

The header features a dark teal background with the text 'ASIS Councils' in white and 'NEWSLETTER' in yellow. On the left, there is a photograph of three men in business attire looking at a laptop. On the right, there is a photograph of a man in a blue shirt and glasses looking at a document.

ASIS Councils NEWSLETTER

Banking and Financial Services Council

Mr. Larry E. Brown – Chairman
First Citizens Bank & Trust

Mr. Terry Huskey, CPP – Vice Chair
Wachovia Corporation

Mr. Kevin O'Brien
The Bank of New York

Mr. Brian R. Abraham, CPP
3SI Security Systems

Mr. Robert S. Ballagh Jr, CPP
CheckFree

Mr. Steven K. Braden
Capital One Financial Corp

Mr. Michael J. Collins
Provident Bank

Mr. Robert D. Croskery
Wells Fargo & Company

Mr. Clark B. Cummings, CPP
FirstBank

Mr. Randy Dicampfi
Wilmington Trust Company

Mr. Johan D. Du Plooy, CPP
Risk Diversion Pty Ltd

Mr. R. P. Handren, CPP
RBC Protection Services

Mr. Alexander Hilton
Canadian Imperial Bank

Mr. Douglas W. Kohlsdorf, CPP

Mr. W. Joseph Majka
Visa USA

Mr. Richard L. Seba, CPP
JP Morgan Chase

Mr. Chris Smith
HBSC

Mr. P. Kevin Smith, CPP
Chevy Chase Bank

Mr. Francis X. Tesorero Jr, CPP
GE Consumer Finance

Dr. Hector R. Torres, PhD, CPP
Banco Popular de Puerto Rico

Mr. James W. Zardecki
Sovereign Bank

Banking and Financial Services Council June – August 2008

2008 ASIS Seminar, Atlanta Georgia

The 2008 ASIS International and 54th Annual Seminar and Exhibits will be held at the **Georgia World Congress Center** in Atlanta, Georgia on September 15-18, 2008.

This annual event is known for its high-quality educational program covering every aspect of security. The seminar consists of more than 150 dynamic sessions on the hottest issues and trends, as well as best practices and core security management topics that successful security professionals need to stay ahead. Each presentation is reviewed and selected by a committee of your peers to ensure that attendees learn from seasoned practitioners and subject matter experts with real-world experience and insights. Make time to participate in the best opportunity for you to:

- Network with security professionals from around the world
- Learn from the industry's top experts
- See the future of security technology at the most influential and comprehensive marketplace

Register early and take advantage of the discounts!!

IN THE NEWS

FBI stepping up efforts to combat Mortgage Fraud; Tribune Reporter; 6/13/08; Susan Chandler

The Federal Bureau of Investigation has ordered more than two dozen of its field offices, including two in Illinois, to stop probing some financial crimes so agents can focus on mortgage fraud. Kenneth Kaiser, chief of the criminal investigative division, issued the directive last week during a conference call with the heads of 26 offices in areas where mortgage crime is rampant, said Bill Carter, an FBI spokesman in Washington.

The shift comes after an analysis was conducted of how agents were spending their time. In recent years, the FBI has shifted resources away from financial crimes to concentrate on homeland security issues. About 150 agents were working on more than 1,300 mortgage cases before the change. During the 12 months ended Sept. 30, the FBI received almost 47,000 so-called suspicious activity reports from lenders detailing potential mortgage crimes, a 31 percent jump over the previous year.

The affected FBI offices are in Illinois, Florida, Georgia, California, Nevada, Arizona, Texas, New York, Ohio, Michigan, Indiana and Minnesota. Illinois has FBI field offices in Chicago and Springfield. Mortgage fraud runs the gamut from inflated-appraisal schemes to fraudulent property transfers to rescue scams that rip off homeowners facing foreclosure. Targets can include real estate agents, mortgage bankers, home builders, attorneys and appraisers.



Attorney General Warns New Check Cashing Scam

The Texas Attorney General is warning of a new scam involving checks that resemble refund checks issued through a state settlement with an unlicensed online payment service. The Attorney General's office said people have been getting the fake checks and depositing them. When the checks aren't honored by the bank that's printed on them, the money is then taken from the account of the person who deposited them. Most of the checks come with a letter claiming you've won a sweepstakes or been selected to be a mystery shopper.

