Spam, Phishing and Malware

Motto:

- Bad news = You cannot be prepared to all attacker's inventions
- Good news = Being slightly more clever, than the attacker expects you are, is enough.
- 1. Quick and automate reaction makes troubles.
- 2. Do not accept what message suggests, until you are perfectly sure you understand the intentions.
- 3. Do not belive the sender's identity until you really verify it (check sender's email address closely).
- Better safe, than sorry.

Bonuses:

Good article about clicking links in emails

How and why Thunderbird block remote content

See also "**Dealing with malware**, **spam**, **suspicious content**" in separated CERGE-EI Wiki article (details about security measures applied to incoming emails)

and "Spam fiters at CERGE-EI" (describing chain of email filters for incoming traffic)

Types of attacks, its danger and adequate reaction:

spam

- Unsolicited mail, just offers unneeded or annoying things.
- By links to <u>fraudulent webpages</u> or <u>danger attachments</u> could be transformed to other type.
- Do not open links and attachments, do not reply to it, delete it.

hoax

- By wiki: A hoax is a falsehood deliberately fabricated to masquerade as the truth.
- You could be abused to help distribute it. Other harmful content could be appended.
- Do not resend it to any other address, delete it.

phishing

• Ask for confidential and private information, often by using fraudulent webpage, masking the request as an account renew etc. Make <u>time pressure</u> and <u>urgency illusion</u>.

- Never use offered links without its <u>authenticity thorough verification</u>.
- Be very careful and abstemious by inserting your login and password anywhere.

spoofing

- The message looks like sent from a trustworthy address, your jobmate, manager, IT crowd, your home institution server etc.
- Verify sender's email address, not only the free text label presented by some e-mail client.
- Take care of "mistyped" form of address, e.g cerce-ei,cz or enlarged form cerge-ei.cz.xxxxx etc.

malware

- The harmful code hidden in an executable attachment or in a document as a macro or on the fraudulent webpage linked from the message.
- Never open documents or pages looking like something very very interesting. There is no chance to take a non-binding look.

ransomware

- Special malware <u>encrypting every data</u> you can access and asking ransom. The process of encrypting could be long term so backups could be affected too.
- Avoid being infected by malware.

What to do, if you become a target of the cyber attack

- 1. Thing first, check all circumstances, ask in doubt.
- 2. Do not accept time presure, postpone action, back to 1, how many times you need.
- 3. Only if you are sure, make some settings, password change etc.
- 4. In case of any suspicion, tell it including all details to IT.
- 5. If you have by mistake compromised your password, change it ASAP and inform IT (compulsory).

In any doubt, do not hesitate to ask **helpdesk@cerge-ei.cz**. Please prepare complete documentation, timeline, addresses, raw text of message (see wiki - problem reporting)

From:

https://wiki.cerge-ei.cz/ - CERGE-EI Infrastructure Services

Permanent link:

https://wiki.cerge-ei.cz/doku.php?id=public:emai:spam&rev=1635241351

Last update: 2021-10-26 09:42



https://wiki.cerge-ei.cz/ Printed on 2025-09-09 00:29