Aumento de estafas a empresas por medio de correos electrónicos

AMERANT

Todos sabemos que la tecnología facilita nuestras vidas en muchos aspectos. Pero desafortunadamente, el mundo cibernético también facilita el camino a los *hackers* y a los ataques fraudulentos. En Amerant Bank nos aseguramos de que nuestros clientes estén protegidos y seguros. Su información es privada, y queremos que continúe siendo así.

Trucos de los Ataques Cibernéticos

Una de las mayores amenazas cibernéticas hoy día son los ataques conocidos como "Estafas a empresas por medio de correos electrónicos" o más conocido en inglés como *Business Email Compromise (BEC)*. Se trata de un sofisticado tipo de fraude a empresas. Los ataques son dirigidos a empleados con acceso a las finanzas de la empresa, enviándoles correos electrónicos en los que los estafadores se hacen pasar por altos ejecutivos o proveedores, y tratan de convencerlos de efectuar transferencias a cuentas bancarias que parecen legítimas.

Originalmente conocidas como "Fraudes del CEO", las estafas *BEC* han evolucionado al comprometer correos electrónicos personales, correos de proveedores, cuentas de correo electrónico de bufetes de abogados, solicitudes de información para planillas W-2, y el ataque al sector de bienes raíces. Estos ataques sofisticados están en aumento, y por eso le presentamos algunos consejos y datos de ayuda para mantener a esos *hackers* alejados de su empresa.

Buenas prácticas para mantener alejados a los estafadores

1. No confíe únicamente en las instrucciones de pago indicadas en un correo electrónico. Confirme solicitudes de pago a través de verificación telefónica, usando números previamente registrados.
2. Conozca los hábitos de sus clientes y proveedores, incluyendo motivos, detalles y montos de pago.
3. Sospeche de solicitudes que requieran discreción o actuar de inmediato.
4. Piense bien antes de hacer clic en correos electrónicos o enlaces de origen desconocido, así como en comunicaciones no solicitadas.
5. Verifique cambios en los pagos con el receptor destinado.
6. Revise minuciosamente solicitudes por correo electrónico que presenten detalles fuera de lo común.
7. Considere procedimientos de seguridad que requieran doble verificación para pagos por transferencia vía *wire*.
8. Cree reglas de sistema tales como:
   - Alertas sobre correos electrónicos con extensiones similares a las de la empresa
   - Alertas sobre comunicaciones vía correo electrónico en las que la dirección para responder es diferente a la dirección de la que proviene el correo
   - Diferenciar los correos electrónicos internos de los externos

Esperamos que estos consejos hayan sido de ayuda. En Amerant Bank, estamos para asistirle si tiene alguna pregunta.
Si cree que ha sido víctima de fraude, contáctenos a través de nuestro centro de atención al cliente a la brevedad posible.