

Privacy and Security Newsletter



DHS Information Security Office

January 2009

In this issue:

- Phishing: Hook, Line, & Sinker
- Managing and logging files
- Online training
- New ISO staff member
- Tip: Transporting confidential information
- Top reported incidences, 4th qtr
- ISO contacts

Introductions



The DHS Information Security Office is pleased to announce the appointment of Linda Kilgore as the Awareness and Education Program Manager. Linda joined the Information Security Office (ISO) in November, 2008. She has been with DHS since March, 2000.

Linda has a Master's Degree in Education and has worked in various school, government, and private organizations providing education, communication, and multimedia services.

Contact Linda at: (503) 945-7004 or linda.j.kilgore@state.or.us.

Hook, Line, and Sinker

Phish on! "Your computer may be infected by a virus!" "To speed up your computer, click here." "Your account is about to be deactivated, click here to prevent this." These are just some examples of common — and printable— phrases used to bait you into visiting a fraudulent website.

What is phishing and social engineering?

Social engineering is the broad term used to describe the act of manipulating you into divulging confidential information or performing an action that compromises security. These acts may be performed in person, over the phone, through e-mail, or the Internet. Phishing is a form of social engineering specific to the use of e-mail and the Internet to obtain confidential information or to gain access to computer systems.

Check your phishing IQ? Try the quiz at:
<http://www.sonicwall.com/phishing>

What do I look for?

In a typical scenario, a phisher sends an e-mail that appears to come from a legitimate business — the government, a bank, a credit card company — requesting verification of information and warning of some dire consequence if it is not provided. The e-mail usually contains a link to a fraudulent web page that appears authentic.

Once your computer is infected, you may experience the following symptoms:

- Your computer suddenly becomes sluggish or freezes frequently;
- You see pop-up advertisements all the time, even when you aren't browsing the Internet;
- Your browser home page is reset to something you did not expect;
- Settings on your computer may have changed and cannot be changed back to how they were;

How do I avoid being a victim?


- Delete it. Be suspicious of unsolicited e-mail and do not open it. Opening a spam e-mail confirms to the sender that the e-mail address is valid.
- Close it. Never click on a pop-up advertisement in a browser window. The best method to close a window is to use the combination of **Alt+F4** on your computer keyboard. No clicking!

TIP

When mailing confidential documents:

- Place items in a sealed envelope;
- Include complete mailing addresses for **both** the recipient and return addresses to include: name, address, building/suite/floor, city, state, zip code;
- Keep an accurate log for checking documents in and out;
- Ship items using a carrier who provides package tracking and security.

Note: For offices on the DAS Shuttle mail route, save money using [PacTrac](#)

- Protect it. Never provide personal or protected information about you or your organization in response to unsolicited e-mail. Directly verify the identity and authority of the sender.
- Be observant. Before sending secure information over the Internet, note whether the web address is secure. Check for the “lock” icon  in your browser’s status area in the lower right corner of the browser window. Also check that the web address of the page begins with **https://**.
- Never install unauthorized software on your work computer. Many downloaded software programs also install additional malware without your knowledge.

Additional reading:

<http://www.oregon.gov/DHS/admin/infosec>

<http://www.microsoft.com/protect/yourself/phishing>

What should I do if I need help?

If your work computer displays any of the symptoms listed above, contact the OIS Service Desk at 503-945-5623.

TOP REPORTED INCIDENTS

The top two privacy and security incidents reported to our office in the 4th quarter of 2008 were:

- Lost client files
- Stolen laptops and mobile devices

Managing and logging files

We all know the frustration of trying to stay afloat amidst a torrent of documents. When multiple people divide work between offices it sometimes is difficult to keep track of where a file lives. Consider the following suggestions:

- Develop a system where client files are logged in and out when being transported;
- Keep your desk organized;
- Work on one client file at a time;
- Take care when placing documents in a folder and as you file the folder in a cabinet to ensure they are in the correct place.
- Include the *complete* mailing address and return address on ALL mailed or shuttled packages.

Refer to policy [DHS-090-010](#) regarding “Transporting Information Assets” for guidance on:

- Logging packages;
- Packing and addressing items correctly;
- Storing items securely while in-transit;
- Reporting incidents when items are lost or exposed.

TO REPORT AN INCIDENT

[Privacy Program](#), (503) 945-5780
[Security Program](#), (503) 945-6812

Look-up all [ISO and Privacy Review Committee contacts](#) on our website.

Online Training

The ISO has online training classes available to all DHS employees. Visit the [DHS Learning Center](#) to register.

Course list:

- Privacy, Security, DHS and You - Part 1
- Privacy, Security, DHS and You - Part 2
- Information Security Misdirected E-mail