PNNL-SA-54316

Application for
The Northwest Academic Computing Consortium
Joanne R. Hugi Excellence Award

Cyber Security Awareness Training

Pacific Northwest National Laboratory
IT Services Division

Abstract:

The weak link in maintaining a reasonably secure computing environment is the human factor. Pacific Northwest National Laboratory (PNNL) has endeavored through a number of initiatives to raise the awareness of cyber security issues and challenges both at work and at home. Elements of the multi-faceted awareness and education program include on-line training (mandatory for all staff and extended-stay visitors), posters, postcards, and newsletters. The program has had measurable impact reducing, for example, PNNL's vulnerability to "phishing" attacks.

Description of the Practice:

To meet our client's expectations and industry best practices, PNNL staff members have developed a multi-layered approach with cyber security awareness training. This approach provides staff development, policy awareness, and, most importantly, protection of our information. The awareness training consists of an online annual training course, directed paper products, and electronic communications products.

Annual Cyber Security Awareness Training

The training course is given to all new hires as part of their initial orientation and annually to each staff member. The training is offered as an interactive online course that features an animated robot named "Cybot" (Figure 1). The course is meant to be both educational and entertaining. It is fairly traditional in nature in that it walks the learner through several pages of content regarding such topics as malware awareness, appropriate uses of computing resources, and password management. However, unlike common read-content-and-answer-questions methods, our training uses interactive exercises to ensure that the content is understood. For example, to recognize spam or phishing messages, the learner is taken to a mock email inbox where several messages are available (Figure 2). The learner may open or delete messages just as with a real email inbox. Instead of just reading about what to do, learners see and can try out the lesson content before they are confronted with the situation in their own email inbox.

