BROWN

Learn about Ransomware and How to Protect Yourself

patricia falcon - 2017-03-09 - Comments (0) - Antivirus and Malware

The threat of ransomware is growing. Here's how to protect yourself and what to do if your computer becomes infected.

Ransomware is malicious code that encrypts your files, making them inaccessible until you pay a ransom. “Locky”, a type of ransomware, which affects both Windows and Mac, has been reported at Brown. It often arrives via email as a Word document that looks like an invoice, or like a supposedly useful small application. If you open the document or application and follow prompts to run a macro, Locky will download and infect your computer, demanding a bitcoin payment in order to restore your access to files.

Important Measures

- **Take action if you notice unusual behavior on your computer, such as inaccessible files, apps that will not run, or notices demanding payment.** Immediately disconnect your computer from the internet by unplugging your ethernet cable and turning off wifi, and shut your computer down. This will avoid spreading the ransomware to other members of the Brown community. Then, immediately contact your department’s computing staff (DCC or ITSC) or the IT Service Center.
- **Make sure your files are backed up**. If you have a Brown-owned computer and are not certain if your files are backed up, we strongly encourage you to check with your department’s computing staff. On a personally-owned computer, consider using Google Drive, which offers unlimited storage. If you're backing up files on a thumb drive or external hard drive, be aware that it too could get infected if it is plugged in to your computer.

Other Suggestions

- **Check that your Microsoft software settings (e.g., Word, Excel) do not allow macros without your permission.** This article has instructions applicable to most Windows and Mac versions: Disable Macros in Microsoft Software
- **If you have a personally-owned computer, make sure you have current anti-virus, anti-spyware, and anti-malware software.** We have options available for download on Brown’s software site. Schedule regular scans, and scan all removable drives before opening files.
- **Don’t open email attachments unless you are expecting them and they come from a trusted source**. Even if they appear legitimate, be suspicious,

because email can be spoofed to look like it is coming from one of your contacts. If you receive an unexpected attachment and are unsure of its legitimacy, check with the sender.

- **Ransomware can also attack from a website.** Make sure your web browsers are updated and that vulnerable plugins like Flash and Java require your permission to run.