computer emergency response team | CERT-EU for the EU institutions, bodies and agencies

Security White Paper

Handling of Potentially Malicious Emails

As a user of email, you may at some point receive a malicious email designed to steal information or cause damage to your information.

Harmless looking links may well be the doorway to a malicious website, which is designed to compel the user to divulge personal or sensitive information.

Hackers also frequently use email-attachments to deploy their malicious software (malware). In such cases, the emails are given a tempting title, or contain an enticing message, which will lure the unsuspecting user into opening the attachment. Opening the attachment may put your computer under control of the hacker, without you even noticing. The malware may also escape detection by the anti-virus system.

To assess the trustworthiness of an email you receive, look for the obvious traits normally found in malicious emails:

- A sense of urgency, which instinctively makes you do something without first thinking about it;
- Requesting sensitive and/or personal information such as account numbers, credit card numbers, passwords, etc. Most reputable organisations do not request such information from you via email, and those who do should have a predefined agreement with you in this regard;
- Long, strange links. A link should be rational, and it should be easy to see what site it will take you to. However, a good-looking link does not guarantee that it is safe. Consider also the other tell-tale signs.
- Spelling mistakes and grammatical errors. In a multi-lingual environment, this feature is not a reliable clue on its own, so consider it in combination with other features in this list;
- The sender is not known to you. Again, attackers have found a way to circumvent this by a method known as 'spoofing'. Therefore, even if the sender appears to be someone you know and trust, look for the other characteristics like unexpected email address extensions;
- If you think an email looks suspicious then most probably it is.

If you receive an email which you feel is suspicious:

- Do not click on any links, not even the "unsubscribe" link
- Do not open any attachments
- Do not delete the email
- Send the suspicious email as an attachment to your Institution's functional mailbox for suspicious emails [to be completed]
- If in doubt, contact your IT Helpdesk for assistance.

CERT-EU Team (http://cert.europa.eu)
Phone: +32.2.2990005 / e-mail: cert-eu@ec.europa.eu
PGP KeyID 0x46AC4383
FP: 9011 6BE9 D642 DD93 8348 DAFA 27A4 06CA 46AC 4383