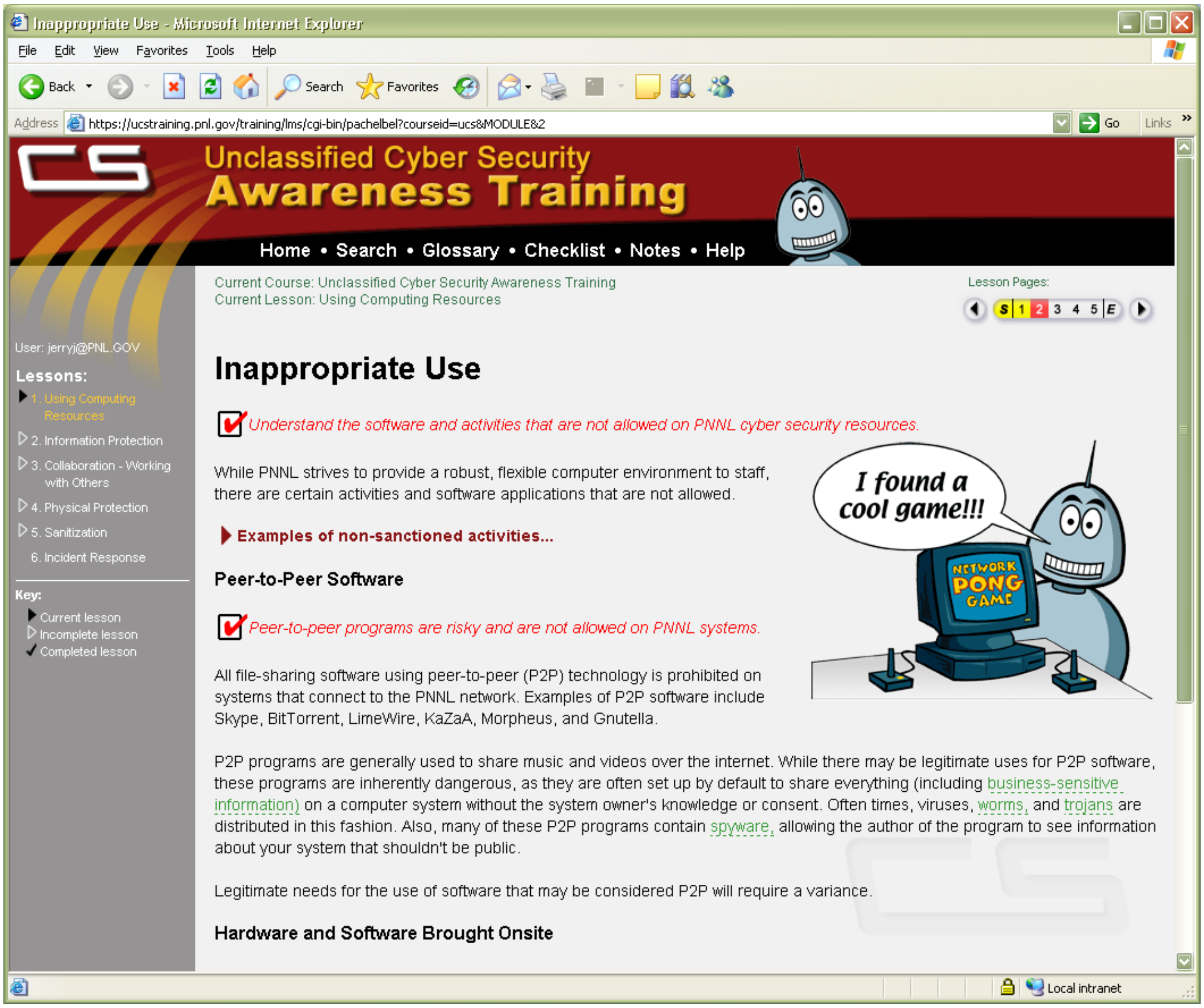
Directed Paper Products

Directed paper products include flyers, posters, and postcards. The flyers or newsletters (Figure 3) are traditional for those who expect that method but the posters and postcards are not. The postcard (Figure 4) is mailed to each staff member and is a two-sided format with a graphical image on one side and text on the other. The artwork has consisted of images pertaining to cyber security issues such as phishing, peer-to-peer software, and cleaning data off of hard drives before transferring equipment. There is also a matching poster (Figure 5) placed in PNNL common-areas, such as copy centers and lunch rooms.

Electronic Communications Products

Electronic communications include directed emails, online PNNL staff newsletter, and online IT Services newsletter. Emails and newsletter items have included such issues as phishing, spam, not sending sensitive information to shared printers, and peer-to-peer software. A few examples of content that sent in a semi-weekly news email are:

- **"E-mail spoofing on the rise**. Have you ever received an e-mail that appeared to be from yourself that you have no recollection of sending? You may be a victim of e-mail spoofing — the forging of e-mail so it appears to originate from someone other than the source. It allows the real sender to attempt to trick the recipient into reading and responding to mail they would otherwise ignore. Staff members recently have seen a rise in these e-mails, which often contain "5556" in the e-mail header or body. The best thing to do is delete the message."
- **"Wireless home network security**. A wireless home network is ideal for a household with multiple computers that access the internet or a single printer. However, if you use a wireless firewall/router for your home network, note that attackers could exploit a variety of security holes that are common with wireless firewall/routers. To help keep your wireless home network safe, we recommend you take these precautions: keep your wireless firewall/router firmware up-to-date, use a strong password, disable wireless access to the router settings and use WEP encryption."


Inappropriate Use - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
https://ucstraining.pnl.gov/training/lms/cgi-bin/pachelbel?courseid=ucs&MODULE&2
Go
Links
Unclassified Cyber Security
Awareness Training
Home • Search • Glossary • Checklist • Notes • Help
Lesson Pages:
S 1 2 3 4 5 E
I found a cool game!!!
NETWORK PONG GAME
Local intranet

Current Course: Unclassified Cyber Security Awareness Training
Current Lesson: Using Computing Resources

User: jerryj@PNL.GOV

Lessons:

1. Using Computing Resources
2. Information Protection
3. Collaboration - Working with Others
4. Physical Protection
5. Sanitization
6. Incident Response

Key:

- Current lesson
- Incomplete lesson
- ✓ Completed lesson

Inappropriate Use

☑ *Understand the software and activities that are not allowed on PNNL cyber security resources.*

While PNNL strives to provide a robust, flexible computer environment to staff, there are certain activities and software applications that are not allowed.

Examples of non-sanctioned activities...

