Cyber MSME

Cybersecurity for Micro, Small & Medium Enterprises

How to recognize credible URLs?

Guidelines

By CTS Customized Training Solutions & CASE

Erasmus+

Table of contents — click to skip to the relevant page:

Before you open any link attached in a message or e-mail, check the following guidelines:

1. Look at the domain first

URLs on domains .gov, .org, and .edu should be safe.
.com and country domains (.pl — Poland, .be — Belgium, .it – Italy, .pt — Portugal, .ro — Romania, etc.) are easy to buy for more than just residents of a particular country, so it's hard to say how reliable they are. Pay attention to new domains on the market that are recently popular, e.g.

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

Erasmus+

The name of such a website would be **example.app** or **example.design** — it usually sounds like the full name of the company or the product.

Technology companies and start-ups more and more often create websites and portfolios on such domains. On the other hand, URLs with such endings are used in social engineering. Our advice: **don't click too fast, always check before**.

2. Beware of very long and unusual links

Harmful links are often long and contain an objectionable string of words and letters. If you cannot recognize the address, do not click on it.

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.

3. Look for typos

Sometimes a URL is almost identical to the one you know well. It contains a minor typo so that instead of going to your bank's or Internet provider's website, the link will take you to a page that will infect your device.

4. Check the spelling in the message

See the message itself in which you received the link:

- Does it contain typos?
- Does the style match the person/institution that supposedly sent it?
- Is the capslock overused in the message? (This is common in spam).
- Is the information that the author of the message provides credible? Does he/she mention sources? Can you verify them?

5. A padlock is not a guarantee of security

When you have visited a website, you probably pay attention to whether it has a security certificate, i.e. has a padlock symbol next to the website address.

The thing is that the closed padlock symbol does not mean that the website is safe. Why? Because such a certificate can be issued by every business itself (it is called a self-signed certificate). Of course, a new and up-to-date browser will recognize an unreliable certificate and let you know right away.

So to make sure that your data and devices are not attacked, click on the padlock and check if the security certificate was issued by a reliable auditing company. And of course, update your browser regularly.

Thank you
for your attention!

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