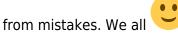
Spam, Phishing and Malware

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.
- Quick and automate reaction makes troubles.
- 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.
- Be brave! Never try to conceal your possible mistake take it in possitive way we all learn



• Cowards who awkwardly try to avoid of mistake revealing usualy make things much worse for them and for the rest of the institution.

Bonuses:

Good article about clicking links in emails (phishing etc.)

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

[Classification: POTENTIALY DANGEROUS]

- 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

[Classification: ANNOYING]

- 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

[Classification: PRETTY DANGEROUS]

- 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

[Classification: DANGEROUS]

- 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

[Classification: DANGEROUS]

- 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

[Classification: THE MOST DANGEROUS]

- 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.
- It is important to avoid being infected by such malware. It affects the whole institution.

What to do, if you are uncertain about email (possible cyber attack)

- 1. Thing first, check all circumstances, ask in doubt (IT, colleagues, sender,...).
- 2. Do not allow the time presure effect, think twice. postpone the action (back to step 1 eventually

3. Only if you are absolutely sure, continue with an action suggested in email (settings review,

https://wiki.cerge-ei.cz/ Printed on 2024-05-02 02:56

password change etc.)

- 4. In case of any suspicion at any time, share it with IT (including all details).
- 5. If you think you have compromised your password or account in any way, change the password 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=1635242573



