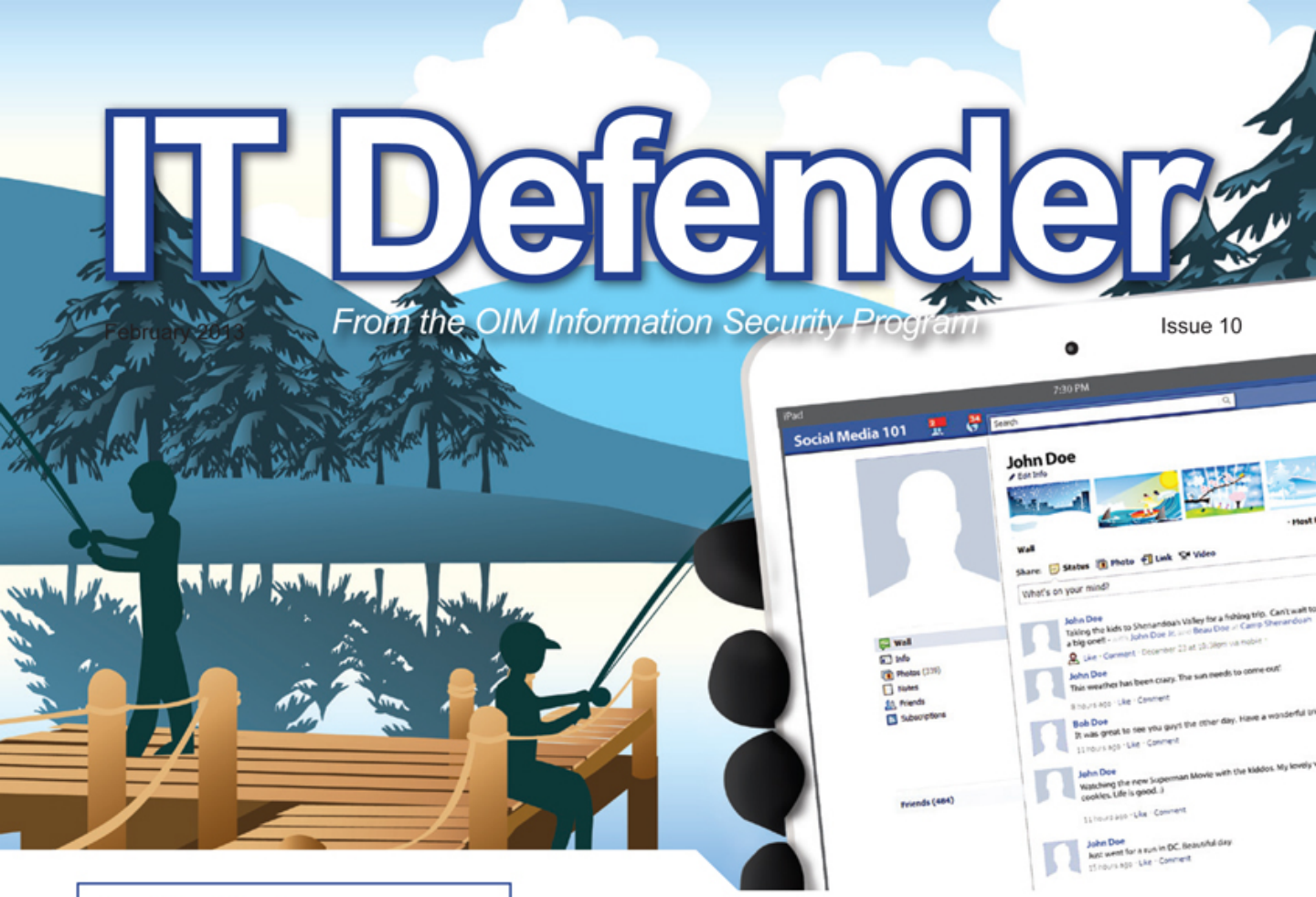
IT Defender

From the OIM Information Security Program

February 2013 Issue 10



Inside this issue:

Report an Incident

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

- **Email: SecurityOperationsandResponse@fda.hhs.gov** or
- **Toll Free Number:** 855-5FDA-SOC (855-533-2762) (24x7)

Cyber Threats on the Internet and Social Media Sites

Cyber-crime costs individuals, businesses, and government agencies billions of dollars every year. An estimated 11.7 million Americans were victims of identity theft and other cyber/internet related crimes.

A recent Federal Bureau of Investigation report stated that "identity theft has emerged as a dominant and pervasive financial crime that exposes individuals and businesses to significant losses and undermines the credibility and operation of the entire U.S. financial system."

Protecting your personal information, privacy, and reputation on the internet is challenging. Online services that allow social networking and work collaboration are also exploited by cyber criminals, hactivists, and foreign governments.

Target sites include online banking, social media sites, professional organizations, private companies and government organizations. Personal information shared online can include personal email address, cell phone number, location, where you work, and photos.

Things You Can Do to Protect Yourself on the Internet

- Be alert, aware and/or limit your personal exposure online *(i.e. shopping, LinkedIn, Facebook, professional forums, blogs)*
- Seek assistance or advice from your Center Information Systems Security Officer (ISSO)

Cyber Threats on the Internet and Social Media Sites continued...

