Promipyme

"PROTEGE TU NEGOCIO Y TUS FINANZAS:

PREVENIR, DETECTAR Y ACTUAR FRENTE A FRAUDES"

¿Qué es la suplantación de identidad y cómo afecta a las PYMES?

La suplantación de identidad ocurre cuando una persona o entidad se hace pasar por otra, utilizando su identidad personal o corporativa de manera fraudulenta.

En el ámbito de las PYMES, esto puede suceder de diversas formas: a través del robo de identidad en credenciales de acceso a sistemas digitales, la creación de documentos falsificados que representan a la empresa o la imitación de comunicaciones oficiales, como correos electrónicos, con el fin de engañar a empleados o clientes.

El fortalecimiento de la identidad corporativa ayuda a minimizar estos riesgos. Proteger la identidad empresarial es esencial para evitar ser víctima de fraude de identidad.

SUPLANTACIÓN DE IDENTIDAD EN LA ERA DIGITAL

La era digital ha traído consigo innumerables beneficios para las PYMES, pero también ha facilitado el aumento de la suplantación de identidad. Los ciberdelincuentes han desarrollado técnicas avanzadas para apropiarse de la identidad de empresas y usuarios, desde el uso de programa malicioso hasta ataques de phishing altamente sofisticados. La protección de la identidad en línea es más importante que nunca, ya que una sola brecha de seguridad puede tener consecuencias devastadoras para la identidad de una PYME.

Las consecuencias de la suplantación de identidad son múltiples y pueden ser devastadoras para una PYME. Los efectos negativos incluyen:

Pérdidas financieras

El fraude generado por la suplantación de identidad puede generar grandes pérdidas económicas para la empresa.

Daño a la reputación

La confianza en la identidad de la marca puede verse afectada si los clientes y proveedores consideran que la empresa no protege adecuadamente su identidad.

Pérdida de clientes

La inseguridad en los procesos de identidad puede llevar a que los clientes decidan cambiar de proveedor o servicio

Riesgos legales

La empresa podría enfrentar problemas legales si se realizan fraudes a su nombre por falta de control en la identidad.

Pérdidas financieras

El fraude generado por la suplantación de identidad puede generar grandes pérdidas económicas para la empresa.

Daño a la reputación

La confianza en la identidad de la marca puede verse afectada si los clientes y proveedores consideran que la empresa no protege adecuadamente su identidad.

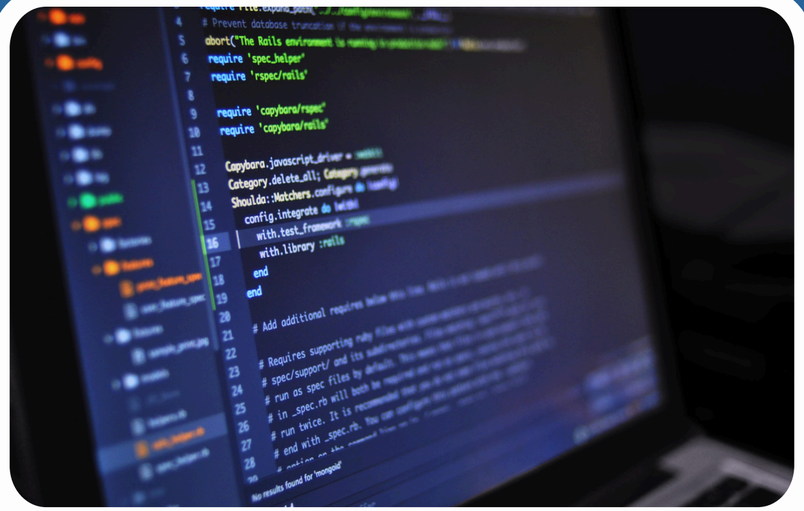
Pérdida de clientes

La inseguridad en los procesos de identidad puede llevar a que los clientes decidan cambiar de proveedor o servicio

Tipos de Amenazas Cibernéticas

El “phishing” “vishing” y “smishing” son algunos los fraudes electrónicos que utilizan los ciberdelicuentespara robar datos privados

PHISHING



VISHING

SMISHING

¿QUÉ ES EL EL PHISHING Y COMO PROTEGERTE?

