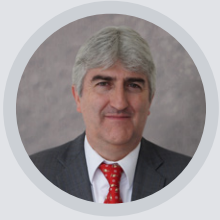
Crimen Cibernético en México

Diciembre 2020

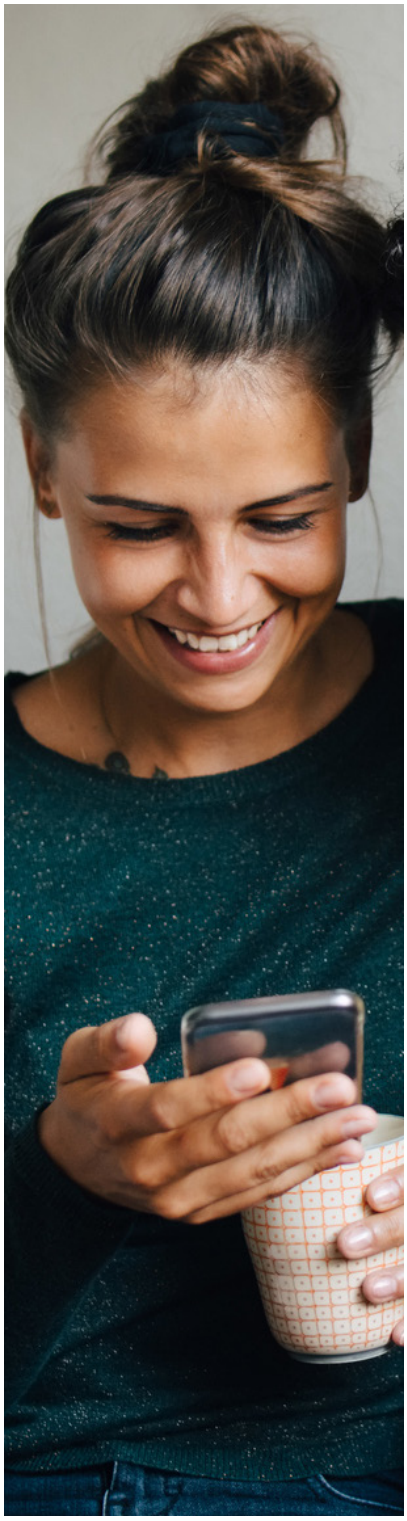
LOCKTON®

AUTORES

Ricardo Alvarado
Director Daños
ralvarado@mx.lockton.com



Luis Bernardo Macías
Productor
lbmacias@mx.lockton.com



Datos Duros sobre telefonía celular e internet en México

- En México hay **120 millones de celulares,** de los cuales el 88.1% son Smartphones.
- El número de usuarios de teléfonos Celulares en marzo de 2020, asciende a **86.5 millones.**
- El número de usuarios de internet es de **80.6 millones** y representan al 70.1% de la población de 6 años o más.
- La penetración del Internet, en las zonas urbanas es del 76.6%, mientras que en las zonas rurales del **47.7%.**
- Las redes sociales preferidas en México son **Tiktok, Instagram, Facebook, Whatsapp y YouTube.**
- Los usuarios pasan **40% de su tiempo** conectados en alguna red social.
- Preferencias de uso: **Smartphone 89%,** Laptop 49% y computadoras de escritorio 34%
- A partir de marzo, en un lapso de 3 meses, en el 2020 **la transformación digital se ha anticipado** a lo que crecería en 3 años **lo cual es aprovechado por los cibercriminales.**

Las hábitos de las personas con un nivel socioeconómico D+ a C+ incrementaron el uso de soluciones digitales para la adquisición de bienes y servicios, desde comida hasta para realizar “el super”.

En el 2020, el incremento de ataques cibernéticos no solo es dirigido a las empresas, sino a las personas

- El 40 % de los cyber ataques son Phising y Vishing(phising en teléfonos); México está entre el Top 10 de países con más phishing por el COVID-19.
- En el caso de robo de datos, se puede llegar a conocer en ocasiones, hasta 2 años después de sucedido.
- El 30% de los ataques registrados no recuperaron su información o sufrió algún daño.
- El crimen en línea ya representa el 50% de los delitos contra la propiedad en el mundo.
- En el Foro Económico Mundial del 2020 los ciberataques y robo de identidad está dentro de los 10 principales riesgos de ocurrencia.
- Para 2021 los daños por delitos cibernéticos alcanzaran los 6 billones de dls. El PIB de la tercera economía más grande del mundo.

