HealthManagement.org
Promoting Management and Leadership

New Cyber security Threat: 'Locky'

Following the recent ransomware incident at Hollywood Presbyterian Medical Centre, that saw the facility paying out $17, 000 in to regain access to IT systems, a new threat has been spotted.

Named ‘Locky’, it is a virus that is delivered in an email attachment disguised as a Microsoft Word invoice. Once a user opens it and enables macros, it encrypts valuable files and holds them hostage.

A typical ‘Locky’ email will have the following subject line:

"Please see the attached invoice and remit payment according to the terms listed at the bottom of the invoice."

When opened, the document appears to be non-sensical and instructs users to activate macros to make the text readable. As soon as this happens, the malware executes.

Cyber security experts have explained that ‘Locky’ creates a lock screen with a timer notifying the user how much time is left until a ransom must be paid. While the computer is still usable, files are encrypted and it is impossible to detect which ones.

See Also: How to Defend Against a Cyber Attack

If the ransom is paid, keys are released to decrypt ‘Locky’. If it is not, the encrypted files disappear.

‘Locky’ is one of the fastest-spreading viruses in cyber space, experts say.

Paying the ransom is more cost-effective for some organisations than rebuilding a system and even protecting their reputation.

The easiest way to avoid a ‘Locky’ attack is to ‘not click’. However, in a busy work environment, it is impossible to expect staff to vet every single email.

One way of keeping safe is to implement a security system that monitors suspicious activity on email and social traffic, experts say.

Source:

Healthcare It News

Image Credit:
It Security Mind

Published on : Mon, 29 Feb 2016