



Network Security 2009

August 5, August 20, & September 2, 2009
12:30 - 2:30 p.m. (MT)



Part 1 - August 5, 12:30-2:30 p.m. MT

Phishing for Identities: The Growing Threat of Crimeware

Phishing, the process of attempting to acquire sensitive information by posing as a trustworthy entity in an electronic communication, continues to plague the financial services industry. New threats, old threats and reinvented malicious attacks continue to emerge:

- Sites infecting PCs with password-stealing crimeware reached an all time high of 31,173 in December 2008 (text messaging and telephone phishing attacks not included)
- Beginning in May, Symantec has observed a new wave of phishing attacks on Facebook users.
- A link redirects to a site masquerading as the Twitter front page.

While implementing controls and detection measures is important, employee and customer awareness is paramount. Highlights include:

- Trends and statistics
- Overview of phishing, malware, crimeware
- What can we do about it

Audience: Senior management, audit, compliance, operations, IT, and anyone else interested in today's threats and security.

Part 2 - August 20, 12:30-2:30 p.m. MT

The Network Security Headache: Is There an Easy Remedy?

Security breaches and identity theft dominate the headlines. Along with protecting your customer's information, you also need to protect the institution's intellectual and proprietary information. We use the terms network and information security synonymously. Since 80-90% or more of our information assets reside electronically, the need for securing that information is imperative. Increasing threats, emerging technology, mobile workforce and new regulations contribute to the challenge of hardening the network, restricting access, monitoring activity and implementing and enforcing controls. This presentation covers the threats facing institutions today and methods for securing your network and protecting valuable information assets including:

- What are the real threats and challenges
- Policies and controls
- Regulatory requirements

Audience: Network administrators, IT auditors, senior management, operations, risk managers, compliance officers.

Part 3 - September 2, 12:30-2:30 p.m. MT

Social Engineering: The Easiest Way to Get Access to Your Systems or Information

Social engineering is the act of manipulating people into performing actions or divulging confidential information. It can happen in person, over the phone or through text messaging and email. The goal is to gain the trust of an individual or enough information from various sources to commit identify theft or gain access into your systems. If employees succumb to social engineering it doesn't matter how many controls are in place. Understanding these types of attacks, educating employees and having a mitigation plan are essential to thwarting attacks and ensuring compliance with GLBA and ID Theft Red Flag Rules. Highlights include:

Types of social engineering and the techniques used

- Real life examples
- What you can do to help prevent social engineering at your bank

Audience: Senior management, auditors, operations, HR, training, security officers or anyone interested in protecting the institution.

Presenter

Susan Orr, Susan Orr Consulting

Continuing Education

Applied: 2.5 hrs./session CRCM/CFSSP w/the ICB

What is a Web Seminar?

A web seminar is an enhanced telephone seminar. The audio portion of the program is delivered by speaker phone. You may also view a corresponding PowerPoint presentation using a PC. No special hardware is needed. You may still participate by phone only. The program consists of 90 minutes instruction and 30 minutes live Q&A. Each web seminar registration provides 1 connection to the live web seminar, written materials and access to the Web Seminar Archive for 30 days following the broadcast. You may have unlimited listeners on your connection by speaker phone and PC. You will receive a PIN, written materials and instructions prior to the seminar. If you do not receive a confirmation at least 2 days prior to the event call 888/262-7701.

Please check all appropriate boxes

Part 1- Phishing for Identities

**SW2-1090
August 5, 2009**

Web Seminar/materials (live web seminar)

\$250 mem \$500 non-mem

Archive/materials*

\$270 mem \$540 non-mem

Part 2- Network Security

August 20, 2009

Web Seminar/materials (live web seminar)

\$250 mem \$500 non-mem

Archive/materials*

\$270 mem \$540 non-mem

Part 3- Social Engineering

September 2, 2009

Web Seminar/materials (live web seminar)

\$250 mem \$500 non-mem

Archive/materials*

\$270 mem \$540 non-mem

*Unlimited online access to a copy of the webinar for 6 months from purchase date

*We cannot guarantee registration for incomplete and/or illegible registration forms received. Please complete the form and type or write carefully.

Name _____

Title _____

Bank _____

Mailing Address _____

City/State/Zip _____

Phone/Fax _____

E-mail _____

-Preferred Payment Method: Online or e-Check

-Payment Must Accompany Registration - Invoices are Not Provided

Four Ways to Register:

Online: Visit www.montanabankers.com (Education)

Fax: Fax completed form with credit card information to 512/381-1571

Mail: Mail completed form with check to Bankers Ed, 5700 S. Mopac, #C310, Austin, TX 78749 ten days prior

Phone: Call Bankers Ed at 888/262-7701

*Late Registration: Please register online when registering 2 days prior to the event (credit cards & e-Checks accepted). Call 888/262-7701 for assistance.

Method of Payment (check one):

Check payable to Bankers Ed (must be accompanied by registration form)

Discover Card MasterCard VISA AMEX

Card Number _____ Security Code _____

Signature _____ Exp. Date _____