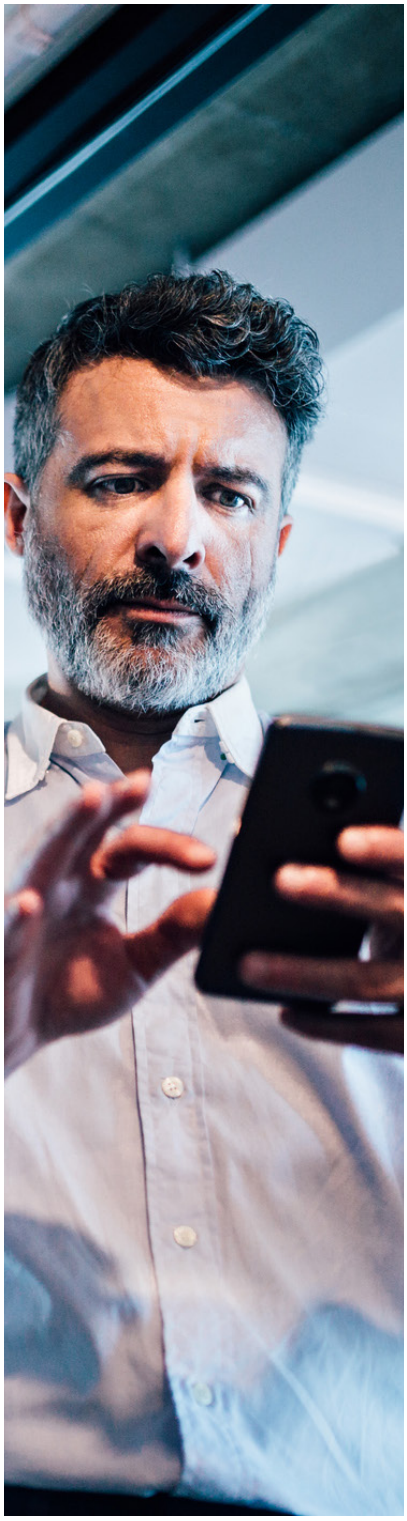
Situaciones comunes, ¿te suenan familiares?

- Estaba navegando en mi computadora y de la nada... ¡dejo de funcionar! y de repente apareció en mi pantalla un mensaje que mi información había sido encriptada y para liberarla tengo que pagar US $400 en bitcoins para recuperarla. ¡Todo por abrir ese correo dudoso del banco !
- Navegando en mis redes sociales desde mi celular, me apareció de repente un sms que mi información ha sido encriptada y debo pagar una recompensa para recuperarla. Todo por bajar un app que era un ransomware.
- Recibí un mensaje por sms que me había ganado un sorteo y al darle click en el enlace puse mis datos la tarjeta y ya me hicieron un cargo por 500 pesos!
- Recibí un mail después una llamada de mi banco/ netflix/cable/celular en donde dicen que mi pago de domiciliación no pasó y que si no ingreso al link y confirmo mis datos o doy una tarjeta nueva, me van a cancelar el servicio... ¿Qué hago?
- Dejé mi bluetooth abierto y en un Café ¡Me hackearon mi cuenta de Facebook/Instagram/ twitter/tiktok!

Conocer e identificar cada una de estas estrategias que usa el crimen cibernético, es fundamental para mitigar el riesgo de caer en un fraude. Las estrategias más comunes son Phishing, Pharming, Vishing y Smishing.

A estas estrategias también se les conoce como “Ingeniería social”, que es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. El principio bajo el cual se basa la ingeniería social es el que en cualquier sistema, “los usuarios son siempre el eslabón más débil”.

¿Qué significa cada una de estas estrategias y cómo podemos estar preparados para anticiparnos a caer en ellas? A continuación las explicamos.