Probablemente sea el método más utilizado por los ciberdelincuentes. Consiste en el envío de correos electrónicos fraudulentos que dirigen a los clientes a páginas 'web' falsas que aparentan ser de la entidad bancaria. Esta modalidad también puede presentarse en Facebook con ‘fan page’ falsas que postean contenido fraudulento y solicitan información confidencial de los usuarios.

Cómo protegerte de los ciberdelincuentes y mantener segura tu información.

Consejos para Protegerte del Phishing:

01

Desconfía de correos extraños: siempre verifica la legitimidad de los remitentes antes de hacer clic en enlaces o descargar archivos adjuntos. Presta atención a errores ortográficos o gramaticales, ya que suelen ser señales de phishing.

02

Piensa antes de compartir información: nunca reveles información confidencial, como contraseñas o datos financieros, a través de correos electrónicos no solicitados o enlaces sospechosos.

03

Activa la autenticación de dos factores (2FA): habilita la autenticación en dos pasos para añadir una capa extra de seguridad. Esto exige una segunda forma de verificación, como un código enviado a tu teléfono móvil, además de tu contraseña.

Cómo protegerte de los ciberdelincuentes y mantener segura tu información.

Consejos para Protegerte del Phishing:

04

Mantén tus dispositivos actualizados: asegúrate de que los sistemas operativos, navegadores y aplicaciones estén actualizados con los últimos parches de seguridad para protegerte de vulnerabilidades.

05

Usa software de seguridad: instala y actualiza regularmente antivirus y programas de seguridad en todos tus dispositivos para prevenir amenazas.

06

Capacita a tu equipo: si trabajas en un entorno laboral, asegúrate de que todos tus compañeros estén informados y preparados para identificar y evitar ataques de phishing.

¿QUÉ ES EL EL VISHING Y CÓMO RECONOCERLO?

El Vishing es un tipo de estafa que se realiza a través de llamadas telefónicas con el objetivo de obtener los datos personales o bancarios de una persona. Los ciberdelincuentes suplantan la identidad de un tercero (banco, empresa o persona) con la finalidad de conseguir que la víctima proporcione información privada o sensible, que pueda servirle de utilidad al defraudador para cometer ciberdelitos. Generalmente, el ciberdelincuente le informa a su víctima sobre “posibles” cargos que se están realizando a alguna de sus cuentas bancarias.

PERO ¿QUÉ ES EXACTAMENTE EL “VISHING” Y CÓMO PODEMOS IDENTIFICARLO? ¿CÓMO SALVAGUARDAR SU INFORMACIÓN SENSIBLE?

Es una combinación de voz y “phishing” (suplantación de identidad), que explota la confianza depositada en la comunicación humana.
“El criminal se hace pasar por empleado del banco, de un servicio técnico o incluso de la policía. Su objetivo es generar urgencia, con frases como ‘hemos detectado un retiro sospechoso’, para que la víctima entregue claves, números de tarjeta o confirme transferencias”.

¿QUÉ HACER ANTE LA DUDA?

Ante cualquier sospecha, lo primero debe ser colgar inmediatamente y volver a marcar al número oficial del banco, que se encuentra en la tarjeta, el sitio web o la aplicación móvil. Nunca utilizar el número que proporcione el interlocutor ni el que aparece en la llamada o el SMS.

Ninguna institución financiera solicitará contraseñas, claves de acceso, códigos de verificación, número completo de tarjeta, CVV, fecha de expiración o confirmación de transferencias no iniciadas. “Si alguien solicita alguno de estos datos, cuelgue: es un intento de fraude”.

LA PREVENCIÓN ES LA PIEDRA ANGULAR DE LA SEGURIDAD FINANCIERA. CADA CLIENTE DEBE RECORDAR QUE SU INFORMACIÓN BANCARIA ES TAN VALIOSA COMO EL EFECTIVO Y NO DEBE SER COMPARTIDA EN NINGUNA CIRCUNSTANCIA.

