Scam alert on

Ransomware

How the scam works

Criminals seize and hold the organization's information systems and data to ransom. Here's roughly what happens:

1. Criminals rent crypto-ransomware (a kind of virus) through the criminal underground.
2. Victims accidentally pick up a ransomware infection, usually by opening infected email attachments, websites or apps.
3. The ransomware secretly encrypts all the data that is on or accessible through device, including hard drives, flash/USB drives, network drives and cloud backups. If victims try to access the information while it is being encrypted, the ransomware decrypts it for them so they notice nothing wrong except maybe a small delay.
4. When all the data has been encrypted, the extortion phase begins: the criminals normally demand a few hundred or thousand dollars' worth of untraceable Bitcoins for the decryption key needed to recover the data.
5. The victim has to decide, quickly, whether to wipe the computer and reload everything from backups that were taken and stored offline *before* the incident, or cave-in to the ransom demands before the time runs out.
6. Despite the best efforts of IT and security professionals, even the FBI, the encrypted information is usually indecipherable. After just couple of days or so, the deadline expires, the key is destroyed and the information is gone - *forever*. It's game over: you lose.

Avoid the scam

- **Be absolutely certain that you have good offline backups**: this is a strong defense and (if the decryption key doesn't work or never arrives) may be the only possible way to recover the data.
- Be *extremely* wary of email attachments, links in emails or text messages, dubious websites and apps from the unofficial app stores, and keep antivirus software and security patches up to date.
- If you receive a ransom demand, call Help Desk to report the incident right away. Don't waste a moment! The clock is ticking until the key expires.

More information

Browse the *Security Zone* or call Help Desk for more on ransomware and advice on other kinds of malware plus backups, antivirus software, patching *etc*. Do it *now*, before you run into trouble.

Copyright © 2017 IsecT Ltd.