Publicado en Latinoamérica el 21/10/2021

Siguen creciendo las estafas de phishing a nivel mundial, según DigiCert

Las organizaciones pueden protegerse contra el phishing habilitando la autenticación, informes y conformidad de mensajes basados en dominios

En el año 2020 en Brasil y Latam los correos electrónicos no deseados promediaron un poco más del 50% de todo el tráfico de correo electrónico global. Además, PhishLabs identificó un aumento del 47% en los intentos de phishing de 2020 a 2021. Se han vuelto demasiado comunes: esos molestos correos electrónicos que inundan las bandejas de entrada, diseñados solo para desviar la información personal y más sensible sin que el usuario lo sepa.

En este contexto la compañia Sophos, en su encuesta global Phishing Insights 2021, revelo que los ataques de phishing aumentaron considerablemente durante la pandemia, ya que millones de empleados que trabajaban desde casa se convirtieron en el principal objetivo de los ciberdelincuentes. La gran mayoría de los equipos de TI de las organizaciones encuestadas en México (61%), Colombia (66%) y Chile (69%) informaron que la cantidad de correos electrónicos de phishing que llegaron a sus empleados aumentó durante 2020; En Israel, el 90% reportaron aumentos, siendo este el país con el crecimiento más significativo. En cuanto a sectores, el incremento más alto a nivel mundial se presentó en: gobiernos (77%), servicios comerciales y profesionales (76%) y atención médica (73%), seguidos de cerca por los sectores minorista y educativo con un 71%.

¿Por qué es importante hablar de phishing?
El phishing es un término originado en inglés (pesca) que en informática es un tipo de robo de identidad en línea. Esta acción fraudulenta se caracteriza por intentos de adquirir ilícitamente los datos personales de otra persona, ya sean contraseñas, datos financieros, datos bancarios, números de tarjetas de crédito o simplemente datos personales.

El estafador utiliza correo electrónico, aplicaciones y sitios web que están diseñados específicamente para robar datos personales. El delincuente se hace pasar por una persona o empresa de confianza enviando un mensaje para atraer a sus víctimas. Por lo tanto, al enviar un mensaje a un correo electrónico, aplicación u otras herramientas, el estafador simplemente espera hasta que el destinatario lo recibe y abre el mensaje. En muchos casos, esto es suficiente para que la víctima caiga en la estafa. En otros, es necesario que la víctima haga clic en un enlace determinado para que el delincuente tenga acceso a la información que desea.

“Como en una pesquería real, hay más de una forma de enganchar a una víctima y este tipo de delito se está volviendo cada vez más sofisticado. Los estafadores digitales se han vuelto bastante expertos en hacer que los correos electrónicos fraudulentos se vean exactamente como los legítimos, a menudo de empresas o establecimientos con los que está familiarizado y en los que confía. Los correos electrónicos de phishing comúnmente se hacen pasar por empresas, pero las cuentas de redes sociales también son un objetivo de tendencia, ya que muchos usuarios son más descuidados a la hora de protegerlas”, afirma Dean Coclin, director senior de desarrollo empresarial de DigiCert

Los phishers perseguirán a cualquiera, pero tienden a apuntar a CEO y CFO, firmas legales, recursos humanos e instituciones financieras. Además, en los últimos años las tiendas online y las redes sociales han visto un aumento de los ataques. Estos grupos tienen datos de clientes e información confidencial que los atacantes buscan y necesitan estar en alerta máxima para protegerse de las estafas de phishing.

La diferencia entre phishing y spam

Si bien muchas personas creen que es lo mismo, el phishing es muy diferente al spam. En la práctica, mientras que el spam solo se relaciona con una gran cantidad de correos electrónicos y mensajes, sin ningún fin delictivo, el phishing, como se ve, es una práctica que tiene como objetivo dañar a la víctima, accediendo a datos e información personal.

El spam es generalmente bastante común en Internet. Todos los días, innumerables mensajes de sitios web, tiendas y aplicaciones llenan la bandeja de entrada de la mayoría de los usuarios. Solo crea el inconveniente de la desorganización de la bandeja de entrada, pero no representa ningún riesgo para el destinatario.

Por otro lado, el phishing utiliza el envío de mensajes masivos para engañar al objetivo, induciéndolo a hacer clic en enlaces falsos y / o proporcionar información personal, siempre con el objetivo de dañar a la víctima.