- Nunca revelar datos bancarios por teléfono, correo electrónico o redes sociales, incluso si la persona parece ser del banco.
- Verificar el remitente, es decir, antes de abrir un enlace o descargar un archivo, comprobar la dirección de correo.
- En caso de llamadas, solicitar un número de referencia y colgar para validar directamente con la entidad.
- Activar alertas transaccionales. Agrega que las notificaciones en tiempo real permiten detectar movimientos no autorizados y reaccionar a tiempo.
- Usar contraseñas robustas y únicas al combinar letras, números y símbolos y cambiarlas periódicamente. Asimismo, invita a evitar redes wifi públicas.

Y SI YA DI MIS DATOS, ¿QUÉ?

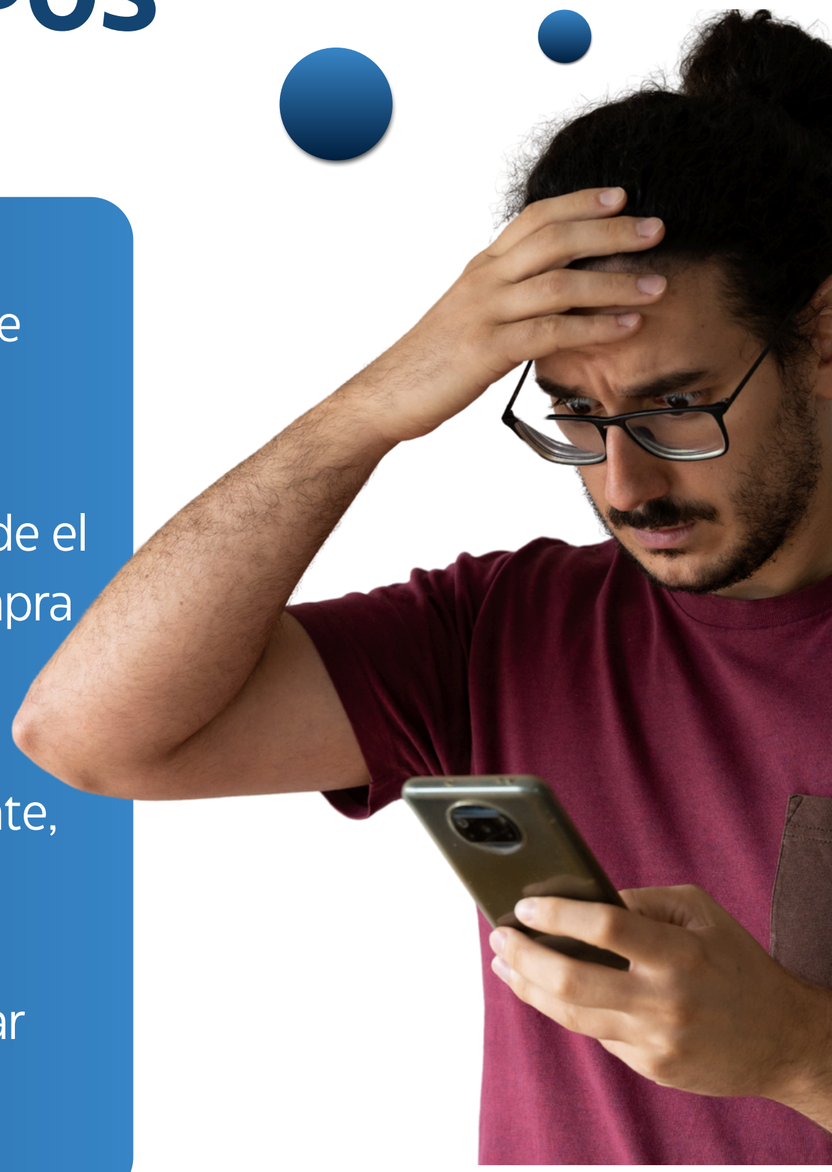
Si ya ha proporcionado información, el tiempo es crucial. El primer paso es llamar de inmediato al banco para bloquear cuentas o tarjetas comprometidas. Segundo, cambiar contraseñas de banca en línea y correo electrónico.

Tercero, presentar su denuncia ante la Procuraduría Especializada contra Crímenes y Delitos de Alta Tecnología (Pedatec). “La regla de oro es desconfiar de todo mensaje que solicite acciones inmediatas o datos sensibles. No hacer clic en enlaces dudosos y reportar al banco”.