Peer-to-Peer Software

☑ *Peer-to-peer programs are risky and are not allowed on PNNL systems.*

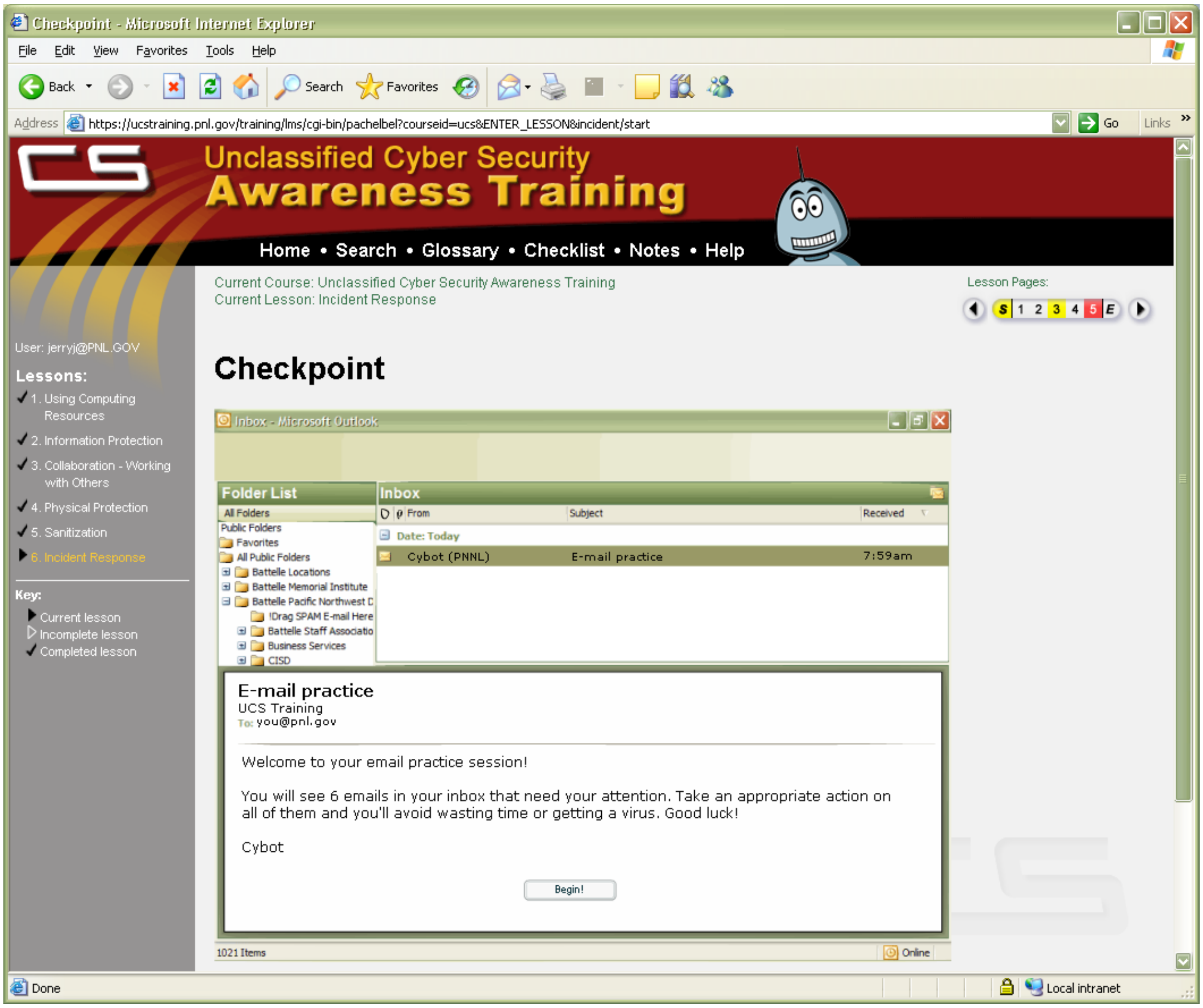
All file-sharing software using peer-to-peer (P2P) technology is prohibited on systems that connect to the PNNL network. Examples of P2P software include Skype, BitTorrent, LimeWire, KaZaA, Morpheus, and Gnutella.

