



COT Security Alert – Bin Laden -Themed Phishing Emails

Headline news events are commonly used by malicious entities as an opportunity to implement phishing attempts themed on the event to spread malware. This is especially true for those news items which are emotionally charged, such as the recent news concerning Osama Bin Laden. These emails will often contain embedded links or claim to contain exclusive photos, videos, polls or articles on the subject, but in actuality they are designed to infect the user's computer with malware.

Preventative Strategies:

- Do not open unsolicited emails, even if they are from someone you know. If you know the sender, verify they actually sent the email and their address was not "spoofed". Spoofing is a common ploy among spammers and phishers.
- Do not open emails that have suspicious subjects or senders, even though they have passed filters and antivirus software. Attackers are constantly releasing new or updated malware which has not yet been addressed by antivirus software. These are called "zero-days".
- Save attachments to your computer and scan them before opening if possible. This will not require opening the attachment, but you can right-click and select "Scan for threats". Delete any attachments you decide not to open.
- Reduce the amount of spam you receive at work by not signing up for anything personal using your work email address.

Please distribute this email to all staff.

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/>