

COT Security Alert - Swine Flu or H1N1 Related Malicious Emails

US-CERT, the United States Computer Emergency Readiness Team, anticipates elevated circulation of phishing attacks and other malicious emails that use the Swine Flu as a ploy. Users should be aware that email relating to this subject may be playing on people's fears or sense of civic responsibility in order to spread malware, to scam or to obtain personally identifying information for the purpose of fraud. In addition to the protective measures already in place, the COT Security Administration Branch reminds users to follow the [Enterprise Internet and Electronic Mail Acceptable Use Policy](#) and to be cautious while online or corresponding by email. These cautions include the following:

- Do not download an application unless it has been approved.
- Do not follow unsolicited links or open unsolicited email messages or attachments.
- Use caution when visiting untrusted websites.

For more information concerning this activity, US-CERT has a link at <http://www.us-cert.gov/current/?tag=mncol:txt>.

For more information on spam, phishing or malicious emails, how they engineer people to respond and what users can do, visit these sites:

- <http://www.ftc.gov/spam/>
- <http://www.onguardonline.gov/default.aspx>

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/security/>**