- Avoid opening suspicious emails *(i.e. spam, phishing)*
- Regularly complete cyber security training and read IT security news stories
- Use and update IT security software, and monitor your credit reports for unauthorized activity
- To learn more, government agencies that provide identity theft awareness include: DOJ, FBI, DHS, NIST ■

Helpful Links

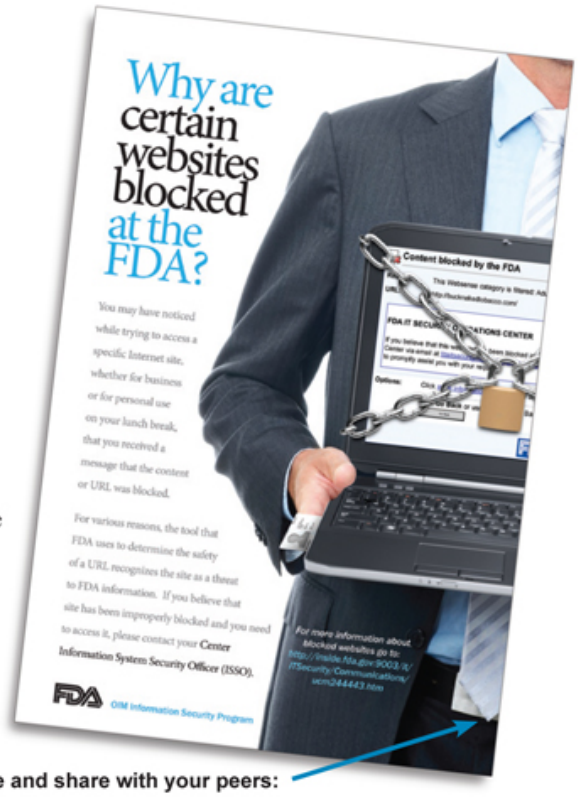
- *www.ftc.gov*
- *www.onguardonline.gov*
- *http://www.dhs.gov/topic/what-you-can-do*

Website Content Blocked at the FDA

Why are certain websites blocked at the FDA? This is a common question the Information Security Program receives from users. To protect the FDA network and data, there is a tool that identifies potentially harmful websites. When you are denied access to a site, you should see the following message: *Content blocked by the FDA*, followed by a filter category. If you have a business justification for needing access to the site or believe it is miscategorized, please contact your Center Information System Security Officer to request the website be unblocked.

When accessing the Internet on FDA resources, it is important to remember FDA policy. Staff Manual Guide 3253.11, Internet and Intranet Connections, states that FDA resources to include Internet access are intended for government business. Some malicious websites will try to fool filters so always use precaution when accessing the Internet from your FDA computer.

For additional details on website blocking and requesting sites be unblocked, check out the FAQs section on Inside.FDA: http://inside.fda.gov:9003/it/ITSecurity/FAQs/ucm356645.htm ■



Please share our Website Blocking Poster by posting it in your office and share with your peers:
http://inside.fda.gov:9003/downloads/it/ITSecurity/Communications/UCM310069.pdf

Examples of Filter Categories Blocked:

- Entertainment Video/Viral Video
- Peer-to-Peer File Sharing
- Personal Network Storage and Backup
- MP3 and Audio Download Services
- Gambling

What is a CITL and How Can They Help?

What is a CITL?

A Center IT Liaison (CITL) is a person who provides guidance for their Center customers and facilitates communication between the Center customers and the Office of Information Management (OIM). The specific duties and responsibilities for a CITL may vary from Center to Center but the basic customer advocate role is the common theme. To find your CITL is click here *http://inside.fda.gov:9003/ProgramsInitiatives/CommitteesWorkgroups/ITLiaison/ucm193405.htm.*

What can a CITL do for me?

A CITL reviews and approves *(when possible)* helpdesk tickets for:

- Software installation
- Requests for accounts with elevated privileges
- Access to group file shares, hardware repair
- Access to Regulatory systems, computer and Blackberry purchases
- Center specific questions submitted to the IT Call Center

Your IT Liaison works closely with OIM to perform software testing before updates and patches are pushed out to Agency computers and image testing before new images are released. CITLs also manage the PC Refresh program for their respective Centers to ensure that hardware and software are up to date and approved. If you need non-standard software installed that has not been previously approved by OIM, your CITL can guide you through the IT Investment Management (ITIM) process.

Pictured left to right: Lorena Moyer, LaToya DeVille, and Marie Bartin. CBER's CITL Team received an Honor Award for Outstanding Program Operations this summer.

Who are the CBER CITL's?

CBER's CITL Team received an Honor Award for Outstanding Program Operations this summer. This team is comprised of three full time employees who have 32 combined years of service at CBER. Lorena Moyer *(pictured left)* has 21 years of service and is the proud mother of 5-year-old son and a two-year-old daughter. LaToya DeVille *(pictured center)* has been with CBER for 4 years and is Mommy to a 5-year-old daughter and one-year-old son. Marie Bartin *(pictured right)* has six years of experience at CBER and has four children ages 23, 21, 20 and 15 years old. ■

Security and Privacy Awareness at White Oak

The Division of Technology (DOT) and Privacy Office team members worked together to promote security and privacy awareness at White Oak on April 24th, 2013. The teams were available to answer questions and hand out educational materials. In the fall, DOT members will be visiting other locations to educate users on security awareness, as well as discuss how we can help with security issues at events hosted by the Policy & Security Awareness team. ■

(Left) Kimberly Conway and Sara Fitzgerald from the Policy and Awareness (P&A) Team at the Security and Privacy Awareness Event at White Oak. (Right) Sara, P&A Lead is joined at the table by Jason Pendergast, Computer Security Incident Response Team (CSIRT), Aaron Hartman, CSIRT and Steven Van Brackle, P&A.

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

ITSecurityAwareness@fda.hhs.gov