



COT Security Alert – Seasonal Malicious Activity Awareness

During the holiday shopping season there is typically an increase in phishing, malware and scam campaigns. This is a time when malevolent entities consider users highly vulnerable to deceptive tactics because of the rush of the season and heavier than normal involvement in online shopping and banking. Users are encouraged to be aware while online at home as well as at work.

Some examples of these malicious campaigns include:

- electronic greeting cards which often contain malware
- fake charities requesting contributions and personal information
- businesses that are either not legitimate or are not trusted who use online ads to obtain personal information
- phishing in the form of charities, credit card applications and shopping incentives
- screensavers or other forms of media or executables that may contain malware
- surveys that include asking for personal information
- online contests offering prizes and which may be engineered to appeal to children, the elderly, etc. who may be more easily convinced to respond with personal information

Users may consider taking the following preventive measures:

- Do not click on links or open attachments in unexpected emails, even if the email is from someone you know. Emails are often the result of an account stolen in a previous phishing campaign and may appear to be from a friend as well as a stranger. If you are not sure, contact the sender to affirm the email is from them.
- Maintain up-to-date antivirus software, as well as browser, operating system and other software.
- Use a source such as the Federal Trade Commission's Charity Checklist or the Better Business Bureau's National Charity Report Index to check on a charity before giving.
- Do not respond to an email by reply or using a link it contains with any personal information.
- To open a credit card account, go to the site yourself rather than clicking on links in emails or online advertisements.
- Educate yourself and your family on how to recognize and avoid scams and how to maintain a secure computer.

Informative links:

<http://www.ftc.gov/bcp/edu/pubs/consumer/telemarketing/tel01.shtm>

<http://charityreports.bbb.org/public/All.aspx?bureauID=9999>

<http://www.onguardonline.gov/topics/avoid-scams>

<http://www.us-cert.gov/cas/tips/ST04-014.html>

http://www.us-cert.gov/reading_room/emailscams_0905.pdf

<http://www.us-cert.gov/cas/tips/ST07-001.html>

<http://www.us-cert.gov/cas/tips/ST04-010.html>

This email contains information that is useful for all end users. Please distribute for security awareness purposes.

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
Frankfort, KY 40601**

COTSecurityServicesISS@ky.gov

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