Andrew Johnson Bank Warns Public of E-Mail Scam

Andrew Johnson Bank is warning its consumers that a fraudulent e-mail is circulating, purportedly issued by the Greeneville-based bank. The bank says, "This e-mail appears to link to Andrew Johnson Bank's Internet banking service, but instead redirects customers to a fraudulent (spoofed) Web site which requests responses to a 'survey' that solicits personal account information. Andrew Johnson Bank has not issued this e-mail."

Identity thieves skim credit info at gas pumps; Inquirer; 07/08/08; Peter Mucha

Thought you were getting robbed by the high price of gas? A type of identity theft can siphon your funds even faster, if you pay at the pump. The practice uses small devices that swipe credit information as people swipe debit or credit cards. Such devices, called skimmers, were apparently furtively installed as early as late April on some Wawa gas pumps in Bucks, Montgomery, Delaware and Chester Counties, as well as New Castle County, Del., according to the Pennsylvania State Police. The stolen debit card information was then used to withdraw money directly from bank accounts. Tens of thousands of dollars were taken from several dozen accounts, according to Trooper Christopher Shoap of the Media Criminal Investigation Unit.

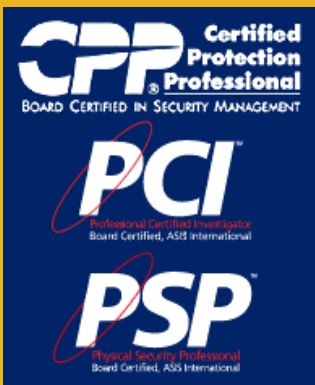
Vishing Attacks Increase; 07/20/08; Rocklin & Roseville Today

The IC3 has received multiple reports on different variations of this scheme known as "vishing". These attacks against US financial institutions and consumers continue to rise at an alarming rate.

Vishing operates like phishing by persuading consumers to divulge their Personally Identifiable Information (PII), claiming their account was suspended, deactivated, or terminated. Recipients are directed to contact their bank via telephone number provided in the e-mail or by an automated recording. Upon calling the telephone number, the recipient is greeted with "Welcome to the bank of ..." and then requested to enter their card number in order to resolve a pending security issue.

For authenticity, some fraudulent e-mails claim the bank would never contact customers to obtain the PII by any means, including e-mail, mail, and instant messenger. These e-mails further warn recipients not to provide sensitive information when requested in an e-mail and not to click on embedded links, claiming they could contain "malicious software aimed at capturing login credentials."

A new version recently reported involved the sending of text messages to cell phones claiming the recipient's on-line bank account has expired. The message instructs the recipient to renew their on-line bank account by using the link provided.





Phishing Attack Uses Vegas Theme; 07/22/08; WHIR News; Justin Lee

Internet intelligence firm Envisional (envisional.com) has warned online banking customers about a new Vegas-themed phishing fraud that dupes them into revealing credit card information through fraudulent emails. The criminals behind the attacks claim to be from Visa, Mastercard and American Express and offer email recipients the chance to win \$100,000 or an all-inclusive Las Vegas holiday package.

Most phishing attacks come in the form of spam emails addressed to customers of a particular bank and manage to trick a few dozen victims. However, this new tactic threatens more victims, because it uses a single email to target online account holders with any one of 12 major banks, and appears to be more legitimate in that it allows the victim to personally select the right bank from a drop-down list.

Envisional analysts say the latest email appears to be from an online travel website, with photos and write-ups depicting grand Las Vegas hotels. The email offers a \$100,000 personal credit card or the chance to win ten days in a top hotel, plus up to \$30,000 spending money, to those who sign up for a new "Casino Rewards" program, supposedly run by Visa, MasterCard and Amex and sponsored by 12 large US and international banks.

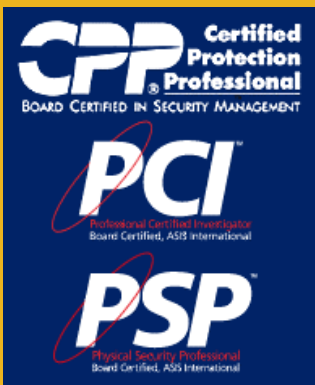
Those who click through to the website that offers further information are invited to choose their bank from a drop-down list, making the susceptible to phishing attacks. One further click takes them to a fraudulent web page that mimics the log-in page of the bank in question, with the username in one slot and password in the other.