¿QUÉ ES EL EL SMISHING Y LOS TIPOS DE ATAQUES?

Así como las llamadas telefónicas son una vía para tratar de engañar a los clientes, también lo son los mensajes de texto o mensajes por WhatsApp y de ahí deriva la modalidad conocida como “**smishing”**.

Esta amenaza se produce cuando el cliente recibe un mensaje de texto, donde el emisor se hace pasar por el banco, y le informan que se ha realizado una compra sospechosa con su tarjeta de crédito. A su vez, el texto solicita que se comunique con la banca por teléfono de la entidad financiera y le brinda un número falso. El cliente devuelve la llamada y es ahí cuando el ciberdelincuente, haciéndose pasar por el banco, solicita información confidencial para supuestamente cancelar la compra. En una variante de esta modalidad el mensaje también podría incluir un enlace a una 'web' fraudulenta para solicitar información sensible.



Tipos de Ataques:

Al igual que ocurre con la creciente sofisticación de los ataques de phishing convencionales, los mecanismos de smishing adoptan formas muy elaboradas. Entre los tipos más comunes de smishing están:

- **Estafas de verificación de cuenta:** En este tipo de ataque, la víctima recibe un mensaje de texto que dice proceder de una empresa o proveedor de servicios de confianza, como un banco o un transportista. El mensaje suele advertir a los usuarios sobre actividades no autorizadas o les pide que verifiquen los datos de la cuenta. Cuando los usuarios hacen clic en el enlace proporcionado, son dirigidos a una página de inicio de sesión falsa, donde se les pueden robar sus credenciales.

- **Estafas de soporte técnico:** Los usuarios reciben un mensaje advirtiéndoles de un problema con su dispositivo o cuenta con la petición de que se pongan en contacto con un número de asistencia técnica. Llamar a este número puede dar lugar a cargos, o el “técnico” puede solicitar el acceso remoto al dispositivo, lo que conduce a un posible robo de datos.

Tipos de Ataques:

- **Alertas de fraude bancario:** Estos mensajes parecen proceder del banco de la víctima, advirtiendo sobre transacciones no autorizadas o actividades sospechosas. A continuación, se pide al usuario que haga clic en un enlace para verificar sus transacciones o que llame a un número, ambos controlados por el atacante.

- **Estafas fiscales:** Cerca de la temporada de pago de impuestos, muchas personas reciben mensajes que dicen ser de agencias tributarias. Estos mensajes suelen prometer devoluciones de impuestos o amenazar con sanciones por impuestos supuestamente impagados, instando al destinatario a facilitar datos personales o financieros.

- **Descargas de aplicaciones malintencionadas:** Los usuarios reciben un mensaje promocionando una aplicación útil o entretenida. Al hacer clic en el enlace de descarga, se instala software malintencionado en el dispositivo del usuario.

Smishing vs. phishing vs. vishing

Comprender las diferencias entre smishing, phishing y vishing es vital para la concienciación y la protección frente a una amplia gama de ciberamenazas. Cada término se refiere a tácticas engañosas que los ciberdelincuentes utilizan para engañar a las personas para que divulguen información delicada. Sin embargo, cada enfoque utiliza diferentes medios y métodos para llevar a cabo el ataque.

Aspecto	Smishing	Phishing	Vishing
Medio	Mensajes de texto (SMS)	Correo electrónico, sitios web falsos, redes sociales	Llamadas telefónicas (tradicionales o VoIP)
Método	Mensajes de texto engañosos con enlaces maliciosos o solicitudes de información	Correos electrónicos fraudulentos que aparentan ser legítimos	Llamadas en las que se hacen pasar por entidades confiables
Objetivo	Obtener datos personales o financieros mediante engaño	Robar credenciales, datos personales o financieros	Obtener información confidencial directamente por voz
Ejemplo típico	SMS que alerta de actividad bancaria sospechosa con un enlace falso	Email de una tienda en línea solicitando restablecer contraseña	Llamada de supuesto agente del gobierno exigiendo pagos

EL VALOR DE LOS DATOS PERSONALES Y LA AMENAZA CRECIENTE DE LOS CIBERATAQUES.

