El ‘phishing’ con la IA dispara la suplantación de bancos y empresas en España

El aumento del fraude digital obliga a reforzar las comunicaciones certificadas y cifradas entre clientes y empresas

Cada vez es más difícil distinguir un correo real de uno fraudulento. La inteligencia artificial (IA) está permitiendo a los ciberdelincuentes generar mensajes que imitan con gran precisión las comunicaciones de bancos, aseguradoras o compañías energéticas, lo que está provocando un aumento del phishing y —en consecuencia— las reclamaciones relacionadas con este tipo de fraude.

Al principio los ciberdelincuentes que empleaban esta táctica de phishing eran identificados fácilmente por errores de redacción, un uso del lenguaje poco propio del remitente o solicitar al cliente tareas realmente sospechosas. Hoy, sin embargo, las herramientas de inteligencia artificial permiten generar correos y mensajes prácticamente indistinguibles de los que envían empresas legítimas, lo que aumenta significativamente la eficacia de estos ataques.

El impacto del fenómeno ya es visible en las cifras. Según datos del Ministerio del Interior, en España se registraron más de 460.000 ciberdelitos en 2024, la mayoría relacionados con estafas informáticas y fraudes digitales. El phishing continúa siendo una de las técnicas más utilizadas para obtener credenciales, datos personales o información bancaria de los usuarios.

El Instituto Nacional de Ciberseguridad (INCIBE) detecta cada año decenas de miles de incidentes relacionados con fraude online, muchos de ellos basados en la suplantación de identidad de empresas conocidas con el objetivo de generar confianza en la víctima.

La inteligencia artificial está amplificando este fenómeno. Los mensajes fraudulentos pueden generarse de forma automática, adaptarse al perfil del usuario e incluso replicar con total exactitud el tono, uso de determinadas palabras y el estilo de comunicación de una entidad concreta, lo que dificulta para el consumidor distinguir entre una comunicación legítima y un intento de fraude.

Y el phishing no es solo un problema tecnológico. Cada vez más se está convirtiendo también en un problema jurídico. Porque cuando una estafa se produce a través de una comunicación que aparenta proceder de una empresa legítima, el conflicto suele terminar en una reclamación o incluso en los tribunales. En estos casos, el debate jurídico suele centrarse en determinar si la entidad cuya identidad ha sido utilizada adoptó medidas suficientes para evitar suplantaciones u ofrecer canales de comunicación verificables con sus clientes.

En los últimos años se han multiplicado las reclamaciones relacionadas con fraudes digitales, especialmente en el ámbito bancario. Por ello los tribunales están analizando con creciente detalle el grado de diligencia exigible a las entidades para proteger a los usuarios frente a este tipo de ataques.

Aunque cada caso depende de sus circunstancias concretas, algunos pronunciamientos judiciales ya apuntan a una tendencia clara: cuando la comunicación fraudulenta resulta especialmente creíble y el usuario actúa confiando razonablemente en que interactúa con una empresa legítima, el análisis jurídico se centra en si la entidad afectada había adoptado medidas adecuadas para evitar ese tipo de suplantación o para facilitar canales de comunicación verificables.

Ante este escenario, muchas compañías están revisando cómo envían determinados mensajes a sus clientes.

No basta con enviar un correo electrónico. Cada vez es más importante que una empresa pueda demostrar que una comunicación procede realmente de ella y que su contenido no ha sido manipulado. Esto explica el creciente interés por sistemas que permiten acreditar la autenticidad de una comunicación digital, certificar su contenido y protegerlo mediante cifrado, especialmente en sectores donde la confianza es crítica, como el financiero, el asegurador o el energético.

Cuando un cliente recibe un mensaje importante de su banco o de su aseguradora, debería poder tener la certeza de que ese mensaje es auténtico y que no ha sido manipulado. Ese tipo de garantías empiezan a ser fundamentales en un entorno donde la suplantación digital es cada vez más sofisticada.

Este tipo de sistemas permiten acreditar el contenido, el envío y la recepción de una comunicación mientras el mensaje permanece protegido mediante cifrado, reduciendo así el riesgo de suplantación o manipulación.

Para las empresas, el reto es reforzar sus canales oficiales de comunicación con sistemas que permitan identificar de forma clara los mensajes auténticos y evitar que los clientes puedan ser víctimas de suplantaciones.

Fuente: Economist Jurist