CYBERSQUATTING

Qué es el Cybersquatting?

Es el **secuestro** o apropiación de dominio. Consiste en registrar un dominio que **simula** uno legítimo, para posteriormente ***traficar*** con él o hacer uso con fines **fraudulentos**.

¿Qué riesgos implica el cybersquatting?

El nombre de **dominio** es el distintivo de las marcas. Algunos de los riesgos son:

1. El **Domain Name Warehousing,** que es la competencia **desleal**, al registrar y querer revender a un precio más alto el dominio
2. **La presencia** de las marcas puede verse afectada por no tener el dominio correcto
3. El **typosquatting**, consiste en el registro de dominios con faltas ortográficas, con el fin de interceptar el tráfico hacia la página oficial.

Ejemplos de Cybersquatting

Empresa oficial	Dominio Cybersquatting
www.yahoo.com	www.campoyahoo.com
www.incibe.es	www.incibecom.es
www.twitter.com	www.twiiter.com

Si tienes preguntas, o necesitas información adicional, puedes escribir al área de seguridad de la información, con lzambrano@visanet.com.gt , jdepaz@visanet.com.gt o jcastellanos@visanet.com.gt

PROTECCIÓN DE DATOS

El **41%** de las **víctimas** de ciberataques **sufren filtraciones de datos**, según un estudio de Sophos.

El **28 de enero**, se celebra el **Día Europeo de la Protección de Datos** para concientizar a los ciudadanos sobre la importancia de proteger y mantener seguros los datos personales.

Alineados con el espíritu de este día, **Sophos** recomienda que para este 2020 tengamos en cuenta los siguientes **5 consejos para mantener los datos personales a salvo** de los ciberataques:

No bajes la guardia con las contraseñas. Ellas son la puerta de entrada de todo tipo de información confidencial acumulada en cada cuenta. Las **contraseñas** deben ser **robustas, complejas** y tener **al menos 8 caracteres** entre **mayúsculas, minúsculas y números**, y **NO** deben compartirse para varias cuentas.

No presiones en enlaces recibidos por email. A través del **phishing,** los ciberdelincuentes suplantan la identidad de personas o empresas para **acceder a información confidencial** de los usuarios (contraseñas, datos bancarios, etc.)

Protege tú móvil de las cargas USB. Cargar móviles o dispositivos en estaciones de carga USB públicas puede exponer los dispositivos y los datos que contienen a un robo de datos si el **punto de carga** ha sido afectado con algún **malware**. Con estas amenazas, muchos smartphones, tablets y ordenadores incluyen un **modo seguro de carga** o acceso a un puerto USB para evitar transferencia de datos y proteger la conexión.

Desconfía de las WiFi-Públicas. Las conexiones a redes wifi-abiertas son puntos vulnerables. Las herramientas de **spoofing** usadas por los ciberdelincuentes transforman los dispositivos maliciosos en **puntos de conexión wifi falsos** para que los usuarios desprevenidos se conecten y expongan sus datos.

Antivirus para el dispositivo móvil siempre. Es fundamental contar con un software de seguridad que proteja los accesos y la información que almacenan nuestros dispositivos móviles.

Si tienes preguntas, o necesitas información adicional, puedes escribir al área de seguridad de la información, con lzambrano@visanet.com.gt , jdepaz@visanet.com.gt o jcastellanos@visanet.com.gt