2023 CELAES
Congreso Latinoamericano
de Seguridad Bancaria

La transformación digital y los riesgos de fraude

ASOCIACION BANCARIA DE PANAMA
ABP

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Evolución de la banca y los riesgos asociados

Tecnología




Banca



Riesgos




CELAES 2023
Congreso Latinoamericano de Seguridad Bancaria

La tarea psíquica que una persona puede y debe establecer por sí mismo no es sentirse segura, sino ser capaz de tolerar la inseguridad. - Erich Fromm

La transformación digital

El acelerado proceso de ***transformación digital*** iniciado por la pandemia trajo una nueva serie de retos y oportunidades a las empresas. Las opciones de servicios y productos han permitido a los clientes continuar con su relación de consumo y, en la mayoría de los casos, aumentar su estándar de consumo.

Al continuar apoyando el gran crecimiento de la demanda generada por sus clientes, las empresas también han enfrentado otro gran desafío: el fraude digital. Según las estimaciones de Juniper Research, ***se espera que el fraude relacionado solo con los sistemas de pago*** supere los 200 mil millones de dólares entre 2021 y 2025.

El punto positivo ante esta expectativa es que la maduración de las tecnologías especializadas en la prevención y detección del fraude basadas en inteligencia artificial (IA) y aprendizaje automático (machine learning) permite a las empresas entrar en este “juego del gato y el ratón” contra los estafadores con posibilidad de ganar o, al menos, reducir sus pérdidas.

La transformación digital

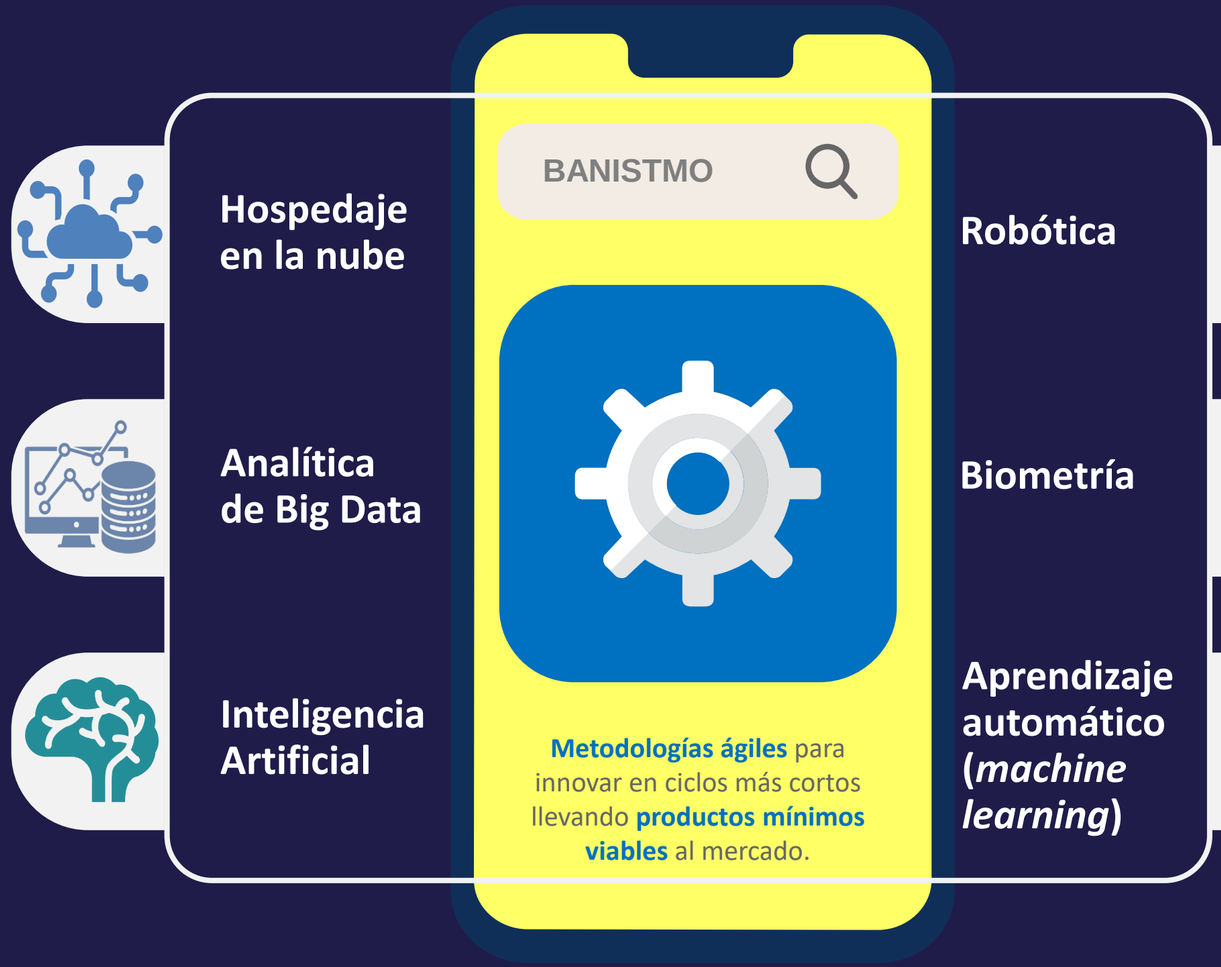
Internamente, el área responsable de la transición al mundo digital se esfuerza para que la experiencia del usuario sea fluida y alineada a su proceso de negocio, dando como resultado el crecimiento de ingresos para la organización. La proliferación de negocios en línea y aplicaciones de e-commerce ha incrementado el potencial de fraudes y el cibercrimen no ha perdido oportunidad de adaptar sus tácticas para generar ganancias en este rubro.