PHISING

Este tipo de fraude engaña a sus víctimas a través del envío de correos electrónicos, mensajes SMS y hasta apps de mensajería como WhatsApp para intentar captar sus víctimas; con frecuencia emplean links que dirigen a otros sitios como instituciones bancarias o compañías de servicios, para que introduzcas números de cuenta, contraseñas, números de tarjeta, etc.

PHARMING

Otro tipo de estafa en donde el terrorista cibernético “planta” un código malicioso en una computadora o dispositivo móvil. Funciona también a través de sitios falsos que se presentan como instituciones financieras o de servicios que facturan digitalmente.

VISHING

Es la versión telefónica del Phishing. Es un poco más sofisticado y usa técnicas de “ingeniería social” para que caigas en sus redes y les proporciones tu información personal para que otros la usen con el fin de accesar y usar tus cuentas o abrir nuevas cuentas a tu nombre.

SMISHING

Es la versión de Phishing en la que se usan SMS para atrapar víctimas. Aquí, el texto del mensaje siempre contiene o una URL o un número telefónico. Usan grabaciones automatizadas, y terminan por pedir información personal para que la potencial víctima caiga en la trampa.

Estrategias para identificar y mitigar estos riesgos

PHISING

¿Cómo reconocerlo? Hazte estas preguntas:

1. ¿Conoces a quien envía el email? Si la respuesta es sí, continúa y confirma con una llamada telefónica a la institución o compañía que te lo manda antes de vaciar cualquier dato.
2. ¿El mensaje/correo contiene errores gramaticales de ortografía? Si sí, aléjate.
3. ¿Checaste el link? Pon el cursor sobre el vínculo, y al igual que en la dirección de correo electrónica, va a detectar si te lleva a algún sitio con dirección sospechosa.
4. ¿El mail te pide datos personales o sensibles? Si los pide, se trata de un phising!
5. ¿El mensaje trae archivos adjuntos que no hacen sentido al contenido del mensaje o tienen una extensión extraña? Si los tiene, no los descargues ni los abras y contacta a la empresa que los envía para estar seguro que es.

PHARMING

¿Cómo identificarlos? Asegúrate que la dirección en el browser cuenta con la “s” de “https” y checa que cuenta con el ícono de candado que confirma una navegación segura.

Si el sitio de la compañía que te lo envía luce distinto a la última vez que lo visitaste, ten cuidado y no des click a menos que estés completamente seguro de que es el sitio correcto.

VISHING

¿Cómo puedes prevenir caer en un Vishing? Te recomiendo los siguientes tips:

1. Si recibes un correo o llamada en la que te piden que marques información y no te suena bien, puede tratarse de una solicitud fraudulenta!. Busca el número telefónico del servicio al cliente de la organización en su página web o en tus estados de cuenta y llámales en lugar de al teléfono que te incluyen en el primer contacto.
2. Reenvía la solicitud al correo de servicio al cliente de la empresa que supuestamente te está solicitando la información y pregunta si el contacto es legítimo.

SMISHING

La mayoría de las veces, el smishing proviene de números tipo “5000” en lugar de presentar un número real. Esto significa que la llamada fue enviada desde un correo electrónico y no desde otro teléfono.

El consejo aquí es muy claro y directo: ¡No respondas ninguno de estos contactos!

ESCUDO DIGITAL Y +

Protección Personal

En Lockton nos gusta estar al pendiente de los riesgos que las personas puedan tener en sus actividades día con día es por ello que **creamos ESCUDO DIGITAL Y +**

Una protección personal durante un año para proteger tu identidad digital.

Con coberturas como:

Indemnización ante **robo de identidad.**

Indemnización ante **robo de bolso y sus contenidos** (dispositivos electrónicos y efectivo).

Además, contarás con las siguientes asistencias:

Resguardo de información

Soporte técnico remoto

Legal telefónica

Telemedicina

Servicio concierge

Estamos seguros que este producto te va a beneficiar a ti y a tus familiares sobre todo en esta temporada donde todos estamos en home office.

Lockton está contigo.

UNCOMMONLY INDEPENDENT

REFERENCIAS

Los datos duros fueron obtenidos de: ift.org.mx

Los datos acerca de la población fueorn obtenidos de: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2019/OtrTemEcon/ENDUTIH_2018.pdf)

