IT Defender

From the OIM Information Security Program

February 2011

Issue 3

Inside this issue:

Report an Incident

If you suspect lost, misplaced or stolen equipment or a breach of Personally Identifiable Information (PII), contact the FDA IT Security Operations Center (SOC) at:

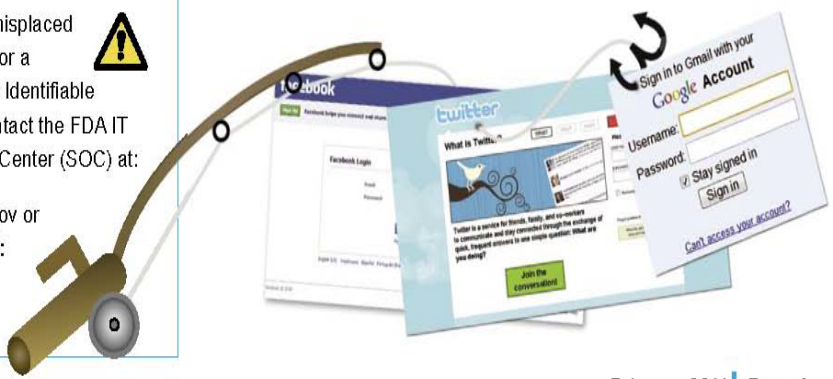
- **Email:** soc@fda.gov or
- **Toll Free Number:** 855-5FDA-SOC (855-533-2762)

What is phishing?

Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. When users respond with the requested information, attackers can use it to gain access to the accounts.

Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as

- Natural disasters (e.g., Haiti earthquake, Hurricane Katrina)
- Epidemics and health scares (e.g., H1N1)
- Economic concerns (e.g., IRS scams)
- Major political elections
- Holidays (e.g., e-cards)



How to spot a phishing email...

It could be a phishing email if..

■ There are misspelled words in the email or it contains poor grammar.

■ The message is asking for personally identifiable information (PII), such as credit card numbers, account numbers, passwords, PINs or Social Security Numbers.

■ There are threats or alarming statements that create a sense of urgency. For example: Your account will be locked until we hear from you or we have noticed activity on your account from a foreign IP address.

■ Be aware of emails that try to get your attention by using all capital letters, especially in the subject line. Using all caps has long been viewed as online shouting. The authors of scam emails tend to write prose that is over-the-top and very emotional.

■ The website address in the message isn't the one you're used to seeing. It's usually close to the real domain name but not exact.

Phishing website: *www.citibanking.com*

Real website: *www.citibank.com*

■ If it is a legitimate email from a business, it will be signed with a person's name and contact information, but if it signs off with something vague, such as Customer Support, be wary.

Did you know?

■ According to Cisco, 800 million spear phishing emails are sent each day with those numbers continuing to rise.

■ On average, financial organizations lose around $1000 every time one of their customers falls for a phishing attack.

■ According to McAfee, 95% of phishing emails pretend to be from Amazon, eBay, or banks.

How to protect yourself from Phishing attacks

■ Be suspicious of unsolicited phone calls, visits, or emails asking about employees or other internal information.

■ Do not reveal or respond to email requests for personal information.

■ Dispose of valuable, sensitive, or proprietary information appropriately.

■ Do not provide passwords, personal, or Department information unless you are certain of the person's authority to have the information.

Reporting Phishing Emails at the FDA

If you receive emails that you think are suspicious, please contact the ERIC IT Helpdesk.

http://inside.fda.gov:9003/EmployeeResources/

Think you have been scammed?

