No caiga en las estafas BEC generadas por la inteligencia artificial (IA):

Cómo detectarlas y detenerlas

BEC por sus siglas en ingles (Business Email Compromise) es un tipo de ataque de phishing dirigido a empresas e individuos que realizan transferencias bancarias u otras transacciones financieras. Los ciberdelincuentes utilizan técnicas de phishing, suplantación de identidad o piratería para hacerse pasar por una persona o entidad de confianza, como un colega, un proveedor, un cliente o un banco con el fin engañarlo para que les envíe dinero o información confidencial.

Las estafas BEC existen desde hace años pero se están volviendo más sofisticadas y frecuentes, especialmente desde la pandemia de COVID-19 cuando muchas personas empezaron a trabajar de forma remota y dependíanmás de la comunicación por correo electrónico. Según el FBI (*Oficina Federal de Investigación de los Estados Unidos de America*, por sus siglas en ingles), las estafas BEC han costado a las empresas e individuos más de 43 mil millones de dólares en todo el mundo desde 2016, lo que las convierte en una de las formas de ataque más costosas y lucrativas utilizadas por los ciberdelincuentes.

Recientemente un número creciente de ataques estilo BEC han utilizado herramientas de inteligencia artificial (IA) para hacer que sus correos electrónicos sean más convincentes y personalizados. Las herramientas de inteligencia artificial, como ChatGPT de OpenAI, Bard de Google y Bing con tecnología de inteligencia artificial de Microsoft se basan en grandes modelos de lenguaje que pueden generar texto realista y relevante basado en una entrada o contexto determinado. Estas herramientas también pueden imitar el estilo de escritura, el tono y la firma de la persona a la que se hacen pasar lo que dificulta que usted detecte la diferencia.

Por ejemplo, una estafa BEC basada en IA puede verse así:

Hola [Nombre],

Espero que este correo electronico te encuentre muy bien. Te escribo desde mi correo personal porque tengo algunos problemas con mi cuenta del trabajo.

Necesito que me hagas un favor y proceses un pago urgente para un nuevo proveedor con el que estamos trabajando. Han entregado los productos que pedimos, pero necesitan el pago antes del final del día para evitar cargos por pagos atrasados.

El monto es $50,000 y los detalles de la cuenta son los siguientes:

Nombre del banco: ABC Bank Número de cuenta: 123456789 Número de ruta: 987654321 Código Swift: ABCD1234 Nombre del beneficiario: Compañía XYZ

Por favor confirme el pago lo antes posible y envíeme el recibo. Este es un asunto confidencial, así que no lo hable con nadie más.

Gracias por su cooperación y comprensión.

Atentamente,

[Nombre del director ejecutivo] [título del director ejecutivo] [firma del director ejecutivo]

Como puede ver, este correo electrónico parece muy auténtico y profesional e incluso puede coincidir con los correos electrónicos anteriores que recibió de su director o ejecutivo, sin embargo es un correo electrónico falso generado por una herramienta de inteligencia artificial y los detalles de la cuenta pertenecen a un ciberdelincuente que intenta robar su dinero.

¿Cómo puede protegerse ud mismo y a su empresa de las estafas BEC basadas en IA?

A continuación se ofrecen algunos consejos que puede seguir:

- Verifique la identidad y autenticidad del remitente antes de responder a cualquier solicitud de correo electrónico. Puede hacerlo comprobando la dirección de correo electrónico, la firma, el tono y el contenido del correo electrónico. Si nota discrepancias o señales de alerta como errores ortográficos, solicitudes urgentes o inusuales o cambios en los detalles de la cuenta bancaria, no responda ni haga clic en ningún enlace o archivo adjunto. En su lugar comuníquese directamente con el remitente mediante un canal diferente como una llamada telefónica o un mensaje de texto para confirmar la solicitud.

- Utilice contraseñas seguras y únicas para sus cuentas de correo electrónico y otras plataformas en línea. También puede utilizar un administrador de contraseñas para generar y almacenar sus contraseñas de forma segura. Esto le ayudará a evitar que los piratas informáticos accedan a su cuenta de correo electrónico y envíen correos electrónicos fraudulentos en su nombre.

- Habilite la autenticación multifactor (MFA) para sus cuentas de correo electrónico y otras plataformas en línea. MFA agrega una capa adicional de seguridad al solicitarle que ingrese un código o un token que se envía a su teléfono u otro dispositivo además de su contraseña cuando inicia sesión. Esto lo ayudará a evitar que los piratas informáticos accedan a su cuenta de correo electrónico o cualquier plataforma en linea.

- Mantenerse actualizado con los parches de seguridad. Los sistemas operativos y las aplicaciones a menudo lanzan actualizaciones y parches de seguridad para abordar vulnerabilidades conocidas. Mantenerse al día con estas actualizaciones es crucial para protegerse de los ataques BEC. Configure las actualizaciones automáticas en todos los dispositivos y asegúrese de que su software de seguridad esté actualizado. Esto ayudará a cerrar cualquier brecha que los atacantes puedan aprovechar.

MUFG Bank México espera que este mensaje le ayude a estar más consciente y preparado para las estafas de BEC impulsadas por IA. Manténgase a salvo y vigilante.
