

PROTECT YOUR IDENTITY

IDENTITY THEFT NEWSLETTER

Don't become a victim.

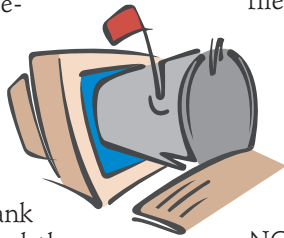
VOLUME 6
JANUARY
2010

Fraudulent E-Mails Claiming to be from the FDIC

The Federal Deposit Insurance Corporation (FDIC) has become aware of e-mails appearing to be sent from the FDIC that are asking recipients to download and open a "personal FDIC insurance file" to check their deposit insurance coverage. These e-mails are fraudulent and were not sent by the FDIC. The FDIC is attempting to identify the source of the e-mails and disrupt the transmission.

Currently, the subject line of the fraudulent e-mails includes the wording "check your Bank Deposit Insurance Coverage." The e-mails state: "You have received this message because you are a holder of a FDIC-insured bank account. Recently FDIC has officially named the bank you have opened your account with as a failed bank, thus, taking control of its assets."

The e-mails ask recipients to "visit the official FDIC website" by clicking on a hyperlink provided, which appears to be related to the FDIC and directs recipients to a fraudulent Web site. The Web site includes hyperlinks that appear to open forms. However, it is believed that



clicking on the hyperlinks will cause an unknown executable file to be downloaded. While the FDIC is working with the United States Computer Emergency Readiness Team (US-CERT) to determine the exact effects of the executable file, recipients should consider the intent of the software as a malicious attempt to collect personal or confidential information, some of which may be used to gain unauthorized access to online banking services or to conduct identity theft. Financial institutions and consumers should NOT access the Web site or download the executable files provided on the Web site.

Information about counterfeit items, cyber-fraud incidents and other fraudulent activity may be forwarded to the FDIC's Cyber-Fraud and Financial Crimes Section, 550 17th Street, N.W., Room F-3054, Washington, D.C. 20429, or transmitted electronically to alert@fdic.gov.

Work at Home Scam

The latest scam to hit the Internet has arrived this year from Nigeria: *Jobs for people seeking part-time positions- called "mail assistants"- for work done at home.* Vacancies are posted on Craigslist.com under the name of ABS Consulting. Based in the country of Luxembourg, ABS purports to have facilities throughout Europe, referred to as "Forward Luxembourg". It claims to be a leading global provider of risk-management services.

Job seekers - typically college students looking for summer work- are told they will provide mail forwarding services for expatriates, international travelers and seasonal workers around the world. They are asked to perform simple tasks:

- Receive mail at home
- Scan the front of each envelope received
- E-mail scanned images to the company
- Ship accumulated mail bi-weekly, using prepaid UPS or FedEx postage labels provided via e-mail

After two weeks on the job, assistants get an email promising an \$800 paycheck, plus an extra \$200 bonus. But to test their "integrity," they're told they'll get a check for \$2,800- and must mail a check back to return the extra money.

The \$2,800 check may look legitimate but - big surprise - it's bogus. So instead of getting paid, the college student now has to pay back the bank the full amount. Worse, the scammer now has access to the student's checking account. And the student is committing a criminal violation by scanning victims' mail.

The Postal Inspections Service is working quickly to shut down this scheme by attacking the problem from several angles. **If you have any information on this or similar scams, report it online at <https://postalinspectors.uspis.gov/> or call 1-877-876-2455, option 3.**



Chelsea
Groton
Bank

448-4100 • 823-4800
599-2406
chelseagroton.com



Member
FDIC

10 Most Prevalent Scams *And How To Prevent Them*

The consumerization of IT and widespread use of mobile technology and social networking, both at work and at home, have increased the risk of financial fraud and identity theft. While scammers are seemingly everywhere, consumers and businesses can do a lot to protect themselves from fraudulent activities. By taking some relatively simple precautions, everyone can maximize the chances that they will beat the cheats.

The dangers of online fraud continue to grow. The number of Americans falling victim to identity theft increased 22 percent to a record 9.9 million in 2008, losing \$48 billion in the process, according to Javelin Strategy & Research.

Unisys Security Index identified 10 of the most prevalent scams that can lead to financial fraud or identity theft and how to prevent them.

1 Online shopping threats: In the United States, the FBI reported that more than \$264 million was lost in 2008 due to online fraud. To avoid being a victim, security experts recommend that online shoppers always shop on safe sites that have SSL (a protocol for secure communications) certification, indicated by a locked padlock at the bottom of the screen. If you have second thoughts about using a site or retailer, follow your instincts and avoid it. Be sure to check your bank statements regularly for any unexpected "purchases."