Debido a esto la convergencia con la ciberseguridad y la prevención de fraudes es inevitable. Muchas compañías no han puesto atención en este tópico, enfocándose únicamente en la experiencia de sus clientes.

La transformación digital no es una opción. Es **NECESARIA** para ser una entidad sólida, competitiva, diversificada y basada en el talento, la tecnología y el conocimiento. No sólo mejora la eficacia y productividad, sino que favorece la evolución y aparición de nuevos modelos de negocio que permitan el crecimiento y el desarrollo.

Uso de nuevas tecnologías

Las entidades financieras están utilizando diferentes tecnologías para mejorar sus procesos y la experiencia de sus clientes



Hospedaje en la nube

Utilizada por las entidades financieras para sus procesos o sus canales digitales

Analítica de Big Data

Necesaria para conocer mejor a los clientes y sus patrones de comportamiento

Inteligencia Artificial

La IA es vital para los sistemas antifraude, servicio al cliente con chatbots y reconocimiento de texto en documentos, etc.

Robótica

Automatización de procesos, que permite aprovechar el talento humano en tareas que aportan mayor valor

Biometría

Biometría para la identificación del cliente en la vinculación y reducción del fraude

Aprendizaje automático (*machine learning*)

Usado para aprender de patrones y poder mejorar procesos e interacciones con los usuarios

Metodologías ágiles para innovar en ciclos más cortos llevando **productos mínimos viables** al mercado.

Sin duda un proceso evolutivo, necesario y beneficioso especialmente para el comercio electrónico

Personalización de los servicios financieros

Enfoque en el cliente

Objetivo o enfoque en brindar la mejor experiencia de usuario.

Automatización

Los procesos automatizados facilitan el uso de las plataformas y herramientas

Modelos operativos de bajo costo

Plataformas digitales que permiten los servicios tecnológicos a demanda, que resultan en soluciones costo-eficiente y escalables

Uso de data y analíticas

Capacidades tecnológicas y analíticas para procesar grandes cantidades de datos.

Transacciones en tiempo real

Tecnologías que permite realizar las transacciones en tiempo real

Tecnologías habilitantes

- Cloud computing
- Artificial Intelligence and Machine Learning
- Big Data and Analytics
- Internet of Things

Las nuevas tecnologías habilitan automatización de los procesos, la inteligencia de los datos y dan soluciones personalizadas para los usuarios.

2023 CELAES
Congreso Latinoamericano de Seguridad Bancaria

Impacto del cibercrimen

Impacto del cibercrimen

90% de los ataques llegan por correo electrónico

91% de ataques son por Phishing

48% por adjuntos maliciosos en email: **OFFICE**

12% crecimiento Ransomware

1 de cada **10** URL es maliciosa

56% ataques Web

Ataques dirigidos a teletrabajadores

Incremento de vulnerabilidades en proveedores y terceros conectados a la organización

Dispositivos, redes e información usadas durante el trabajo remoto son vulnerables a ataques cibernéticos

Incremento en ataques cibernéticos y dominios registrados

Aumento de correos de Phishing, enfocados a extraer credenciales de O365 e inyectar malware

Incremento en aplicaciones y software malicioso con contenido ransomware (beneficios, alias de apps)

