¿Qué es el spear phishing?

El spear phishing es una estafa de correo electrónico o comunicaciones dirigida a personas, organizaciones o empresas específicas. Aunque su objetivo a menudo es robar datos para fines maliciosos, los cibercriminales también pueden tratar de instalar malware en la computadora de la víctima.

Funciona así: llega un correo electrónico, aparentemente de una fuente confiable, que dirige al destinatario incauto a un sitio web falso con gran cantidad de malware. A menudo, estos correos electrónicos utilizan tácticas inteligentes para captar la atención de las víctimas. Por ejemplo, el FBI advirtió de estafas de spear phishing que involucraban correos electrónicos supuestamente procedentes del Centro Nacional para Menores Desaparecidos y Explotados.

En numerosas ocasiones, estos ataques son lanzados por hackers y activistas informáticos patrocinados por gobiernos. Los cibercriminales hacen lo mismo con la intención de revender datos confidenciales a gobiernos y empresas privadas. Estos cibercriminales emplean enfoques diseñados individualmente y técnicas de ingeniería social para personalizar de forma eficaz los mensajes y sitios web. Como resultado, incluso objetivos de alto nivel dentro de las organizaciones, como altos ejecutivos, pueden acabar abriendo

correos electrónicos que pensaban que eran seguros. Ese descuido permite que los cibercriminales roben los datos que necesitan para atacar sus redes.

Cómo protegerte

A menudo las medidas de seguridad tradicionales no bastan para detener estos ataques porque están personalizados de forma muy inteligente. En consecuencia, se están volviendo más difíciles de detectar. El error de un empleado puede tener graves consecuencias para las empresas, los gobiernos e incluso para organizaciones sin ánimo de lucro. Con datos robados, los estafadores pueden revelar información sensible desde el punto de vista comercial, manipular precios de acciones o cometer diversos actos de espionaje. Además, los ataques de spear phishing pueden implementar malware para secuestrar computadoras y organizarlas en enormes redes llamadas botnets, que después se pueden usar para lanzar ataques de denegación de servicio.

Para contrarrestar las estafas de spear phishing, los empleados deben ser conscientes de las amenazas, como la posibilidad de recibir correos electrónicos falsos. Además de la educación, se necesita tecnología centrada en la seguridad del correo electrónico.