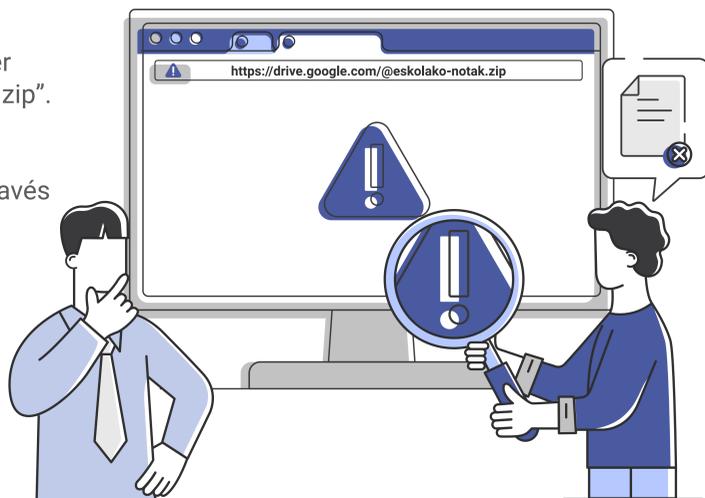
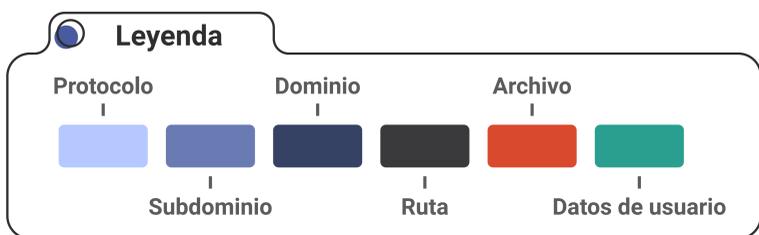


RIESGO DE PHISHING DETRÁS DE LOS NUEVOS TLD: DOMINIOS .ZIP

Google ha lanzado nuevos dominios de nivel superior (TLD o lo que es lo mismo, sufijos que aparecen al final de la URL), que son susceptibles de ser usados para suplantaciones, phishing u otro tipo de estafas online, como “.zip”.

Los ciberdelincuentes siguen innovando e intentando coger al usuario desprevenido, y confundirle entre el nombre de dominio y el de archivo, a través de URLs falsas que parecen legítimas.



¡CUIDADO CON EL USO MALICIOSO DE LA @ EN LAS URL!



En esta URL auténtica, podemos descargar el archivo “eskolako-notak.zip” de forma segura.



Aunque parecen prácticamente iguales, la segunda URL ha sido creada para llevar al usuario a la dirección <https://eskolako-notak.zip>, donde nos encontraremos con un phishing, descarga de malware o ejecución de código malicioso.

OTROS EJEMPLOS DE URL LEGÍTIMAS VS FALSAS CON LAS QUE ANDAR CON OJO:

<https://micarpetasaludberria.osakidetza.eus/analitica.zip>

<https://micarpetasaludberria.osakidetza.eus/@analitica.zip>

<https://e-s.araba.eus/rentafacil.zip>

<https://e-s.araba.eus/@rentafacil.zip>

https://sede.dgt.gob.es/es/mi_dgt/notificacion.zip

https://sede.dgt.gob.es/es/mi_dgt/@notificacion.zip

<https://dbus.eus/dbus-en-mugitzea/lineen-mapa-eta-ordutegiak/ordutegiak.zip>

<https://dbus.eus/dbus-en-mugitzea/lineen-mapa-eta-ordutegiak/@ordutegiak.zip>

<https://ehu.eus/eu/web/unibertsitaterako-sarbidea/egutegia.zip>

<https://ehu.eus/eu/web/unibertsitaterako-sarbidea/@egutegia.zip>

<https://teatroarriaga.eus/proximos-espectaculos/programa.zip>

<https://teatroarriaga.eus/proximos-espectaculos/@programa.zip>

Mantente alerta de las URLs a las que accedes y verifica siempre antes de picar. No rellenes nunca un formulario o descargues un contenido de una página en la que la URL sea sospechosa. Guárdate estos ejemplos y tenlos muy presentes para no caer en la trampa.