CELAES 2023
Congreso Latinoamericano de Seguridad Bancaria

La seguridad no es cara, es inestimable. - Jerry Smith

Principales vectores de ataque

Ingenieria Social

Sim Swapping

Fraude

Phishing
Vishing
Smishing
Quishing

DNS Spoofing / Hijacking

Suplantación de identidad

Ingenieria social

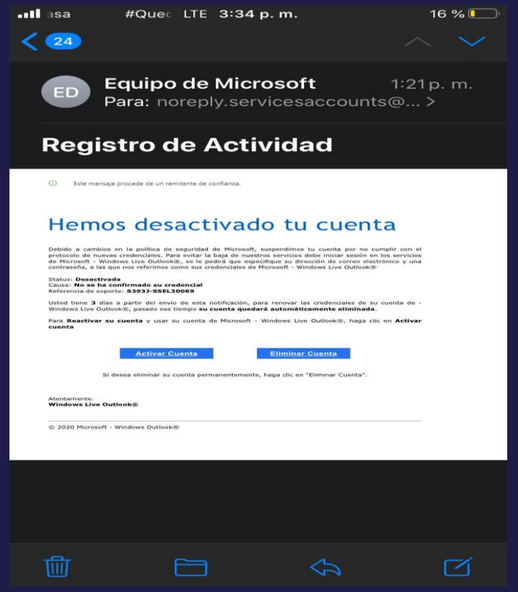
En el mundo de la tecnología y la informática **la seguridad de la información es crucial**, tanto para usuarios como para empresas. Por lo que protegerla e implementar medidas contra los hackers y sus técnicas de ingeniera social se convierte en una prioridad. Pero, **¿qué es la ingeniería social?** Se trata de un conjunto de prácticas con las que los cibercriminales buscan, generando contextos de confianza, que los usuarios entreguen datos confidenciales o faciliten información relevante para robarles.

¿Qué son las técnicas de ingeniería social?

Son las técnicas usadas por los ciberdelincuentes que se basan en la **generación de confianza** por medio del lenguaje amable, empático o atractivo. Estas llevan a que la víctima se sienta con la tranquilidad para dar continuidad a un proceso determinado.

Tanto las técnicas para personas como para empresas y organizaciones necesitan de la **cooperación de la víctima** sin que esta percate el peligro.

Phishing



De: "AVISO BANCOLOMBIA BLOQUEO ." <miryamcortes3@outlook.com>
Fecha: 10 de febrero de 2023, 7:07:45 p. m. GMT-5
Para: yuky1945@hotmail.com
Asunto: Restablecer acceso a cuenta

Banco General

Aviso Importante:yuky1945@hotmail.com

Esta Es Una Notificación Electrónica Para Informar Que Su Banca En Línea Ha Sido Suspendida

Debido A Que Debes Registrar y Validar Sus Datos Frecuentemente Restablecer Al Acceso Te

Llevará Unos Minutos Muchas Gracias Por Su Atención Banco General.

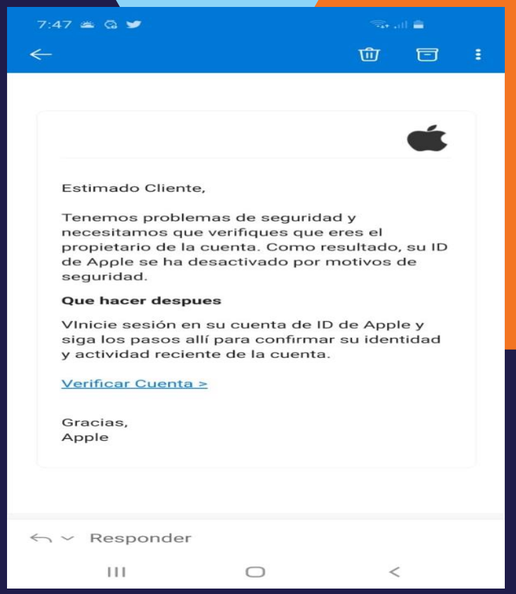
Es Importante Que Registres Sus Datos Solicitamos Para Que Nuestro Sistema Valide Su Información En Caso Contrario No Podrá Recibir Ni Realizar Ningún Tipo De Movimientos En Su Banca Online.

