Alerta por estafas online: Google habilitó nuevas extensiones de dominio que podrían aumentar el robo de datos

06/06/2023

Google anunció recientemente la habilitación de ocho nuevas extensiones de dominio para sitios web, un hecho que generó inquietud entre los usuarios de Internet. Además de las ya conocidas extensiones como .com y .net, ahora es posible registrar sitios web con extensiones como .zip, lo cual puede ser confuso debido a su asociación con archivos comprimidos, y abre la puerta a nuevas formas de estafas en línea.

La preocupación surgió a raíz de un comunicado oficial de Google en el que se informa que ahora está permitido adquirir sitios web con nombres que terminan en ocho nuevas extensiones: .dad, .esq, .prof, .phd, .nexus, .foo, .zip y

.mov. Esta última extensión, .mov, también representa un conflicto, ya que históricamente se utiliza para indicar un formato de video.

El problema radica en que **esta medida brinda una oportunidad para que los estafadores desarrollen campañas de robo de datos** a través de técnicas de **phishing.** Se trata de una práctica en la que los atacantes engañan a las personas para que revelen información personal y confidencial, como contraseñas, números de tarjetas de crédito o datos bancarios.

Nunca se deben entregar datos sensibles en páginas externas sin corroborar el dominio. Fuente: Unsplash.

Los atacantes pueden utilizar diversas técnicas, como el **envío de correos electrónicos o mensajes falsos**, y la creación de **sitios web similares a los que los usuarios suelen visitar**. En todos estos casos, **los atacantes se hacen pasar por personas o entidades de confianza**.

Con la introducción de la posibilidad de tener páginas web con la extensión .zip, se presenta un **nuevo vector de ataque** que **preocupa a los expertos en seguridad cibernética**. Para comprender los riesgos involucrados, es importante entender la implementación de Google y qué representa un dominio.

Los **dominios en Internet** son **nombres únicos asignados a los sitios web** y **tienen extensiones**. Lo que implementó la empresa es el registro de nuevos **Dominios de Primer Nivel** (TLD, por sus siglas en inglés). Los dominios de Internet se dividen en diferentes nombres separados por un punto, como **canal26.com** o **anses.gob.ar**, donde la parte que sigue al último punto se conoce como TLD.

Inicialmente, existían solo unos pocos TLD, como **«.com» para empresas comerciales y «.gov» para entidades gubernamentales**, y posteriormente se agregaron los TLD de código de país (cTLD)

de dos letras, como «**.ar**» **para Argentina o «.uy» para Uruguay.**

Sin embargo, **Google Registry**, un modelo de negocio operado por **Google**, registró algunos **gTLD (TLD genéricos)** para su uso interno, como **.google**, y otros para alquiler. Actualmente, cualquier persona que pague una tarifa anual significativa pueda obtener un «**.algo**» siempre que no sea ofensivo ni se confunda fácilmente con un código de país, como .online, .cafe, .gratis y otros.

Como resultado, la decisión de Google de permitir que casi cualquier palabra sea un dominio **plantea un grave problema de seguridad para los usuarios de la web.**

Los hackers envían masivamente contenido malicioso, por lo que cualquiera puede estar expuesto a una estafa. Fuente: Unsplash.

Para protegerse, es importante seguir una serie de pautas de seguridad, no solo en relación con este tipo de direcciones web, sino también durante la navegación en general. Lo más indispensable para evitar las estafas es **verificar siempre el nombre de dominio** antes de ingresar información privada.

Consejos clave para evitar el pishing

- Tener precaución y **desconfiar** al recibir correos electrónicos, mensajes o llamadas no solicitados.
- **No dejarse llevar por el sentido de urgencia** que los delincuentes intentan generar, ya que desean que uno se sienta temeroso por un posible bloqueo de cuenta, lo cual dificulta el análisis de la situación.
- **Examinar** cuidadosamente el remitente y los **enlaces** en los correos electrónicos, asegurándose de que redirijan al sitio correcto.
- Evitar hacer clic directamente en los enlaces, y en su

lugar, abrir una nueva pestaña e **ingresar manualmente al sitio web** de la organización.

- Antes de ingresar información privada, siempre **validar que el dominio sea el correcto**, que comience con «**https://**» y que no esté marcado en rojo.
- Mantener un **software antivirus actualizado**.
- En caso de duda, **ponerse en contacto directamente con la empresa** o institución involucrada.

Es fundamental mantenerse informado sobre las últimas tácticas empleadas por los ciberdelincuentes y ser cauteloso al navegar por Internet. Verificar siempre las **URL** antes de hacer clic en ellas resulta especialmente importante cuando se reciben por correo electrónico o mensajes de fuentes desconocidas.

Con o sin las medidas implementadas por **Google**, la vigilancia constante es esencial, ya que los estafadores lanzan sus redes entre miles de usuarios y con solo un pequeño porcentaje que caiga en la trampa, habrán logrado su cometido.

Fuente: Diario 26