



COT Security Alert - Income Tax Themed Phishing Emails

The COT Security Administration Branch warns users that emails specially crafted around events such as income tax deadlines are utilized to spread malware or to obtain personal information from the user. They may use scare tactics such as indicating your refund is held up until they clarify your personal information, or they may offer to file your taxes to get you a new "tax break" and scam your money and your identity. These emails most often appear to be from an income tax preparer or from the IRS.

Avoid falling victim to these phishing emails, as well as any others by:

- Making it a rule to never respond to an unsolicited email with personal information, or clicking on a link or attachment within an unsolicited email.
- Never using contact information in an unsolicited email. If you feel you need make contact with the IRS or your tax preparer, use the official websites to obtain their phone number or other contact information.
- Keeping your home computer current on antivirus, antispyware, operating system and application updates.

For more information from the IRS:

<http://www.irs.gov/uac/Suspicious-e-Mails-and-Identity-Theft>

<http://www.irs.gov/uac/Report-Phishing>

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

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