Julio 2021

BOLETÍN INFORMATIVO

Acerca de Chubb

Con operaciones en 54 países y territorios, Chubb ofrece seguros comerciales y personales de propiedad y accidentes, accidentes personales y seguro médico complementario, reaseguro y seguro de vida a un grupo diverso de clientes. Como empresa de suscripción, evaluamos, asumimos y gestionamos el riesgo con conocimiento y disciplina. Atendemos y pagamos nuestros reclamos de manera justa. La compañía también se define por su amplia oferta de productos y servicios, amplias capacidades de distribución, solidez financiera excepcional y operaciones locales a nivel mundial. La empresa matriz Chubb Limited cotiza en la Bolsa de Valores de Nueva York (NYSE: CB) y es un componente del índice S&P 500. Chubb mantiene oficinas ejecutivas en Zurich , Nueva York , Londres , París y otras ubicaciones, y emplea aproximadamente a 33.000 personas en todo el mundo.

“4 estafas de ciberseguridad de ingeniería social a tener en cuenta “

Las pequeñas empresas suelen ser el blanco de las estafas de ingeniería social, por lo que es importante informarse a sí mismo y a su personal sobre algunas señales de alerta clave que podrían indicar un fraude.

Aquí hay cuatro estafas comunes de ingeniería social, qué hacer cuando es un objetivo y cómo puede evitar estas estafas.

Según un informe de 2021 de PurpleSec , la gran mayoría (98%) de los ciberataques actuales involucran alguna forma de ingeniería social. Los piratas informáticos que llevan a cabo este tipo de estafas a menudo se hacen pasar por una fuente conocida y confiable para sus víctimas, como un jefe, un compañero de trabajo, un amigo, un pariente o una institución legítima como un banco o el IRS. Luego explotan esa confianza para engañar a las víctimas para que cumplan con una solicitud fraudulenta de información confidencial o dinero.

Las pequeñas empresas suelen ser el blanco de las estafas de ingeniería social, por lo que es importante informarse a sí mismo y a su personal sobre algunas señales de alerta clave que podrían indicar un fraude.

Tipos de estafas de ingeniería social

Si bien la ingeniería social se presenta en muchas formas, aquí hay cuatro categorías de estafas que los ciberdelincuentes llevan a cabo con frecuencia:

Phishing o smishing

El phishing, el tipo más común de ataque de ingeniería social, ocurre cuando un ciberdelincuente envía un correo electrónico o mensaje de texto (también llamado "smishing") que alienta a la víctima a hacer clic en un enlace o archivo adjunto e ingresar datos personales confidenciales o información financiera. Estos mensajes suelen tener cierto sentido de urgencia o incorporan una amenaza.

Un ejemplo bien conocido de phishing es cuando una persona recibe un correo electrónico de su banco que dice que hay un problema con su cuenta y que necesitará iniciar sesión para solucionarlo. Si la víctima no sabe buscar señales de fraude, puede insertar su información bancaria en un sitio web de phishing y enviarla directamente a un pirata informático.

Pretextando

El pretexto es una estafa de suplantación de identidad en la que los malos actores se hacen pasar por un individuo conocido, como un ejecutivo de la empresa. Estos delincuentes suelen pedirle a la víctima que lleve a cabo una tarea financiera relacionada con el negocio o que comparta información personal para "confirmar su identidad". Si un pirata informático obtiene acceso a los archivos de personal y las direcciones de correo electrónico de una empresa, es relativamente sencillo para él ponerse en contacto con los empleados y hacerse pasar por su jefe o director de recursos humanos y realizar esas solicitudes, que el empleado ni siquiera puede cuestionar.

Vishing

Los ataques de Vishing ocurren por teléfono y generalmente involucran a un estafador que le dice a su víctima que está "bajo investigación" o que debe pagar una multa para resolver un problema con la organización que dice representar. Según un estudio de 2020 realizado por BeenVerified , algunas de las estafas telefónicas más comunes del año pasado involucraron a delincuentes que se hicieron pasar por empresas de entrega, agencias gubernamentales como la Administración del Seguro Social y empresas de tarjetas de crédito o de cobro de deudas.

Cebo o quid pro quo

Un ataque de cebo ocurre cuando un estafador atrae a su víctima con algún tipo de oferta. Esto podría ser una promoción falsa para una tienda minorista en línea o medios gratuitos, como música o películas. Estos ataques suelen explotar la curiosidad y tienen como objetivo engañar a los usuarios para que obtengan sus credenciales de inicio de sesión.

Las 'banderas rojas' de la ingeniería social que hay que buscar

Chris Arehart, vicepresidente senior y gerente de productos de delitos, secuestros y rescates en Chubb , dijo que algunas estafas de ingeniería social, especialmente los correos electrónicos de phishing, son "virtualmente indetectables en los mensajes legítimos", lo que hace que sea fácil enamorarse de ellas. Sin embargo, señaló que hay algunas señales de advertencia clave en el contenido del mensaje o la dirección del remitente que pueden indicar un posible fraude:

- **Mensajes que crean una sensación de urgencia.**
- **Solicitudes para trabajar de forma confidencial o trabajar con una persona que se presenta en la comunicación por correo electrónico como abogado.**
- **Solicitudes para realizar tareas financieras inusuales, como transferir fondos o cambiar la información de pago de la empresa.**
- **Mensajes relacionados con la empresa enviados desde un dominio público, como un servicio de correo electrónico gratuito.**
- **Direcciones de correo electrónico incorrectamente escritas o nombres de dominio de apariencia legítima con caracteres inusuales.**
- **Errores ortográficos y gramática deficiente en todo el correo electrónico.**
- **Archivos adjuntos sospechosos que no esperabas recibir.**
- **Enlaces que apuntan a un dominio diferente o no reconocido cuando pasa el cursor sobre ellos.**

“En los últimos años, estas señales de alerta comunes han disminuido en gran medida, lo que hace que sea mucho más difícil para el destinatario detectar la legitimidad usando solo lo que ven en la pantalla”, dijo Arehart a CO.

Qué hacer si cree que se ha encontrado con una estafa de ingeniería social.

Si recibe un correo electrónico, una llamada telefónica o un mensaje de texto de apariencia sospechosa, no lo responda. Eric Breece, director de ciberseguridad de Sunrise Banks , recomendó hacerse estas preguntas:

- ¿Es esta una comunicación que normalmente recibiría de esta persona u organización?
- ¿Es esta una solicitud que la persona u organización me haría?
- Si bien puedo sentir que puedo confiar en esta persona u organización, ¿es esto algo que normalmente iniciarían?
- ¿Están pidiendo cambiar un proceso que puede parecer razonable, pero que no está sincronizado o no es normal para el individuo o la organización?

Si cree que ha sido blanco de una estafa de ingeniería social, Breece dice que es mejor ir directamente a la fuente para confirmar la solicitud. Si no se trata de una persona conocida (como un jefe o un colega) a quien pueda contactar a través de un canal diferente, vaya al sitio web oficial de la organización que el estafador dice representar y busque un número de teléfono para llamar, agregó.

Si no puede confirmar que la solicitud es legítima, informe inmediatamente el incidente a su departamento de TI y a las autoridades, especialmente si ya hizo clic en un enlace o le dio al estafador información confidencial.

CO: tiene como objetivo brindarle inspiración de los principales expertos respetados. Sin embargo, antes de tomar cualquier decisión comercial, debe consultar a un profesional que pueda asesorarlo en función de su situación individual.

FUENTE Chubb