Cyber MSME

Cybersecurity per Micro, Piccole e Medie Imprese

Come riconoscere gli URL? - Guidelines

By CTS Customized Training Solutions & CASE

Erasmus+

Indice degli argomenti— clicca per andare direttamente alle pagine rilevanti:

Prima di aprire qualsiasi link in allegato, esegui questi passaggi:

1. Look at the domain first

URLs con dominio.gov, .org, and .edu dovrebbero essere sicuri.

.com and domini del Paese(.pl — Poland, .be — Belgium, .it – Italy, .pt — Portugal, .ro — Romania, etc.) possono essere acquistati da tutti, perciò è difficile dire se sono o meno affidabili. Stai attento ai domini appena creati e sono conosciuti da poco tempo, e.g.

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

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.

Il nome del sito potrebbe essere **example.app** or **example.design** — è molto commune che venga riportato il nome complete dell'azienda o del prodotto.

Le aziende tecnologiche e le start-up creano sempre più spesso siti con tali domini. D'altra parte, però, questo tipo di terminazioni sono usate anche nel social engineering
Il nostro consiglio: **non avere fretta di cliccare, controlla sempre attentamente!**

2. Stai attento a link molto lunghi e inusuali

I link dannosi sono spesso molto lunghi e contengono una serie di parole e lettere discutibili.
Se non riesci a riconoscerle, evita di aprire il link!

Erasmus+

3. Controlla gli errori di battitura

Spesso l’url è molto simule a uno che conosci bene. Se contiene errori di battitura, tale link invece di rimandarti sulla pagina web della tua banaca infetterà immeditamente il tuo PC.

4. Verifica gli errori di ortografia

Controlla il messaggio che ti hanno inviato insieme al link:

- Contiene errori di battitura?
- Il tono comunicativo rispecchia quello dell’organizzazione da cui dice di provenire?
- È presente un lucchetto aperto? (è tipico delle email spam).
- Le informazioni riportate sono credibili? Viene menzionata la fonte? Puoi verificarla?

5. Il lucchetto non è una garanzia di sicurezza

Quando visitate un sito web, probabilmente prestare attenzione a se ha una certificazione di sicurezza, ad esempio il simbolo del lucchetto chiuso.

Il problema è che non sempre tale simbolo è sinonimo di sicurezza. Perché?

Perché si tratta di un autocertificato di cui ogni azienda può dotarsi.

Naturalmente un browser aggiornato è in grado di riconoscere quando un Url è fittizio.

Quindi, per assicurarsi che i dati e i dispositivi non vengano attaccati, è importante cliccare sul lucchetto per vedere da chi è stato rilasciato il certificato

E, naturalmente, aggiornare il tuo browser regolarmente. .

Erasmus+

Grazie per l’attenzione!

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