P2P programs are generally used to share music and videos over the internet. While there may be legitimate uses for P2P software, these programs are inherently dangerous, as they are often set up by default to share everything (including business-sensitive information) on a computer system without the system owner's knowledge or consent. Often times, viruses, worms, and trojans are distributed in this fashion. Also, many of these P2P programs contain spyware, allowing the author of the program to see information about your system that shouldn't be public.

Legitimate needs for the use of software that may be considered P2P will require a variance.

Hardware and Software Brought Onsite

Figure 1. All employees and extended-stay visitors are required to complete annual Unclassified Cyber Security Awareness Training. The training is offered as an interactive online course.


Checkpoint - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
Home • Search • Glossary • Checklist • Notes • Help
Lesson Pages:
S 1 2 3 4 5 E
Inbox - Microsoft Outlook
Folder List
Inbox
Begin!
Done
Local intranet

https://ucstraining.pnl.gov/training/lms/cgi-bin/pachelbel?courseid=ucs&ENTER_LESSON&incident/start

Unclassified Cyber Security Awareness Training

Current Course: Unclassified Cyber Security Awareness Training
Current Lesson: Incident Response

User: jerryj@PNL.GOV

Lessons:

- ✓ 1. Using Computing Resources
- ✓ 2. Information Protection
- ✓ 3. Collaboration - Working with Others
- ✓ 4. Physical Protection
- ✓ 5. Sanitization
- ▶ 6. Incident Response

Key:

- ▶ Current lesson
- ▷ Incomplete lesson
- ✓ Completed lesson

Checkpoint

All Folders
Public Folders
Favorites
All Public Folders
Battelle Locations
Battelle Memorial Institute
Battelle Pacific Northwest D
!Drag SPAM E-mail Here
Battelle Staff Associatio
Business Services
CISD

From	Subject	Received
Date: Today		
Cybot (PNNL)	E-mail practice	7:59am

E-mail practice
UCS Training
To: you@pnl.gov

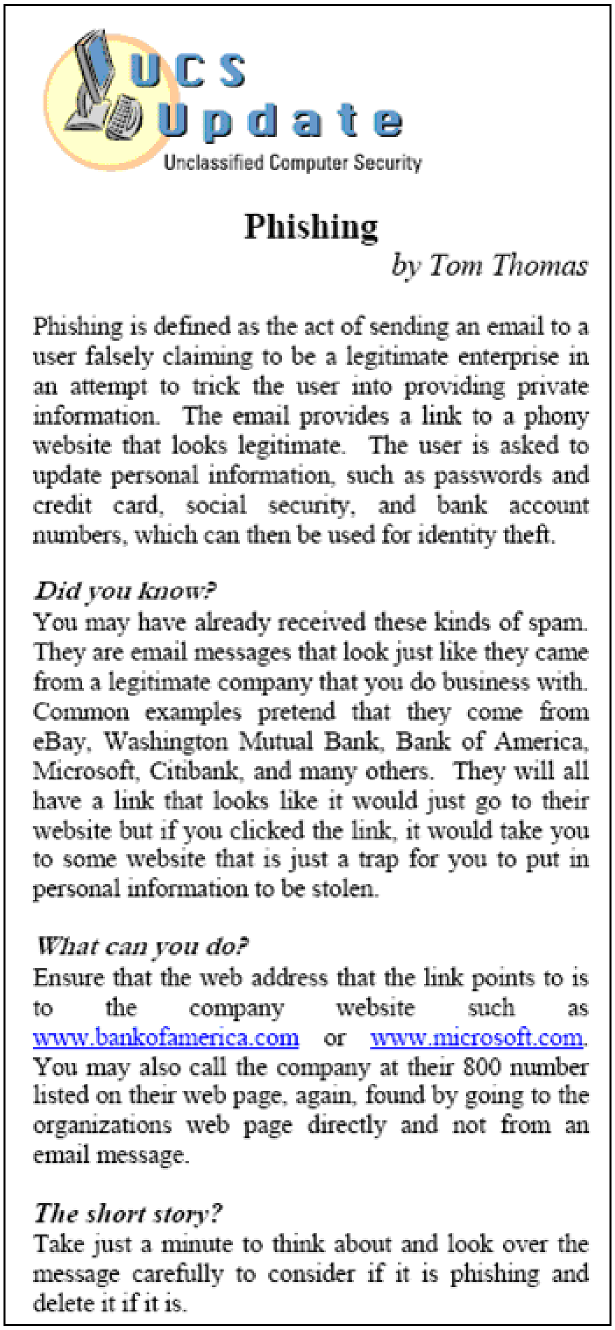
Welcome to your email practice session!