2 The number of malicious e-cards circulating to personal and business computers is expected to rise this year. Experts suggest that even in a workplace setting, individuals never open an email or attachment from an unknown sender. If a site looks suspicious, follow your instincts and don't click on it. Finally, be sure to install personal firewall, anti-malware and protection agent software on your computer.

3 Enterprises and individuals are making increasing use of social networking sites such as Facebook and Twitter to keep in touch with clients, partners, friends and family. Experts warn that these sites can be a goldmine for identity thieves. According to GetSafeOnline, one in four people using social networking sites have posted confidential or personal information such as phone numbers, address or e-mail on their online profile. To avoid ID theft, never offer personal information to anyone over a social networking site, even if the request comes from a relative. Always be sure to apply the right privacy settings to protect yourself and avoid posting photos of

expensive belongings or dates when you are away from home for holiday travel or vacations.

4 Beware of ATM skimmers. Whether at your neighborhood bank or at your office lobby or financial institution, experts stress the importance of being aware of your environment when using an ATM to obtain cash. If you think someone is too close behind you or looking over your shoulder, find a different ATM machine. Thieves are becoming more sophisticated so also check the actual machine to make sure that it is solid and sturdy. Some skimming scams have involved fitting the front of an ATM with a false panel containing a small webcam or digital camera that can capture your card details. If the ATM machine appears to be behaving oddly or does not work the first time, go to a different machine- don't try it again.

5 Fake Online Payment Sites: Escrow services such as PayPal allow businesses and consumers to securely and conveniently send and receive payments online. However escrow scams are increasing as fraudsters set up fake payment sites to con both buyers and sellers out of money. To ensure payment sites are legitimate and secure, security experts suggest checking the site has SSL certification. Also, check the website address and be sure it starts with https:// rather than http:// as the absence of the "s" is often an indicator of rogue traders. A real escrow company will also only ask you to transfer money to them directly from your bank, i.e. a traceable transfer. If they ask for another method, refuse. Before you send anything, verify with your bank where the receiving bank is located. If this looks like it is outside the seller's own country, stop the transaction.

6 Charitable donations scams: With the economy in the worst shape it has been in a very long time, the need for charitable donations is on the rise and as a result thieves will often make the most of people's generosity. Watch out for emails or tweets from charities that ask for donations, particularly if you have never signed up to receive correspondence from them. Be sure to check that charity collectors in your neighborhood or near your office have some form of identification.

7 Gift grabbers: Now that the holidays are over and all of your gifts have been opened, security experts recommend breaking down the boxes completely so that what was in the box is not obvious to passers on the street. Thieves are more likely to target homes with

home theatre or PC boxes in the trash. The same is true of business related or personal bills, receipts and financial statements- all of which could contribute to identity theft and should be kept someplace secure or completely shredded.

8 Protect your new computer. If you received a new PC or laptop running on MS Vista or Windows 7, security experts suggest making sure you are using anti-malware software and have enabled the firewall BEFORE connecting to the Internet. Whether you are connected to a wireless network or via a cable, on average, it can take just nine seconds for your new laptop/PC to receive its first "ping" attack and less than a minute to receive its first virus.

9 "Free" Wi-Fi and wireless network hacking: If you are using that new laptop on a wireless network at home or workplace, be sure that the network is secure. This is because the Wi-Fi network range will radiate beyond the confines of your building, leaving it vulnerable to "wardriving" (the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer so they can use your unsecured network for free). Hackers could use an unprotected wireless network to anonymously download illegal material or perpetrate attacks that would appear as if they were coming from you. Wardrivers are also known to hack into computers to steal personal details and information.

10 Account checking and phishing cons: Experts recommend that individuals at home or work be wary of account checking scams in which a phony representative of a bank or supplier contacts you by phone or online to ask for account details to update their records. Callers will often claim that they need certain data in order to check the security of your account while actually obtaining very valuable information to carry out fraud. Remind family and friends to err on the side of caution and refuse to give out any personal details either on the phone or online. If you think the call is genuine, ask to call them back and check the number by visiting their website before you call back. Also, do not assume that an email that looks like it comes from your bank or company you've done business with is legitimate. In common phishing attacks, email messages from imposters contain links to phony lookalike sites where your logon ID and password can be captured. Always suspect that web links in unsolicited emails may be fraudulent and don't provide any personal information to such sites.