FBI warns of New Email Scam; 07/23/08; Deseret News

The Salt Lake City office of the FBI is warning of an e-mail scam purporting to come from the FBI director. It claims a large amount of money has been deposited into your bank account and they want to know if it's terrorist-related. If you send your bank account number, your full name and other personal information, they'll check to see. "The FBI advises the best thing to do if you receive this e-mail or one similar is to immediately file a complaint with the FBI, then delete it and ignore it," FBI Special Agent Juan Becerra said in a statement.

"U.S. Fails to Prosecute Internet Fraud Cases: Report" Reuters (08/12/08)

The Center for American Progress (CAP), working with the Center for Democracy and Technology, said that U.S. federal and state law enforcement authorities have not been doing enough to resolve the problems of Internet fraud and spam. Twenty states reported a total of about 20,000 Internet-related complaints in 2007, with about \$7.1 billion lost to spyware, viruses, and phishing that year. In 2006 to 2007, the National Association of Attorneys General's Cybercrime Newsletter mentioned only 55 Internet fraud prosecutions. Although few online crimes have been prosecuted, Paula Selis, senior counsel for the office of Washington state's attorney general, says that Internet-related crime could damage online commerce. According to Reece Rushing, CAP's director of regulatory and information policy, the states that make Internet consumer protection a higher priority have been able to win settlements in cases of Internet crime.





CYBER SECURITY NEWS

Trojan Lurks, Waiting to Steal Admin Passwords IDG News Service; 07/02/08; McMillan, Robert

Attackers are using a six-year-old Trojan horse program called Coreflood to gain access into networks and steal information from thousands of computers across entire enterprises, SecureWorks says. Criminals gain access to a network by first tricking a user into downloading the program. The attacker waits until a system administrator accesses the compromised machine and then piggybacks on a Microsoft program called PsExec in order to access every machine on the network. Joe Stewart of SecureWorks estimates hackers have amassed 50 gigabytes worth of information from more than 378,000 computers over a 16-month period. "Once you have credentials that give you local admin rights via remote access, you own that system," says Microsoft's Mark Russinovich. Attackers must wait patiently for the network administrator to log on, but once this happens an entire system can be compromised relatively quickly. One global hotel chain had more than 14,000 of its computers infected, and even the SANS Internet Storm Center experienced a coup on 20 percent of its machines.

Potentially Serious Security Flaws Found In Most Bank Websites, Including Large Bank Sites, Study Shows; 07/23/08; Science Daily

More than 75 percent of the bank Web sites surveyed in a University of Michigan study had at least one design flaw that could make customers vulnerable to cyber thieves after their money or even their identity.

Atul Prakash, a professor in the Department of Electrical Engineering and Computer Science and doctoral students Laura Falk and Kevin Borders examined the Web sites of 214 financial institutions in 2006. They will present the findings for the first time at the Symposium on Usable Privacy and Security meeting at Carnegie Mellon University July 25.

These design flaws aren't bugs that can be fixed with a patch. They stem from the flow and the layout of these Web sites, according to the study. The flaws include placing log-in boxes and contact information on insecure web pages as well as failing to keep users on the site they initially visited. Prakash said some banks may have taken steps to resolve these problems since this data was gathered, but overall he still sees much need for improvement. The flaws leave cracks in security that hackers could exploit to gain access to private information and accounts. The FDIC says computer intrusion, while relatively rare compared with financial crimes like mortgage fraud and check fraud, is a growing problem for banks and their customers.

NEW BANKING TRENDS

Bank of the Future *Rocky Mountain News (07/14/08) P. 1*

Check 21 is driving a number of banking technology innovations. At Wells Fargo Bank in Colorado, 65 business customers each week are learning how to migrate their systems to remote deposit, which the bank started providing in 2005, says Micki Burciaga, a Wells Fargo vice president. Burciaga says a property-management firm that switched to remote deposit in June 2006 is saving \$100,000 per month just in courier fees.