You will see 6 emails in your inbox that need your attention. Take an appropriate action on all of them and you'll avoid wasting time or getting a virus. Good luck!

Cybot

1021 Items
Online

Figure 2. The Unclassified Cyber Security Awareness Training course includes interactive exercises that teach how to identify common cyber security threats.



UCS Update
Unclassified Computer Security

Phishing

by Tom Thomas

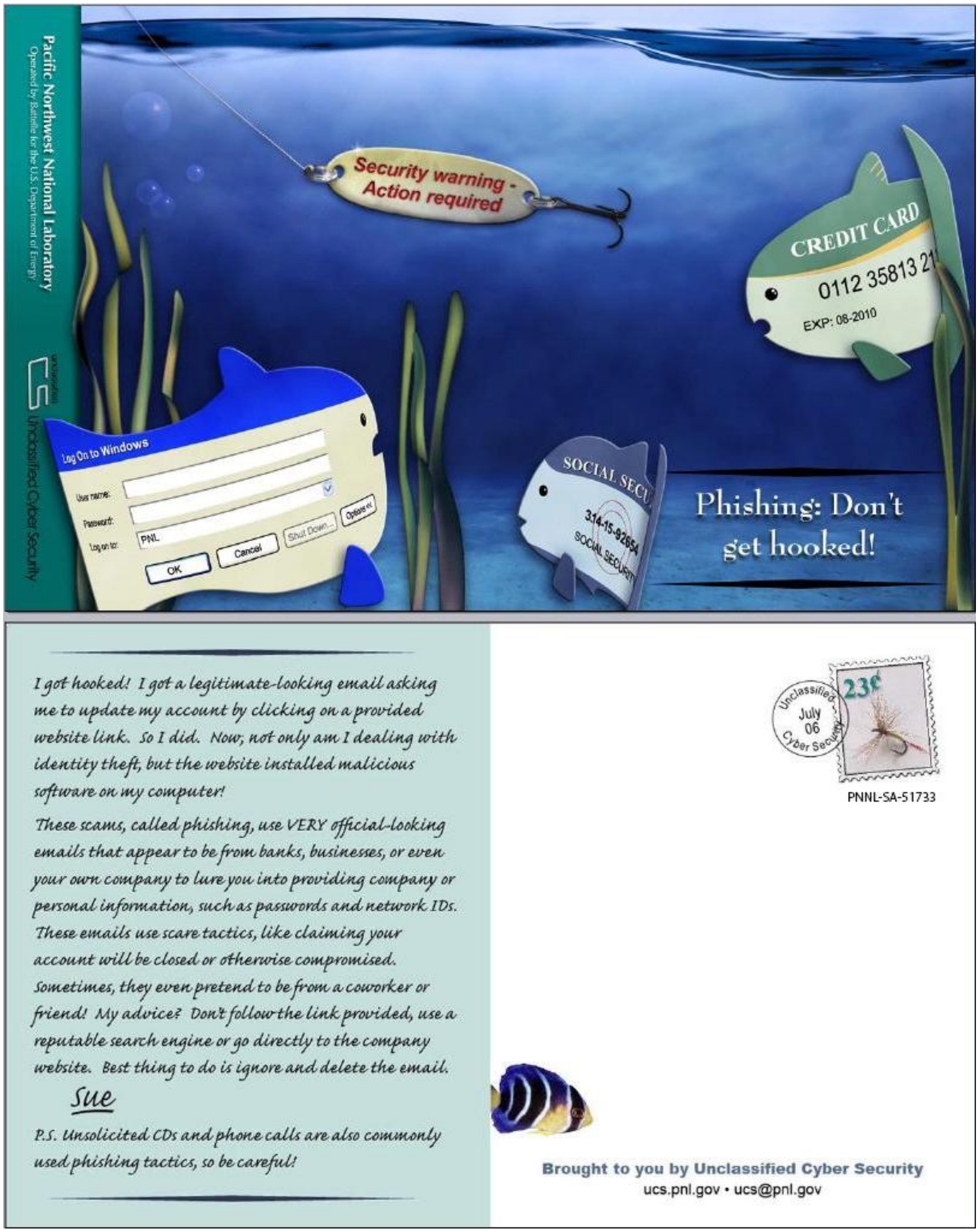
Phishing is defined as the act of sending an email to a user falsely claiming to be a legitimate enterprise in an attempt to trick the user into providing private information. The email provides a link to a phony website that looks legitimate. The user is asked to update personal information, such as passwords and credit card, social security, and bank account numbers, which can then be used for identity theft.

