciberdelincuentes en la Dark Web

- ✓El modelo de negocios de ransomware como servicio (RaaS, por sus siglas en inglés) incluye la descarga del software malicioso, soporte, la venta de vulnerabilidades Zero Day y de credenciales de acceso robadas por un lado, como así la posibilidad de asociarse con grupos de ciberdelincuentes para ejecutar ataques a cambio de un porcentaje de las rentabilidades, por otro.


:-)
Welcome to Leaks site
created by Babuk ransomware
CONTI
NEWS
If you are a client who declined the deal and did not find your data on cartel's website or did not find valuable files, this does not mean that we forgot about you, it only means that data was sold and only therefore it did not publish in free access!
"CHANTELLE GROUP"
"TALIS GROUP"
"HOLIDAY BUILDERS"


BlackByte BLOG
Kangean Energy Indonesia
LOCKBIT 2.0
LEAKED DATA
CONDITIONS FOR PARTNERS AND CONTACTS
hajery.com
mailbroker.com
urbandevelop.co...
piolax.co.th
dcashpro.com
lipinskilogging...

Ransomware

- ✓Los desarrolladores de un ransomware ofrecen a hackers maliciosos —incluso sin grandes conocimientos técnicos—herramientas para que puedan iniciar una campaña de ransomware contra una víctima al contratar el servicio o la posibilidad de sumarse a través de un programa de afiliados para distribuir una familia de ransomware a cambio de un porcentaje de las ganancias.

Ransomware

- ✓Los afiliados, (quienes contratan el servicio) son responsables de distribuir la amenaza mediante el acceso a una infraestructura con software malicioso y el soporte.
- ✓tienen acceso a un panel de control donde podrán establecer los montos que solicitarán a cada víctima por el rescate y configurarán el mensaje para el usuario después del compromiso, entre otras cosas.
- ✓El concepto es muy similar a contratar un servicio en la nube, solo paga la tarifa mensual para tener acceso a todo lo que la estructura ofrece.

Ransomware

❖En estos últimos tiempos se presenta en algunos casos una nueva modalidad de extorsión:

✓Se amenaza a la organización con filtrar su información a sus clientes corporativos si es que brinda servicios a otras empresas y organizaciones, intentando afectar su imagen y reputación, un claro intento de perjudicarla económicamente, lo que constituiría una triple extorsión.

Ransomware

- ✓Asimismo durante pandemia, se registró un incremento de ataques a infraestructuras críticas de información (IICC), sistemas informáticos que hacen al funcionamiento de servicios esenciales de un país o región (red eléctrica, servicio de provisión de combustible, sistemas hidrológicos, sistemas de transporte, conductos de gas, entre otros)

Ransomware

Mayo de 2021:

- ✓Un ataque de ransomware afectó a una empresa de transporte de petróleo y gas de los Estados Unidos, “Colonial Pipeline”, produciendo demoras en los servicios a toda la Costa Este de ese país durante casi una semana.
- ✓De manera preventiva, la firma decidió suspender la provisión de insumos desde la ciudad de Houston hasta New York ante la posibilidad de que los ciberdelincuentes dañaran físicamente el oleducto.

Ransomware

- ✓El ataque comprometió información corporativa sensible, motivo por el cual la empresa pagó 5 millones de dólares para la liberación (o no publicación) de la información cifrada.
- ✓Para el FBI se trató de un grupo organizado llamado “DarkSide” 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 aun no esclarecidos, pese a las recomendaciones habituales de no efectivizar el pago por parte de los especialistas.

"Te estoy sacando de un quilombo", los audios de las extorsiones a visitantes de una página de citas hot

Un preso, alojado en una unidad penitenciaria de Florencio Varela, engañaba a sus víctimas y les hacía creer que habían contactado a menores de edad que estaban bajo una red de trata de personas y les exigía dinero para evitar quedar imputados en una causa judicial; se estima que se hizo de un botín cercano a los 2.500.000 de pesos

16 de noviembre de 2021 • 08:00

Fraude de soborno extorsivo

- ✓El fraude se inicia a partir de un intercambio de mensajes por parte de un usuario hombre con una interlocutora mujer mediante los servicios de mensajería de una aplicación de encuentros o sistemas chats que existen dentro de sitios web de citas.
- ✓En el proceso comunicacional, la mujer obtiene datos personales de la potencial como nombre, edad, ciudad de residencia y numero de teléfono celular de la victima.

