NCCIC ADVISORY

National Cybersecurity & Communications Integration Center

2 MAY 2011 – 1400: OSAMA BIN LADEN – THEMED PHISHING ATTEMPTS

SUMMARY

The intent of this advisory is to provide general guidance to public and private sector organizations and individuals on potential targeted phishing attacks (often referred to as "spear phishing") with respect to the Osama Bin Laden related media reporting, and to offer some suggested methods that may minimize the likelihood of a successful attack. Widest distribution of this advisory is highly encouraged.

OVERVIEW

In the wake of large news events, it is common for malicious actors to take advantage of increased media attention by implementing associated "spear phishing" attempts. These emails will often contain embedded links or purport to include exclusive photos or videos, either found on suspicious websites, or included as attachments or links in emails. To protect yourself from these threats, the National Cybersecurity & Communications Integration Center recommends the following actions:

PREVENTATIVE STRATEGIES

The following preventative strategies are intended to help our public and private partners proactively look for emails attempting to deceive personnel into 'clicking the link' or opening attachments to seemingly real emails regarding the ongoing media coverage on the death of Osama Bin Laden. Although this is not an all inclusive list, it represents common best practices.

- **Be wary of unsolicited attachments, even from people you know** - Just because an email message looks like it came from a familiar source, malicious actors often "spoof" the return address, making it look like the message came from someone else. If you can, check with the person who supposedly sent the message to make sure it's legitimate **before** opening any attachments. This also includes email messages that appear to be from your Internet Service Provider (ISP) or software vendor claiming to include patches or anti-virus software. ISPs and software vendors do not send patches or software in email.
- **Keep software up to date** - Install software patches so that attackers can't take advantage of known problems or vulnerabilities (see Understanding Patches for more information). Many operating systems offer automatic updates. If this option is available, you should enable it.
- **Trust your instincts** - If an email or email attachment seems suspicious, don't open it, even if your anti-virus software indicates that the message is virus free. Attackers are constantly releasing new viruses; these are called 'zero-days' and most likely your anti-virus software does not have a signature for it yet. Don't let your curiosity put your computer at risk.
- **Save and scan any attachments before opening them** - If you have to open an attachment before you can verify the source, take the following steps:
    1. Be sure the signatures in your anti-virus software are up to date (see Understanding Anti-Virus Software for more information).

2. Save the file to your computer or a disk.
3. Manually scan the file using your anti-virus software.

- **Turn off the option to automatically download attachments** - To simplify the process of reading email, many email programs offer the feature to automatically download attachments. Check your settings to see if your software offers the option, and make sure to disable it.
- **View emails in "Plain Text"** – many email applications have options to view emails in "Plain Text", which will restrict link functionalities and other unnecessary, but potentially dangerous, features in emails. If possible, choose "plain text" in your email viewing options.
- **Apply additional security practices** - You may be able to filter certain types of attachments through your email software (see Reducing Spam) or a firewall (see Understanding Firewalls).

The National Cybersecurity and Communications Integration Center (NCCIC) encourages the public to use safe, common sense cyber practices, such as not opening emails from unknown individuals or organizations, using spam filters and firewalls, running anti-virus and anti-spyware software and keeping them updated regularly. For more information regarding computer security, visit the United States Computer Emergency Readiness Team (US-CERT) www.us-cert.gov or the Federal Bureau of Investigation's (FBI) 'Be Crime Smart' website at:

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

POINTS OF CONTACT

Please direct questions concurrently to the NCCIC and/or its appropriate component listed below:

NCCIC	US-CERT	NCS/NCC	ICS-CERT
NCCIC@HQ.dhs.gov	SWO@US-CERT.gov	NCS@HQ.dhs.gov	ICS-CERT-SOC@dhs.gov
(703) 235-8831	(703) 235-8832/8833	(703) 235-5080	(877) 776-7585