SUPLANTACIÓN DE IDENTIDAD, CORREOS ELECTRÓNICOS, Y ESTAFAS

Cada vez, más congregaciones y ministerios están siendo blanco de estafadores, y ataques de phishing. Estos correos electrónicos, o mensajes de texto a menudo fingen que son un(a) Pastor(a) u Obispo(a), y solicitan una conversación privada, o la necesidad de un favor, o de comprar tarjetas de regalo..

Estos ataques son una estafa de “Phishing” o “Spoofing”. Esto significa que la cuenta de correo electrónico, o el número de teléfono probablemente NO han sido hackeados. Los atacantes están utilizando direcciones de correos electrónicos, números de teléfono alternativos, y contactos encontrados a través de software de Inteligencia Artificial.

Este tipo de ataque a menudo se llama “CEO Phishing o Business Email Compromise”. En 2019, el FBI informó que se trata de una estafa de $26 mil millones de dólares.

¿CÓMO OPERAN?



Los atacantes eligen un objetivo o víctima, (sea una congregación, ministerio o sínodo) y hacen una búsqueda de nombres, y direcciones de correo electrónico de los líderes.



Los atacantes crean direcciones de correo electrónico con un nombre, o dominio convincente para que se parezca al del líder real.



Luego usan software para encontrar direcciones de correo electrónico, o números de teléfono asociados con su objetivo o víctima.



Envían correos electrónicos o mensajes de texto a quienes enviaron el mensaje, pretendiendo ser un Pastor(a) u Obispo(a), para solicitar dinero e información.

¿CÓMO EVITAR O DETENER LAS ESTAFAS?

1. Compruebe la dirección de correo electrónico, o el número de teléfono del cual se envía el mensaje: Los programas de correo electrónico modernos, a menudo sólo muestran el nombre la persona como predeterminado, no específicamente el correo electrónico. Los atacantes utilizan esto como ventaja a su favor, y crean correos con un nombre real, pero usan una dirección de correo electrónico falsa. A menudo usan cuentas de Gmail o Yahoo. Los estafadores de mensajes de texto, usarán “códigos de área” que se encuentran en el área donde usted reside, pretendiendo ser un nuevo número de teléfono.

2. Busque signos de alerta en el tono, y la gramática del correo electrónico, o texto: Los atacantes querrán crear un sentido de urgencia, aprovecharse de su deseo de ayudar. A menudo

afirman que el Obispo(a) o Pastor(a) necesita algo, y está en una reunión. “O necesita tener urgentemente una conversación privada.” Estos correos electrónicos a menudo contienen faltas de ortografía, puntuación extraña, o “mala” gramática. Lea cuidadosamente los mensajes con dichas solicitudes.

3. Pregúntale a alguien: Pídale a otra persona que lea el mensaje para que usted vea si nota algo extraño. Llame o envíe un correo electrónico a la iglesia, o a la oficina del sínodo para verificar cuál es realmente la dirección de correo electrónico, o el número de teléfono de la persona.

4. No compre tarjetas de regalo, ni proporcione información: Estas estafas a menudo solicitan la compra de tarjetas de regalo, o quieren que proporcione más información (para más estafas). Nunca comparta información, ni realice compras a partir de una solicitud de texto, o correo electrónico sin primero verificar la información.

5. Repórtelo: Repórtelo a la persona, sínodo o líder. Es muy probable que, si usted recibió un correo electrónico, o mensaje de texto fraudulento, alguien más también lo recibió. También, informarlo a la FCC, (Comisión Federal de Comunicaciones). Sí usted es víctima de una estafa, repórtelo a la policía local.