Fraude de soborno extorsivo

- ✓En el intercambio, la mujer convence a la víctima de practicar sexting, dentro de la aplicación o el sitio o por sistema de mensajería.
- ✓El sexting es el intercambio de imágenes y videos eróticas y/o pornográficos con escenas de desnudez, semidesnudez o representaciones genitales para luego quedar en un posible encuentro personal posterior.

Fraude de soborno extorsivo

- ✓Una vez finalizado el intercambio, horas después llega una comunicación por WhasApp a la víctima por parte de un supuesto policía o empleado de una fiscalía aduciendo que dicha persona se había comunicado con una menor de edad victima de una red de trata que estaba siendo investigada por la justicia o en su defecto, que la madre o el padre de la menor se presentó en la comisaría para realizar la denuncia al descubrir los mensajes en el celular de su hija.

Fraude de soborno extorsivo

- ✓Una vez notificada la situación, el agente de la ley le ofrece solucionar el problema legal a cambio de una suma de dinero para evitar presentar la denuncia formalmente.
- ✓Para que el engaño sea mas creíble, el mensaje puede estar acompañado por el envío de una copia de la denuncia en curso donde figura el nombre de la victima y los cargos que se le imputa, como también así la muestra de las “pruebas”, las imágenes eróticas intercambiadas por el hombre dentro de la red social

GUARDIA CIVIL

ESTRUCTURAS DE COLABORACIÓN DE INTERPOL – POLICÍA DE SEGURIDAD Y GENDARMERÍA
DEPARTAMENTO FEDERAL DE JUSTICIA Y POLICÍA

A su atención:

Soy Dña. **María Gámez Gámez**, elegida para el cargo de Directora de la GUARDIA CIVIL, Comisaria de División, Jefa de la Brigada de Protección de Menores, me pongo en contacto con usted a poco tiempo de una incautación informática, Ciberinfiltración (Autorizada, especialmente en materia de pornografía infantil, pederastia, Ciberpornografía, exhibicionista, tráfico sexual desde (2009) Para informarle que es objeto de varias Actuaciones Judiciales en vigor

Tomaremos medidas legales contra usted poco después de una incautación por infiltración cibernética para : **Pedopornografía, Pedofilia, Ciberpornografía, Exhibicionismo**

Para su información, el legislador ha declarado que cuando los delitos previstos en el Código Penal se realicen a través de una red de telecomunicaciones, las sanciones penales previstas se verán incrementadas.

Tras la investigación, certificamos que ha cometido estos delitos, a saber, la adquisición, la posesión, el visionado, la transmisión y la consulta de imágenes y vídeos de carácter exhibicionista o pornográfico infantil, por medio de Internet (sitios de anuncios, sitios pornográficos, sitios de citas, redes sociales).

Durante la investigación, también observamos que se difundían contenidos obscenos suyos en sitios web o redes de gran audiencia, entre ellos muchos menores de 16 años.

Conviene recordar que cuando se exhibe la desnudez de esta manera, constituye un delito de exhibición sexual ante el público y ante los menores de 16 años. Este delito está severamente castigado por la ley.

Los registros de imágenes, vídeos de desnudos tuyos y de menores, grabados por la Ciberinfiltración son pruebas de tus delitos

Se le pide que se manifieste por correo electrónico, escribiendo sus justificaciones para que puedan ser examinadas y verificadas con el fin de evaluar las sanciones; esto en un plazo estricto de 48 horas. Transcurrido este plazo, nos veremos obligados a transmitir nuestro informe al Tribunal Judicial de su región, para el establecimiento de una orden de detención contra usted, que irá seguida de una detención inmediata por parte de la Policía de Seguridad más cercana a su domicilio.