Did you know?
You may have already received these kinds of spam. They are email messages that look just like they came from a legitimate company that you do business with. Common examples pretend that they come from eBay, Washington Mutual Bank, Bank of America, Microsoft, Citibank, and many others. They will all have a link that looks like it would just go to their website but if you clicked the link, it would take you to some website that is just a trap for you to put in personal information to be stolen.

What can you do?
Ensure that the web address that the link points to is to the company website such as www.bankofamerica.com or www.microsoft.com. You may also call the company at their 800 number listed on their web page, again, found by going to the organizations web page directly and not from an email message.

The short story?
Take just a minute to think about and look over the message carefully to consider if it is phishing and delete it if it is.

Figure 3. A topical cyber security awareness campaign often begins with traditional newsletter articles or flyers. Shown: Sidebar article on “phishing” that was included in a quarterly general security newsletter.


Pacific Northwest National Laboratory
Operated by Battelle for the U.S. Department of Energy
Unclassified Cyber Security
Security warning - Action required
CREDIT CARD
0112 35813 21
EXP: 08-2010
Log On to Windows
User name:
Password:
Log on to:
PNL
OK
Cancel
Shut Down...
Options <<
SOCIAL SECU
314-15-92654
SOCIAL SECURITY
Phishing: Don't get hooked!
Unclassified July 06 Cyber Security
23¢

I got hooked! I got a legitimate-looking email asking me to update my account by clicking on a provided website link. So I did. Now, not only am I dealing with identity theft, but the website installed malicious software on my computer!

These scams, called phishing, use VERY official-looking emails that appear to be from banks, businesses, or even your own company to lure you into providing company or personal information, such as passwords and network IDs. These emails use scare tactics, like claiming your account will be closed or otherwise compromised. Sometimes, they even pretend to be from a coworker or friend! My advice? Don't follow the link provided, use a reputable search engine or go directly to the company website. Best thing to do is ignore and delete the email.