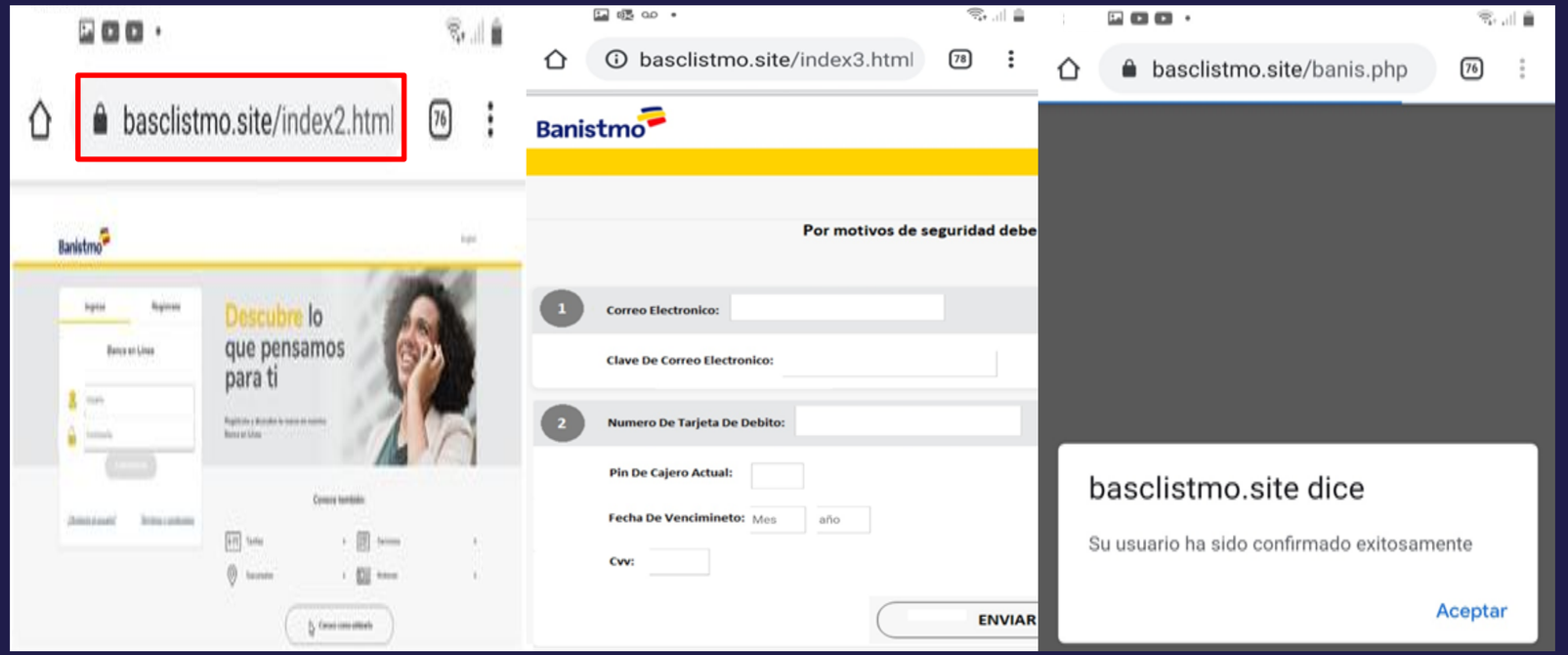
Restablecer Acceso

De acuerdo con la ley N°13, del 27 de abril del 2015 de prevención de bloqueo de capitales.

Gracias por utilizar nuestros servicios.

Banco general de Panamá.





2023 CELAES
Congreso Latinoamericano de Seguridad Bancaria

Smishing / Sim swapping / Qishing

SMISHING.- Es un tipo de ataque de phishing que **funciona por medio de mensajes de texto o SMS**. Normalmente, estos ataques piden a la víctima que realice alguna acción inmediata a través de vínculos maliciosos en los que hacen clic o dan números de teléfono para llamar.

El SIM SWAPPING.- Es un tipo de fraude que permite a los criminales robar tu identidad mediante el secuestro del número de teléfono al obtener un duplicado de tu tarjeta SIM.

QHISHING.- También conocido como phishing de códigos QR, consiste en engañar a alguien para que escanee un código QR mediante un teléfono móvil . Luego, el código QR lleva al usuario a un sitio web fraudulento que podría descargar malware o solicitar información confidencial.