Hoy en día, los datos personales se han convertido en el oro del siglo XXI para los ciberdelincuentes. Información como nombres, correos, números de cédula, contraseñas, historiales financieros o incluso simples direcciones de correo pueden ser utilizada para robar identidades, vaciar cuentas, extorsionar o venderse en mercados negros digitales por sumas considerables. Cada fragmento de información es una pieza de un rompecabezas que, al juntarse, permite a los atacantes suplantar a una persona o infiltrarse en empresas enteras.

Para los criminales, estos datos no son simples registros: son activos con un valor económico directo, mientras que para las víctimas representan pérdidas financieras, daños a la reputación y, en muchos casos, una vulneración profunda de su privacidad y seguridad.

LOS CIBERDELINCUENTES EMPLEAN LOS DATOS PERSONALES ROBADOS EN DIVERSAS ACTIVIDADES DELICTIVAS, TALES COMO:

VENTA EN LA DARK WEB

Información como números de tarjetas de crédito, credenciales de acceso, documentos de identidad y registros médicos son vendidos a terceros en mercados clandestinos. donde otros delincuentes pueden adquirirlos para su uso.

SUPLANTACIÓN DE IDENTIDAD

Los datos personales se emplean para realizar fraudes financieros, como abrir cuentas bancarias, obtener créditos o realizar compras utilizando la identidad de otra persona.

EXTORSIÓN

En muchos casos, los atacantes utilizan los datos robados para extorsionar a las víctimas, amenazando con publicar la información sensible si no se paga un rescate.

CREACIÓN DE PERFILES FALSOS

Configuran cuentas en plataformas en línea para realizar fraudes bajo una identidad ficticia.

“La creciente sofisticación de los ciberataques nos recuerda que la protección de los datos personales debe ser una prioridad constante. Adoptar medidas de ciberseguridad robustas no solo protege la información, sino también la tranquilidad de las personas y las organizaciones”.

Esta realidad pone de manifiesto el alto valor que los ciberdelincuentes atribuyen a los datos personales, los cuales, dependiendo de su tipo, pueden alcanzar precios de hasta $100 en la web oscura. Información como contraseñas, documentos médicos y credenciales de acceso son convertidos en mercancías lucrativas en mercados clandestinos.

Frente a este panorama, la protección de los datos personales no es solo una necesidad individual, sino una responsabilidad compartida entre individuos, empresas y gobiernos, que deben colaborar para fortalecer las defensas contra estas amenazas.

IMPORTANT

- **Confidencialidad**. Nunca comparta sus credenciales bancarias (usuario, contraseña, código de verificación) ni por teléfono, correo o mensajes. Ningún banco las solicita de esa forma.
- **Verificación**. Verifique con su banco que tenga activados todos los controles de seguridad disponibles, como alertas de transacciones, límites de transferencias y notificaciones.
- **Precaución**. No haga clic en enlaces sospechosos que lleguen por correo, SMS o redes sociales, aunque parezcan oficiales. Verifica siempre desde el sitio web o “app” oficial.
- **Desconfianza**. Confirme la identidad de quien le contacta. Si alguien dice llamarle del banco y usted no está seguro, cuelgue y vuelva a llamar usted al número oficial. Recuerde, el banco jamás le pedirá esos datos.
- **Seguimiento**. Monitoree constantemente sus cuentas. Revise sus movimientos con regularidad para detectar cualquier actividad inusual y esté pendiente de las notificaciones al instante.
- **Denuncia**. Reporte cualquier intento de estafa. Si recibe un mensaje o llamada sospechosa, informe de inmediato al banco o a la autoridad competente, incluyendo la Policía Nacional.

Promipyme

REFLEXIÓN:

En el mundo digital, no todo lo que parece confiable lo es. Hoy, más que nunca, la desconfianza inteligente es una forma de defensa. Estar informados y atentos no es paranoia, es prevención. Cada clic, cada respuesta, cada llamada atendida puede marcar la diferencia entre la seguridad y la vulnerabilidad.

Promipyme

Consejo Nacional de Promoción y Apoyo a la Micro,
Pequeña y Mediana Empresa

Accede a nuestro Grupo de Whastapp

Inscribete en nuestra Aula Virtual

809-473-6089
Ext. 265 / 330

promipyme.gob.do

@promipymerd