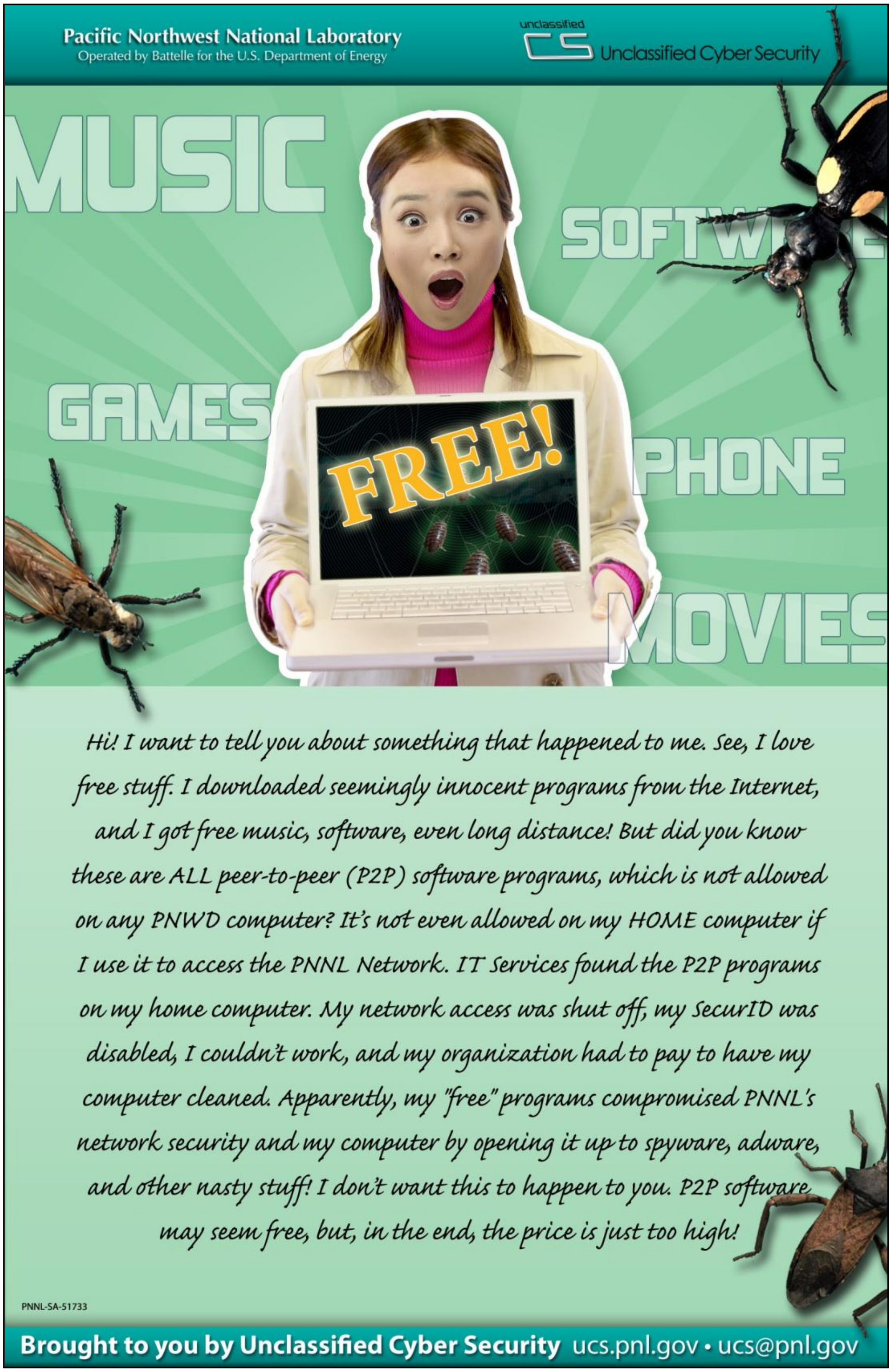
Sue

P.S. Unsolicited CDs and phone calls are also commonly used phishing tactics, so be careful!

PNNL-SA-51733

Brought to you by Unclassified Cyber Security
ucs.pnl.gov • ucs@pnl.gov

Figure 4. Awareness campaigns also include postcards distributed to staff through the plant mail service. Shown: Example of a postcard warning about phishing.



Pacific Northwest National Laboratory
Operated by Battelle for the U.S. Department of Energy

unclassified CS Unclassified Cyber Security

Hi! I want to tell you about something that happened to me. See, I love free stuff. I downloaded seemingly innocent programs from the Internet, and I got free music, software, even long distance! But did you know these are ALL peer-to-peer (P2P) software programs, which is not allowed on any PNWD computer? It's not even allowed on my HOME computer if I use it to access the PNNL Network. IT Services found the P2P programs on my home computer. My network access was shut off, my SecurID was disabled, I couldn't work, and my organization had to pay to have my computer cleaned. Apparently, my "free" programs compromised PNNL's network security and my computer by opening it up to spyware, adware, and other nasty stuff! I don't want this to happen to you. P2P software may seem free, but, in the end, the price is just too high!

PNNL-SA-51733

Brought to you by Unclassified Cyber Security ucs.pnl.gov • ucs@pnl.gov

Figure 5. Posters placed in common areas such as break rooms and copy centers reinforce the current awareness campaign. Shown: Poster warning about peer-to-peer software.

Responses to Evaluation Criteria:

Innovation

Typical cyber security training, if there is any at all, is a one-time, read-content-and-answer-questions training course. This format addresses only the first two categories of Bloom’s taxonomy of educational objectives: knowledge and comprehension.[1] PNNL has gone beyond the norm for cyber security training by not only implementing a multi-faceted awareness program, but by incorporating Bloom’s third objective—application—into our interactive on-line training class.

