Publicado en Ciudad de México el 11/01/2019

# [¿Cómo Avast realiza el reconocimiento visual de phishing?](http://www.notasdeprensa.es)

## El phishing sigue siendo un método de ataque importante porque permite que los ciberdelincuentes se dirijan a personas a gran escala y los sitios web de phishing pueden ser difíciles de identificar. Es por ello que en Avast, usa inteligencia artificial (IA) para detectar fraudes de phishing

 Por lo general, los actores malintencionados distribuyen estafas de suplantación de identidad (phishing) simulando ser representantes de las compañías donde los usuarios tienen alguna cuenta. Los sitios web de phishing pueden ser difíciles de identificar. Es por ello que Avast, (LSE: AVST) el líder global en productos de seguridad digital, usa inteligencia artificial (IA) para detectar fraudes de phishing y proteger a los usuarios de malware y sitios maliciosos. A continuación el proceso de detección. Sitios web falsosEl ciberdelincuente crea sitios web de phishing muy similares a los sitios legítimos para engañar exitosamente a las personas. Las similitudes visuales suelen ser suficientes para engañar a los usuarios para que ingresen sus credenciales y otros datos confidenciales solicitados por el sitio malicioso. Aunque los motores de detección de Avast marcan sitios de phishing basados en contenido HTML, los métodos más sofisticados utilizados por los ciberdelincuentes para crear sus páginas de phishing pueden evitar las detecciones de antivirus. Detectando phishing con IALa vida útil de la mayoría de los sitios de phishing es muy corta, demasiado corta para que los motores de búsqueda los indexen. Esto se refleja en la calificación de un dominio. La popularidad y el historial de un dominio también pueden ser indicadores iniciales de si una página es segura o maliciosa. Al analizar esto y comparar las características visuales del sitio, se decide si el sitio web es limpio o malicioso. El siguiente paso es verificar el diseño del sitio web. Se prueba otro enfoque utilizando hashes de imágenes: un método para comprimir datos de imágenes enriquecidos en un espacio más pequeño (pero todavía expresivo), como un vector de tamaño fijo de bytes con una métrica simple. Estos métodos ayudan a transmitir las imágenes a la inteligencia artificial de Avast al observar de manera muy detallada los píxeles particulares, así como los píxeles que los rodean, los píxeles elegidos por su algoritmo son llamados puntos interesantes. Un problema común con la detección de puntos interesantes en una imagen ocurre cuando una imagen contiene texto. Hay muchos degradados en el texto y las letras que, por diseño, crean muchos bordes. Cuando una imagen contiene muchas letras, hay muchos puntos interesantes en un área pequeña, que pueden resultar en falsos positivos, a pesar de la verificación espacial. Por este motivo, Avast creó un software que puede clasificar los parches dentro de las imágenes y decidir si un parche contiene texto. En casos como este, la IA evitaría usar los puntos del parche como parte del proceso de comparación. Todo este procedimiento es automático, y el 99% de las veces reconocerá un sitio web de suplantación de identidad en menos de diez segundos, lo que a su vez permite bloquear ese sitio malicioso y proteger mejor a los usuarios. Sitios de phishing reveladosLos sitios de phishing han evolucionado enormemente a lo largo de los años para convertirse en falsificaciones convincentes. Algunos incluso usan HTTPS, dando a los usuarios una falsa sensación de seguridad cuando ven el candado verde. Las fallas menores en un sitio web de phishing pueden parecer obvias cuando se ubican junto a una página legítima, pero no son tan notorias por sí mismas. Es probable que los usuarios tengan dificultades para recordar todos los detalles del sitio original, que es exactamente lo que los estafadores de phishing esperan cuando diseñan sus páginas. ¿Cómo se propaga la amenaza?Históricamente, la forma más común de difundir sitios web de phishing ha sido a través de correos electrónicos de phishing, pero también se propagan a través de anuncios pagados que aparecen en los resultados de búsqueda. Otros vectores de ataque incluyen una técnica llamada clickbait. Los delincuentes cibernéticos suelen utilizar clickbait en las redes sociales al prometer algo, como un teléfono gratuito, para alentar a los usuarios a hacer clic en enlaces maliciosos. ¿Qué pasa cuando un phisher tiene éxito?Como casi todos los ataques cibernéticos, el phishing se utiliza para obtener ganancias financieras. Cuando los usuarios entregan las credenciales de inicio de sesión a un sitio de phishing, los ciberdelincuentes pueden abusar de ellas de diferentes formas, según el tipo de sitio utilizado para phishing. Muchos ataques de phishing imitan a instituciones financieras como bancos o compañías como PayPal, que pueden generar importantes recompensas financieras para los ciberdelincuentes. ¿Cómo protegerse?A lo largo de 2018, Avast presenció correos electrónicos maliciosos enviados desde cuentas comprometidas de MailChimp, estafas de extorsión sexual y campañas de phishing relacionadas con GDPR (Reglamento General de Protección de Datos) entre muchas otras. En el futuro, se puede esperar que los ataques de phishing aumenten en volumen y surjan nuevas técnicas para camuflar los esfuerzos de los ciberdelincuentes por robar datos confidenciales de los usuarios. A continuación se incluye una breve lista de verificación que ayudará a evitar que los usuarios sean víctima de una de las formas más exitosas de ataque cibernético: En primer lugar, instalar una solución antivirus en todos los dispositivos, ya sea PC, móvil o Mac. El software antivirus actúa como una red de seguridad que protege a los usuarios en línea. No hacer clic en los enlaces ni descargar archivos de correos electrónicos sospechosos. Evitar responderles también, incluso si supuestamente provienen de alguien en quien confía. En su lugar, los usuarios deben ponerse en contacto con esas entidades a través de un canal separado y asegurarse de que el mensaje realmente proviene de ellas Introducir directamente la URL de un sitio web en su navegador siempre que sea posible, para que el usuario termine visitando el sitio que desea visitar, en lugar de una versión falsa No confiar únicamente en el candado verde HTTPS. Si bien esto significa que la conexión está cifrada, el sitio aún podría ser falso. Los ciberdelincuentes cifran sus sitios de phishing para engañar aún más a los usuarios, por lo que es importante verificar que el sitio que está visitando sea el verdadero.

**Datos de contacto:**

Marketing Q S

Agencia de Relaciones Públicas

+ 52 55 5615

Nota de prensa publicada en: [https://www.mexicopress.com.mx/como-avast-realiza-el-reconocimiento-visual-de](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Inteligencia Artificial y Robótica Hardware Software Ciberseguridad Dispositivos móviles Ciudad de México



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)