- If you believe your personal accounts have been compromised, contact the appropriate institution immediately (e.g., bank or credit card company) and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
- File a report with the Federal Trade Commission at *www.ftc.gov*
- You also may report phishing emails to *reportphishing@antiphishing.org*. The Anti-Phishing Working Group, a consortium of ISPs, security vendors, financial institutions and law enforcement agencies, use these reports to fight phishing.
- For more information on Phishing, see links below:
  - *http://www.sophos.com/security/best-practice/phishing.html*
  - *http://www.onguardonline.gov/topics/phishing.aspx*

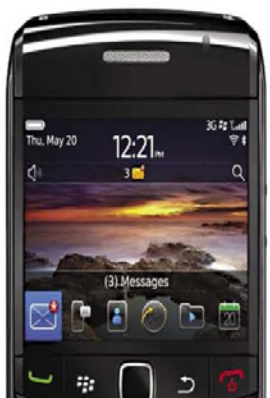
Note: Some of the Phishing content was provided/produced by US-CERT, a government organization.

TIPS

- Never respond to requests for personal information via email.
- Do not follow web links in email messages.
- Do not open attachments. Only open the attachment if the authenticity has been verified.
- Phishing emails usually do not address the recipient by name.
- Make sure to double-check urls before typing in any personal information. Make sure the website uses authentication (usually shown as https in the address bar.) Look for a closed padlock in the web browser's status bar.

What is the FDA Alert System?

FDA Alert System (FDA AS) is a communications service that connects people instantly anytime, anywhere, across any device – cell phone, home phone, work phone, email, or pager. The FDA AS is built on the Send Word Now subscription service which provides high capacity, on-demand emergency notification services. This subscription service allows you to send high volumes of simultaneous alerts to a pre-defined group or to selected individuals from a group via common voice and text-based communications.



How is FDA using it?

It has been used to support the Information and Computing Technologies for the 21st Century Program migration, Office of Information Management (OIM) outages and during the wind storm in July 2010 when electrical outages plagued FDA and the metropolitan area for days. The OIM staff was able to quickly assemble key OIM response teams on Sunday to address FDA IT outages.

The Planning & Disaster Recovery (PDR) team continues to improve the FDA AS and FDA's emergency response communications. The Center for Veterinary Medicine recently initiated the service with over 500 users added to the system. Also, the PDR team is exploring the integration with EASE, Active Directory or another directory service to automate new user additions, employee updates and user exits.

For additional information on the FDA AS, please visit the FDA IT security web pages and click the FDA Alert System (FDA AS) link in the IT Security PDR tab:

http://inside.fda.gov:9003/it/ITSecurity/SecurityOverview/ucm220704.htm#soHeader

Raffle Winners

Dynna Bigby (OC)

Steve Donald (CDER)

Clarise Thompson (CTP)

Manashi Dey (CFSAN)

FDA's Celebration of National Cyber Security Awareness Month

October 2010 marked the seventh annual National Cyber Security Awareness Month. Several members of the OIM Information Security Program focal areas including Policy & Awareness, Planning & Disaster Recovery, Risk & Compliance and Center Information System Security Officers (ISSO's) participated in a series of events to introduce the team and promote security awareness.

Team members visited four locations including White Oak and offices where Center's including CTP, CDER, CVM and CFSAN are located, showing users security videos on protecting themselves against scams and ID theft, where to locate information security policies and security awareness information on the internal website and more. Users also left the event with useful materials including our quarterly newsletter "IT Defender", FTC publications on social media and teaching children and teens about internet safety, and fun giveaways with security tips including fortune cookies, pens, flashlights and notepads.

Users answered security awareness questions and learned new information such as who their Center ISSO and FDA Chief Information Security Officer (CISO) were for a chance to enter a raffle and win one of four iPod shuffles. It was also a great opportunity to remind users to complete their annual Online Security Awareness Training and answer questions about user's security concerns. Promoting security awareness is an important initiative year round and the team plans to take lessons learned from the events to identify other ways to provide awareness across FDA.

David Alston, Mechelle Munn, Carol Davis, Sara Fitzgerald, Mo Moore pictured above at the event held at the CFSAN location.

Note: All of the FTC publications can be ordered free to share with peers at the following link: http://bulkorder.ftc.gov/

If you have any questions, comments or suggestions on topics to include in future newsletters, please contact...

ITSecurityAwareness@fda.hhs.gov