Key elements of innovation are:

- Multi-faceted cyber security awareness program that includes interactive on-line training, directing mailings and posters, and frequent electronic communications.
- On-line cyber security training is both educational, and through incorporation of an animated character, entertaining. Unlike most policy/procedure training, staff report that they actually enjoy the class.
- On-line cyber security training incorporates exercises that don’t just test comprehension of the readings, but application in practical and realistic situations.
- On-line training implemented using Pachelbel© – PNNL’s own SCORM 1.2 conformant learning management system. Course content can be exported as SCORM-conformant packages.

Benefits

PNNL conducts contract research for a broad number of government and commercial institutions. The research conducted ranges from open science to company proprietary to national security related. The beneficiaries of PNNL’s cyber security awareness training program are our clients and partners, whose information we are entrusted to protect, and PNNL, which is able to attract and retain these customers by demonstrating a trustworthy computing environment.

Technical cyber security controls such as firewalls, intrusion detection, active patching, and virus scanners are critically important to the protection of information and information resources. However, these controls are only partially effective, and the human factor must also be considered. Users make mistakes and can override controls. New threats may not yet be recognized by firewalls, intrusion detectors, vendor patches, or virus scanners. Making users aware of these threats is an essential element of an effective cyber security defense.

PNNL’s user awareness program has had measurable impact. For example, PNNL had a less than 1% response to a phishing message generated by a recent security review team, compared to 15% or greater response typical in other organizations.[2,3]

Replicability

Our multi-faceted approach can easily be replicated by other institutions. The posters and postcards have been released for public use, as has a booklet that provides computer security training for home users (see Links below). The on-line awareness training course is copyrighted. It is available at no cost to U.S. federal government agencies and contractors, and can be licensed to others. The course is uses PNNL’s Pachelbel© e-Learning Content Development and Management System. Pachelbel is a SCORM

[1] Bloom, BS, and DR Krathwohl. *“Taxonomy of Educational Objectives: The Classification of Educational Goal.”* in Handbook I: Cognitive Domain. Longmans, Green, New York, 1956.

[2] Dhamija R, JD Tygar, and M Hearst. 2006. “Why Phishing Works.” In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems 2006,* pp 581-590, April 22–27, 2006, Montréal, Québec, Canada.

[3] Bank D. August 17, 2005 “’Spear Phishing' Tests Educate People About Online Scams,” *The Wall Street Journal.*

1.2 conformant learning management system. Course content can be exported as SCORM-conformant packages.

Costs

Resources in staff time in creating, maintaining, and distributing the content are used at about a third of a full time staff member. Web servers and paper are also used to distribute the content. However, the servers are shared with other projects and the paper averages about eight sheets of standard weight paper and three sheets of card stock per staff member per year.

The training is cost-effective in that it satisfies our client's and partner's requirements and meets best business practices for cyber security awareness training. This allows our organization to retain existing contracts and attract new business. While it is difficult to accurately measure the average loss per cyber security event, it is expensive to perform the forensics and repair, if not replacement, necessary to return a previously compromised system to the network. Lost information from lost or stolen laptops could also prove to be very expensive. Awareness training that prevents just a few events a year and reduces overall risk to the information we are entrusted with, at our current budgeted levels, is considered cost effective by our management.

Links

Mahan RE. 2005. Guide for Home Computer Security. PNNL-SA-44008.
[Available online at http://www.pnl.gov/media/homeguide_public.pdf]

Thomas TC. 2006. Unclassified Cyber Security (UCS) posters and postcards. PNNL-SA-51733.
[Available upon email request to tom.thomas@pnl.gov]

Pachelbel© e-Learning Content Development and Management System:
http://www.pnl.gov/cogInformatics/pachelbel.stm

Principal Contact:

Tom Thomas
tom.thomas@pnl.gov
509-375-6876

Other Key Contributors:

Andrew Korson, Cyber Security Program Manager
andrew.korson@pnl.gov

Nathan Johnson, Graphics (posters, postcards)
nathan.johnson@pnl.gov

Darcy Short, Editor (email, posters, postcards)
darcy.short@pnl.gov

Jennifer Irlam, Editor (newsletter articles)
jennifer.irlam@pnl.gov

Sharon Eaton, Editor (UCS Awareness Training)
sharon.eaton@pnl.gov