Ransomware and Phishing – increasing in large proportion

April 4, 2016

In the past few months, we have seen a serious increase in the number of companies affected by Ransomware and the encryption virus.

The encryption virus (Locky, WinPlock, Cryptolock …) is a virus that you catch through reading a phishing email or following a link to a website that is infected. Ransomware is a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back.

As a general precaution, if you get an email from an unknown or known address, suggestion you to click on a link to get access to an order, or an invoice or anything else that you are not expecting, it is better not to click on it. If you have an email from a bank or email server or anything asking you to type your username and password to regenerate or unlock your account, you should not type anything and simply delete the email.

You should as a rule never follow a link to a URL and then type a user name and password to gain access, if you need any access to any website, you type

the UR yourself and click on a shortcut or a bookmark in your browser but not from a link you received in email or a link on internet.

To prevent ransomware infections, keep these things in mind:

- Backup your files regularly and keep a history, we suggest at least 30 days.
- Apply software patches as soon as they become available. Some ransomware arrive via vulnerability exploits.
- Bookmark trusted websites and access these websites via bookmarks.
- Download email attachments only from trusted sources.
- Scan your system regularly with anti-malware.

Read here to learn more