Cyber MSME

Ciberseguridad para PYMES

¿Cómo reconocer URLs de confianza?

Directrices

Creado por CTS Customized Training Solutions & CASE

Erasmus+

Índice— pulse para ir a la página correspondiente:

Antes de abrir ningún enlace adjunto en un mensaje o email, verificar lo siguiente:

1. Mirar primero el nombre del dominio

Las URLs en dominios .gov, .org, y .edu deberían ser seguros.

.com y dominios de países (.es – España, .pl — Polonia, .be — Bélgica, .it – Italia, .pt — Portugal, .ro — Rumanía, etc.) son fáciles de comprar, no sólo para residentes de un cierto país, por lo tanto no es fácil saber si son de confianza o no. Prestemos atención también a los nuevos dominios que se están popularizando recientemente en el mercado, por ejemplo:

- .app
- .agency
- .center
- .design
- .network
- .online
- .tech
- .training
- .university

El nombre de una web debería ser **example.app** o **example.design** — normalmente suena como el nombre completo de la empresa o el producto.

Las empresas tecnológicas y start-ups suelen crear cada vez más páginas web y portfolios en dichos dominios. Por otro lado, URLs con tales terminaciones se usan en ingeniería social.

Nuestro consejo: **no hagas clic demasiado rápido, verifica antes siempre**.

2. Tener cuidado con enlaces muy largos o extraños

Los enlaces dañinos a menudo son bastante largos y contienen cadenas de palabras y letras sospechosas. Si no reconocemos la dirección, no hacer clic nunca en ella.

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3. Buscar errores tipográficos

A veces una URL es casi idéntica a otra que conocemos bien. Contiene un pequeño error tipográfico de tal manera que en vez de ir a la página web de nuestro banco o proveedor de internet, el enlace nos lleva a una página que infectará nuestro dispositivo.

4. Revisar la ortografía del mensaje

Revisemos el mensaje en el que hemos recibido el enlace:

- ¿Contiene errores tipográficos?
- ¿El estilo de escritura concuerda con la persona/institución que supuestamente ha enviado el mensaje?
- ¿Se usan en exceso las mayúsculas en el mensaje? (Esto es común en el spam).
- ¿La información que proporciona el autor del mensaje parece creíble? ¿Menciona fuentes? ¿Puede verificarlas?

Erasmus+

5. Un candado no es una garantía de seguridad

Cuando visitamos una página web, probablemente nos fijamos si tiene un certificado de seguridad, es decir, si tiene un símbolo de candado junto a la dirección de la página web.

El problema es que el símbolo del candado cerrado no significa que la web sea segura. ¿Por qué? Porque cada empresa puede emitir un certificado de este tipo (se denomina certificado autofirmado). Por supuesto, un navegador nuevo y actualizado reconocerá un certificado no confiable y nos informará de inmediato.

Por tanto, para asegurarnos que nuestros datos y dispositivos no sufran ataques, pulsemos en el candado y verifiquemos si el certificado de seguridad fue emitido por una empresa de auditoría de confianza. Y por supuesto, hay que actualizar nuestro navegador con regularidad.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

¡ Gracias por su atención!

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained