Comunicados

Phishing creado con IA Generativa: ¿cómo protegerse?

Durante la temporada de fin de año, cada vez más usuarios están optando por los canales digitales para realizar sus compras. Si bien, tecnologías como la IA generativa están siendo aprovechadas por las empresas para mejorar la experiencia online, también están siendo usadas por ciberdelincuentes para disfrazarse de las marcas de confianza, haciéndose atractivos para que las víctimas hagan clic en un link malicioso o abran archivos adjuntos con malware.

Uno de los principales canales utilizados por los ciberatacantes para lograr este objetivo es el correo electrónico, enviando e-mails falsos (phishing) a las personas y ahora, con IA generativa, no sólo están aumentando la cantidad de e-mails, sino también su efectividad al hacerlos más convincentes según el último análisis de IBM X-Force. Ante las nuevas campañas de phishing creadas con IAG, estas son cinco recomendaciones de IBM para protegerse durante la temporada de fin de año:

- **Si algo le genera dudas, vaya directamente a la fuente.** Si se pregunta sobre la legitimidad de un correo electrónico, levante el teléfono y verifique la veracidad de la información directamente con la organización o con la persona correspondiente. Considere elegir una palabra “clave” que pueda usar con amigos cercanos y familiares para validar la legitimidad de una llamada, esto en el caso de vishing o de estafas telefónicas generadas con IA (Deep Fake).

- **Tenga los ojos bien abiertos, siempre desconfíe.** Una de las tácticas más usadas en el último año es el secuestro de conversaciones de e-mail o thread hijacking, en el que un atacante compromete la cuenta de una persona y responde a las conversaciones de correo electrónico como si fuera la víctima. Por eso, si recibe un correo electrónico inesperado, incluso si proviene de alguien confiable, no haga clic en los archivos o enlaces que contiene.

- **Analice cuidadosamente la información de cada correo.** Revise el e-mail completo del remitente. Una dirección real no debe contener errores tipográficos o letras de otros alfabetos como “r” y “ꭇ”. Si el mensaje tiene links, compruebe a dónde llevan pasando el cursor sin hacer clic. Evalúe si el tono o el idioma en el e-mail coinciden con el remitente. Si le parece fraudulento, repórtelo a quien ‘supuestamente’ lo envió poniéndose en contacto directamente.

- **Use un e-mail exclusivamente para las compras.** Hacer compras con su e-mail corporativo puede poner en riesgo a la compañía para la que trabaja, más aún si utiliza la misma contraseña para iniciar sesión en los sistemas de la empresa. Se recomienda crear una dirección de correo electrónico que pueda aprovechar únicamente para realizar compras en Internet y asegurarla con una contraseña alfanumérica larga y con autenticación multifactor.

- **Sólo use las aplicaciones o sitios web en los que confía.** Regístrese para hacer compras o recibir ofertas por e-mail solo en los lugares que conoce y tenga especial cuidado con los descuentos que recibe por parte de los 'comercios' de los que nunca ha oído hablar. Si por error ingresa a una página sospechosa, no registre ninguna información y ciérrela inmediatamente.

A medida que los canales de compra continúan digitalizándose, una buena higiene de seguridad es imprescindible. Debe ser un compromiso no solo durante la temporada de compras, sino en el día a día. Aprender constantemente sobre las ciberamenazas y entrenarse a sí mismo para formar hábitos de seguridad a lo largo del año, es el mejor mecanismo de protección que se puede tener.
