2009 FISSEA Entry Form

Name of submitter: David Kurtz

Organization: U.S. Department of the Treasury, Bureau of the Public Debt (BPD)

Type of entry: Website

Title of Entry: BPD Monthly Security Reminder

Description of Entry: Near the start of each month, a brief security reminder is posted on the BPD intranet (PDWeb). Written by the OIT Security Analysis Branch, it provides yet another venue for our multi-faceted security awareness program. Although each month's reminder gets its own page on PDWeb, our intranet "Security Zone" pages (the location for all of our branch's intranet presence) provide an archive directory of previous monthly security reminders for employees to reference at any time. This practice has been in place since 2001, so we have quite an archive of useful monthly security reminders.

PDWeb's homepage (which employees see upon start-up each day) always shows the title of whatever intranet webpage has been posted that day (and the previous few days), under a prominent banner entitled "What's New on PDWeb." It is important to have an intriguing title to promote readership, and June 2008 provides a good example of one of our monthly security reminders.

In this particular month, the dangers of social networking websites is discussed. Facebook, LinkedIn, and other such services have seen incredible growth this past year, and we wanted to highlight some security concerns related to Public Debt. Other topics this past year included password storage, tales of USB drives lost and found, true stories of employee virus experiences, etc.

Please note that when it comes to website design, we have to abide by the prerequisites for PDWeb. Thus, our monthly security reminder webpages, while providing interesting tidbits of security awareness, may not dazzle judges for their use of graphics, animation, video, etc. We merely provide the written text each month to the group which controls PDWeb. However, these intranet webpages have proven to be a popular way to inculcate our employees with an appreciation for good security practices.

Page 3 shows an example of the PDWeb Homepage, although from February, since June was no longer available. As you can see, the monthly security reminder is displayed prominently. Employees know that a simple click will lead them to a quick and educational story about security (in February, it was an employee telling her story of a virus incident at home).

Security Reminder - June 2008

Social Networking/Social Engineering

Many of you are familiar with the growth of social networking websites, which are designed to easily allow people to share their lives and interests by creating an on-line profile and connecting with all their friends. MySpace and Facebook are two of the best known, but there are plenty of others, such as Xanga, Orkut, Hi5, LinkedIn, Plaxo, Bebo, Google Talk, Yahoo 360, and the like.

Some of you may have already joined one of these sites. If so (or if you're considering doing so), please be cautious. There are legitimate concerns about users giving out too much personal information. Not only is this dangerous from an identity theft perspective, it can also provide valuable information to someone trying to harm Public Debt.

Attackers use a tactic called "social engineering" when they're crafting phishing messages and other attacks. They try to put you at ease and then convince you to do things that are not safe (for example, share passwords, provide insider information, visit virus-laden websites, etc). The more that social engineers know about you, the easier their job becomes. Some of you may recall the "Jack Scanlon" video we always show in the End User Basic Computer Security class, which shows a successful social engineer at work.

Be discreet about sharing work-related information on-line. The less said about your work, the better. If you identify your place of work as Public Debt, you should be extra cautious about providing information about our facility, your job responsibilities, whom you work with, contact information at work, and the like. Such information could be useful to someone with the goal of hacking into our systems.

PDWeb - Windows Internet Explorer

http://ntpdweb/oa/pdwebmain.htm

Scandoo

File Edit View Favorites Tools Help

PDWeb

Page Tools

PDWeb
YOUR BUREAU RESOURCE





Local Weather
» Parkersburg, WV
» Washington, DC

ARC COMM GSRS PLAS OCC OF OIT OMS OPDA RETAIL WSS

EMPLOYEE RESOURCES | MISSION, VISION, & VALUES | REPORTS, STATISTICS, & METRICS | RULES, REGS, & POLICIES | TOOLS & SERVICES

Search PDWeb GO

Quick Links

- Web Phone
- Applications
- WebTA
- Values
- NFC Employee Personal Page
- BPD Enterprise Architecture
- IT Security
- TreasuryDirect.gov
- Public Debt Online
- Treasury Intranet
- Ethics
- NTEU

What's New

News Archive

February 3, 2009
Security Reminder - February 2009: She Didn't Fall for It!

January 30, 2009
OPDA Wire - the Newsletter of the Office of Public Debt Accounting: Read about the newest employees in OPDA in the January issue of OPDA Wire!

January 28, 2009
Diversity Committee Home: Read about upcoming activities and new leadership.

Public Debt Selected as Shared Service Center (SSC) for Information Security Systems Line of Business (ISSLOB)

January 27, 2009

Unknown Zone (Mixed) 100%

start David Kurtz... 2 Microso... Microsoft P... PDWeb - Wi... 11:00 AM