A continuación, será inscrito en el Registro Nacional de Delincuentes Sexuales. En esta situación, su expediente también se remitirá a las organizaciones antipederastas y a los medios de comunicación para su publicación como persona en el NSOR.

DEPARTAMENTO DE COORDINACIÓN DE OPERACIONES : [redacted]

María Gámez Gámez,
DIRECTOR DE LA GUARDIA CIVIL
POLICÍA ESPAÑOLA
C. Gerona, 8, 47013 Valladolid, España

NICOLETTA DELLA VALLE
DIRECTRICE DE FEDPOL

Fraude de soborno extorsivo

- ✓El fraude extorsivo se complementa con amenazas de que si el pago no se realiza rápidamente su domicilio puede ser allanado o en su defecto, los padres de la menor van a hacer publica esa información en las redes sociales “escrachando”, en oportunidades, en medios de comunicación.

Fraude de soborno extorsivo

Aquí el estafador explota dos vulnerabilidades:

1. Las aplicaciones de citas o sitios de encuentros exigen en sus términos y condiciones de uso que los usuarios sean mayores de edad.

   El desconocimiento de esta condición por parte de los usuarios sumado a los **mecanismos de acreditación de identidad endebles** implementados por parte de las empresas brindar la oportunidad de comisión de esta estafa.

2. El factor **temor** de la victima ante la posibilidad de acarrerar problemas legales y de ver seriamente afectada su imagen y reputación a nivel social.

Prevención situacional en ciberseguridad

- ✓En criminología, existe una dimensión de la prevención delictiva que constituye un aspecto específico de la misma, que es el de *prevención situacional.*
- ✓Esta escuela criminológica surge durante los años 70 en Gran Bretaña y suele denominarse “orden público basado en resolución de problemas.
- ✓La prevención situacional se centra en problemas, lugares, personas y momentos específicos.

Prevención situacional en ciberseguridad

- ✓En materia de cibercriminalidad, existe una tendencia a establecer como factor más importante de la prevención la **concientización** de los usuarios en el uso de las tecnologías de la información y comunicación, fundamentalmente en Internet**.**
- ✓Volcado al plano de Internet, la concientización de los usuarios de servicios y aplicaciones web está dado por conocer cuáles son los peligros y amenazas en línea y modalidades delictivas que utilizan los ciberdelincuentes; que datos o información de tipo personal es recomendable publicar en Internet para no ser víctima de un ciberdelito y las vulnerabilidades técnicas de los dispositivos que puedan afectar la seguridad de la información que almacenan o contienen, entre otras.

Prevención situacional en ciberseguridad

- ✓En primer lugar, si la prevención de la cibercriminalidad se reduce únicamente a la concientización, si un usuario es víctima de un delito informatico es por que no ha tomado los recaudos suficientes, es decir, no ha tomado la conciencia suficiente, de los riesgos y posibilidades existentes en el manejo de la tecnología y en el uso de Internet.
- ✓En segundo lugar esto dejaría afuera quizá las oportunidades generadas por los fabricantes de tecnología informática, ingenieros de software y diseñadores o administradores de sitios web, entre otros, lo que presupone a su vez, que tanto la tecnología utilizada por las personas tanto así como los servicios y aplicaciones digitales son seguros por defecto.

Prevención situacional en ciberseguridad

- ✓La prevención en materia del ciberespacio, por ejemplo no debe limitarse únicamente a las medidas de resguardo que puedan adoptar las personas en el uso de las TICS e Internet, sino en la seguridad que puedan brindar tanto los fabricantes de dispositivos informáticos, los programadores de software y las empresas de servicio y aplicaciones en Internet para generar entornos digitales seguros, es decir, reducir las posibilidades de que se produzcan fallos de seguridad que puedan ser explotados por ciberdelincuentes.

Gustavo Sain
Dirección Nacional de Ciberseguridad
26 de Mayo 2022

EXTRAIDO DE

JEFATURA.SANTACRUZ.GOB.AR/CIBERSEGURIDAD2022/