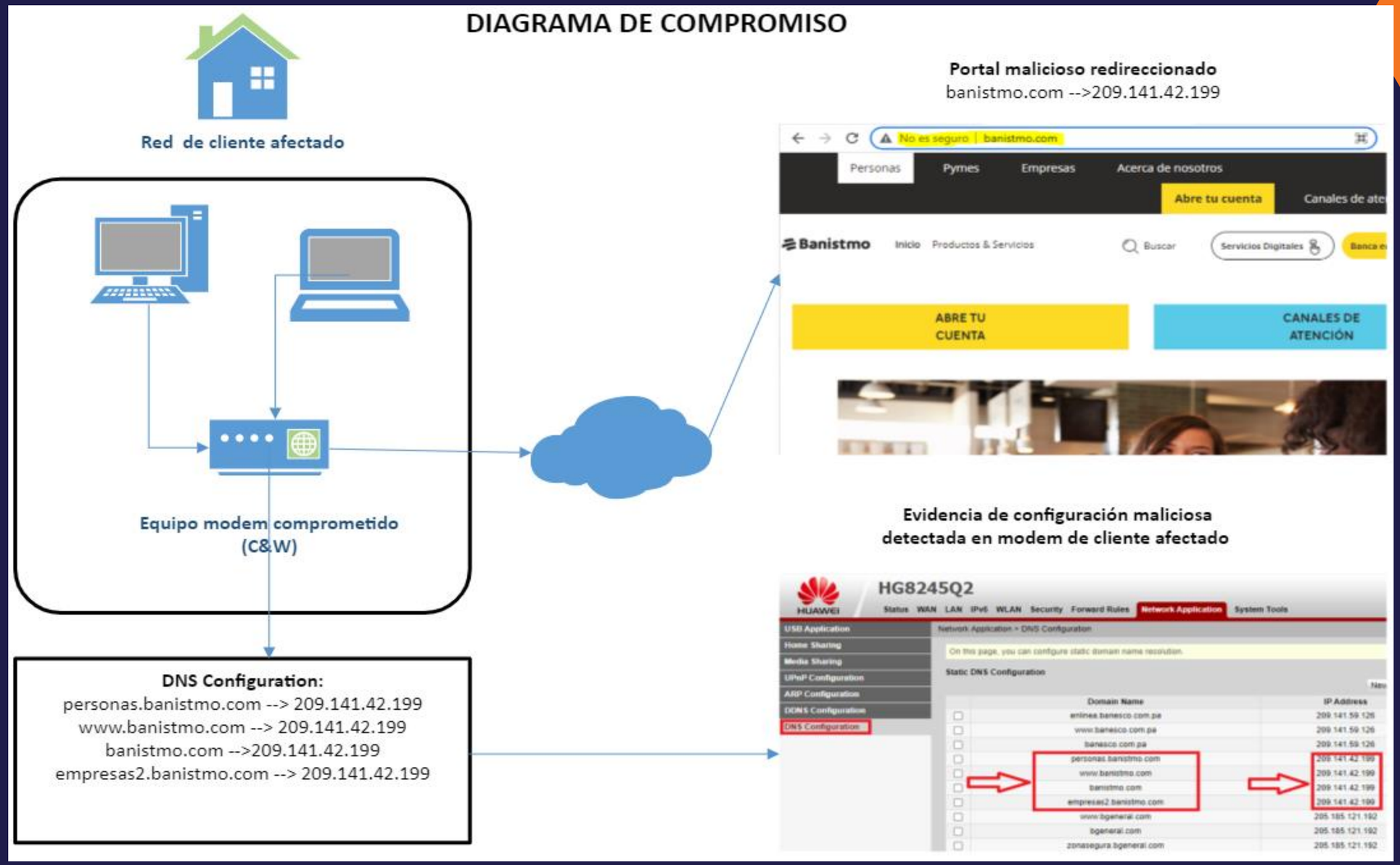
Vishing

También conocido como **phishing por voz**, es un tipo más actualizado de ataque de phishing. Esta técnica consiste en la **suplantación de un número de teléfono** para que parezca legítimo. Así los atacantes se hacen pasar por técnicos, compañeros de trabajo, personal de informática, e inclusive, familiares o amigos.

Seguramente, has recibido llamadas de un sobrino, primo o el nieto de un amigo que fue encarcelado por la policía y debe pagar una cuantiosa suma de dinero para que salga de ese problema.

Desafortunadamente, por las historias y discursos bien construidos, y con ayuda de un lenguaje de confianza, muchas personas son víctimas de este ataque. Compartiendo no solo sus datos personales o su cuenta bancaria una única vez, sino que pueden llegar a ser víctimas por un largo periodo de tiempo.

Hijacking / DNS spoofing



CELAES 2023
Congreso Latinoamericano
de Seguridad Bancaria

MUCHAS GRACIAS!!

JAIME BERRY CORTES
Director de Seguridad Corporativa
jaime.x.berry@banistmo.com

CELAES 2023
Congreso Latinoamericano
de Seguridad Bancaria