Cyber MSME

Cyberbezpieczeństwo dla mikro, małych i średnich f irm

Jak rozpoznać wiarygodne adresy URL?

Wskazówki

Autorzy: CTS Customized Training Solutions i CASE

Erasmus+

Spis treści — kliknij, aby przejść do odpowiedniej strony:

Zanim otworzysz jakikolwiek link załączony w wiadomości lub e-mailu, zapoznaj się z poniższymi wskazówkami:

1. Najpierw spójrz na domenę

Adresy URL w domenach .gov, .org i .edu powinny być bezpieczne.

Domeny .com i domeny krajowe (.pl - Polska, .be - Belgia, .it - Włochy, .pt - Portugalia, .ro - Rumunia, itd.) są łatwe do kupienia nie tylko dla mieszkańców danego kraju, trudno więc powiedzieć, na ile są wiarygodne. Zwróć uwagę na nowe domeny na rynku, które są ostatnio popularne, np.:

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

Erasmus+

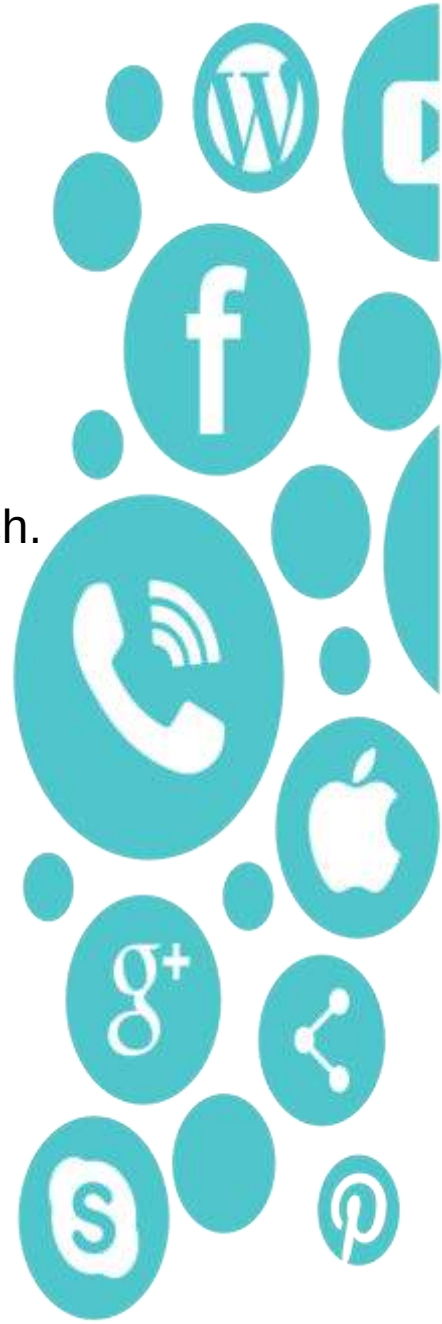
Nazwa takiej strony to example.app lub example.design — zazwyczaj brzmi ona jak pełna nazwa
firmy lub produktu.

Firmy technologiczne i start-upy coraz częściej tworzą strony i portfolio na takich domenach. Z drugiej strony adresy URL z takimi końcówkami są wykorzystywane w socjotechnice.

Nasza rada: **nie klikaj zbyt szybko, najpierw zawsze sprawdzaj**.

2. Wystrzegaj się bardzo długich i nietypowych linków

Szkodliwe linki są często długie i zawierają budzący zastrzeżenia ciąg słów i liter. Jeśli
nie możesz rozpoznać adresu, nie klikaj na niego.



Erasmus+

3. Szukaj literówek

Czasami adres URL jest prawie identyczny jak ten, który dobrze znasz.

Zawiera jednak drobną literówkę, która sprawia, że zamiast na stronę banku lub dostawcy Internetu, link przeniesie Cię

na stronę, która zainfekuje Twoje urządzenie.

4. Sprawdź pisownię w wiadomości

Sprawdź treść samej wiadomości, w której otrzymałeś/-aś link:

- Czy zawiera literówki?
- Czy styl pasuje do osoby/ instytucji, która rzekomo ją wysłała?
- Czy użyto przesadnie capslocka w wiadomości? (Jest to częste w przypadku spamu).
- Czy informacja, którą podaje autor wiadomości jest wiarygodna? Czy podaje on/ona źródła? Czy możesz je zweryfikować?

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.

5. Kłódka nie gwarantuje bezpieczeństwa

Kiedy odwiedzasz jakąś stronę internetową, zapewne zwracasz uwagę na to, czy posiada ona certyfikat bezpieczeństwa, czyli ma symbol kłódki przy adresie strony.

Sęk w tym, że symbol zamkniętej kłódki nie oznacza, że strona jest bezpieczna. Dlaczego? Ponieważ taki certyfikat każda firma może wystawić sobie sama (jest to tzw. certyfikat samopodpisany, ang. self-signed certificate). Oczywiście nowa i aktualna przeglądarka rozpozna niewiarygodny certyfikat i od razu da Ci o tym znać.

Dlatego, aby upewnić się, że Twoje dane i urządzenia nie są narażone na atak, kliknij na symbol kłódki i sprawdź, czy certyfikat bezpieczeństwa został wystawiony przez wiarygodną firmę audytorską. I — co nie powinno być zaskoczeniem — regularnie aktualizuj swoją przeglądarkę.

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.

Dziękujemy za uwagę!

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