



## **COT Security Alert – Ransomware Threat**

---

A variant of ransomware known as CryptoLocker surfaced in 2013 and as a result an increasing number of ransomware infections have occurred nationwide. Ransomware is an infection that encrypts the user's system or files and gives instructions, usually in a pop-up window, demanding a payment before the user will be given the key to decrypt files and recover their system. USB drives, shared network drives and other external or network devices **can be affected** by the infection of one computer, depending on the user's privileges. The most popular method used to spread this infection is by phishing emails containing malicious attachments.

While COT has taken preventive measures to protect state users from falling prey to CryptoLocker, attackers will regularly change code or attack methods in efforts to avoid detection and expand the number of potential victims. It is important that users are always aware so that changes in tactics are not successful.

Users should do the following **at all times** to reduce the likelihood of infection:

- Avoid clicking on links in unsolicited emails.
- Avoid opening email attachments in unexpected emails, even if the sender is known.
- If an unexpected email containing a link or attachment comes from a known sender, contact the sender to verify they intended the email to be sent.
- Save work or important files where they can and will be backed up regularly and often.
- Keep operating system, antivirus and software patches up-to-date. While this may be done by the IT department at work, home systems are susceptible and need this protection as well.

Should any state computer become infected with ransomware, do not respond to extortion attempts by making the payment requested. **First action** should be to disconnect the network cable or turn off wireless network connections immediately, however **do not** shut the device down or unplug the power cable. The Commonwealth Service Desk ([CommonwealthServiceDesk@ky.gov](mailto:CommonwealthServiceDesk@ky.gov)) should then be contacted immediately to open a ticket and notify the COT Security Operations Forensics Team to investigate. Information derived from an investigation may assist in protecting state users from future attacks. Home users are advised to contact the Internet Crime Complaint Center (IC3) which is a section of the FBI.

Links:

Internet Crime Complaint Center

[www.ic3.gov](http://www.ic3.gov)

US-CERT Alert TA13-309A

<http://www.us-cert.gov/ncas/alerts/TA13-309A>

**Please share this information with end users. End users will find this information useful for both state and home computer system security and for overall security awareness.**

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

**Security Administration Branch  
Commonwealth Office of Technology  
120 Glenn's Creek Road, Jones Building  
Frankfort, KY 40601**

[COTSecurityServicesISS@ky.gov](mailto:COTSecurityServicesISS@ky.gov)

<http://technology.ky.gov/ciso/>