Cómo protegerse a sí mismo y a su empresa del phishing

Existe un software anti-phishing en el mercado, con filtros anti-spam efectivos, que avisan de indicios de irregularidades en los correos electrónicos. En cuanto a los sitios web, existen antivirus y cortafuegos que escanean y notifican irregularidades o bloquean el acceso, cuando detectan alguna posibilidad de fraude. Si sigue estos 10 consejos, estará en el buen camino para convertirse en un experto en defensa contra estafas de phishing.

En lugar de hacer clic en un enlace en un correo electrónico, abrir una nueva página del navegador y escriba la dirección / URL del sitio que se desea visitar. A veces, un enlace fraudulento será muy similar a uno de confianza, simplemente cambiando algunas letras imperceptibles.

Actualizar tanto el sistema operativo como el software del navegador. Las últimas versiones de la mayoría de los navegadores vienen equipadas con filtros anti-phishing. A medida que los atacantes idean nuevos ataques, las actualizaciones de software mejoran sus filtros.

Es una buena idea bloquear las ventanas emergentes cuando se navega por Internet. Es posible orientarse en la web sin la ayuda de direcciones no solicitadas.

Nunca ingresar información personal en ventanas emergentes a menos que se esté completamente seguro de que provienen del sitio deseado.

Para el uso diario de la computadora, utilizar una cuenta de usuario estándar en lugar de una cuenta de administrador. Cambiar a la cuenta de administrador solo cuando las funciones de administrador

sean necesarias. Esto protege la computadora al reducir el acceso a funciones administrativas críticas.

Eliminar y no abrir los mensajes de correo electrónico sospechosos. Puede ser tentador y, a veces, la línea de asunto puede ser pegadiza o tan genérica que se desee obtener más información, pero evitar la tentación y simplemente eliminarla.

Aceptar solo certificados de confianza en páginas web. No ignorar las advertencias del navegador. A veces se reciben tantas advertencias de la computadora o navegador que es casi como el niño que gritó lobo. No descartar simplemente las advertencias que se crean haber visto sin leerlas detenidamente y considerar las implicaciones.

No hacer clic en enlaces que llevan a un sitio o una dirección IP desconocidos.

Estar atento a las advertencias no seguras del navegador. Por ejemplo, Chrome muestra un triángulo de advertencia con "No seguro" en la barra de direcciones si un sitio no tiene habilitado el protocolo de seguridad HTTPS. Habilitar la protección contra malware. Por lo general, esto puede detectar y disuadir la mayoría de las amenazas sin necesidad de hacer nada.

En general, si se recibe un correo electrónico de phishing, no abrirlo, no hacer clic en ningún enlace o archivo adjunto y eliminarlo de inmediato. Si se sigue recibiendo correos electrónicos sospechosos, informar al Grupo de trabajo Anti-Phishing (APWG).

Las organizaciones pueden protegerse contra el phishing habilitando la autenticación, informes y conformidad de mensajes basados ??en dominios (DMARC). DMARC es un protocolo de correo electrónico que dicta la autenticación y los informes de correo electrónico para ayudar a prevenir el phishing y la suplantación de identidad.

Una vez que haya habilitado y aplicado DMARC, la organización puede solicitar un Certificado de marca verificada (VMC) que le permite poner su marca en el marketing y las comunicaciones por correo electrónico. Un VMC le permite representar el logotipo de su marca en el campo del remitente de los clientes de correo electrónico para que los usuarios sepan que su mensaje ha sido autenticado. Es similar a ser verificado en las redes sociales, con los beneficios de seguridad adicionales de la validación y DMARC para proteger contra el phishing.

El phishing es una práctica delictiva muy dañina en el mundo virtual, que provoca pérdidas económicas, daños a los equipos y daños morales. Los estafadores están continuamente buscando nuevos temas y sistemas para capturar nuevas víctimas. Mantenerse al día con las técnicas, trucos y payasadas de los ciberdelincuentes y usar software anti-phishing, antivirus y firewall son las mejores formas de escapar de esta terrible amenaza.

Datos de contacto:
Prensa DigiCert Latam

3125893314

Nota de prensa publicada en: Latinoamérica

Categorías: Internet General Hardware Tecnología Software Seguridad

MexicoPress
https://www.mexicopress.com.mx