Member Security Alerts

Southland Federal Credit Union values your identity and as such will NEVER ask you via phone or e-mail for your account number or password. If you ever receive a call where this information is requested, do not give this information out.

News

- Smishing Alert (Text Message Scams)
- Get the facts about NCUA deposit insurance
- Awareness Key to Avoiding Phishing, Vishing Scams
- Watch Out For The MasterCard Scam
- Spoofing Site At Southland Federal Credit Union
- Southland Federal Credit Union Account Suspended Phishing Scam
- IC3 Warns of Storm Worm Virus
- When is a Credit Repair Offer A Scam?
- IRS E-mail and Telephone Scam
- CUNA Phishing Alert
- Spoof Credit Union E-Mails Could Ruin Consumers' Holidays
- Beware of JQ Bank Grant Scam
- "Evil Twin" Wi-Fi Attacks Trend Raise Identity Theft Fears
- New "Credit Repair" Scam Disguised as ID Theft Resolution
- Protect Yourself From Fraud: Get Informed
- Phony Check Scam
- Are You Ready For Vishing?
- Do You Know How To Put Your Identity Back Together Again?
- Suspicious? Just hang up and call Social Security
- Consumers Should Stay On Alert To Avoid Being "PHISHED"
- Beware of Online Scams and Security Risks From Hurricane Katrina
- Credit Unions Are The Target of "Phishing" Scams
- ALERT: New Phishing Attack Targets CU Members
- CUNA Website Subject of Illegal Phishing Message
- Identity Theft - What You Should Know
- FBI Fraud Alert

Credit Reporting Agencies

Equifax
Experian
Trans Union

Useful Links

Fraud Complaint Center
Anti-Phishing Working Group
Consumer Affairs - Scam Alerts

SMISHING ALERT (Text Message Scams)

Credit unions across the country are reporting that their member's are receiving unsolicited text messages. It is an attempt at **Smishing**, the latest form of phishing. In **Smishing**, an e-mail tries to lure a recipient into giving personal information via SMS, the communications protocol used to send text messages to a wireless device. The recent scam is targeting credit union and other financial institution members.

In **smishing**, the members receive a text message via cell phone warning that their bank account has been closed due to suspicious activity. It then tells them they need to call a certain phone number to reactivate the account.

Unsuspecting callers who dial the number provided in the text message will be taken to an automated voice mail box that prompts them to key in their credit card or debit card number, expiration date, and PIN to verify their information.

If you have a question concerning your account or credit/debit card, contact Southland Federal Credit Union using a telephone number obtained independently, such as the phone number from your statement, a telephone book, or other independent means.

Helpful Recommendations:

- Be wary of any message received from an unknown sender.
- Do not open unsolicited e-mails or text messages.
- Do not click on any links provided in unsolicited e-mails
- Don't display your wireless phone number or e-mail address in public. This includes newsgroups, chat rooms, Web sites, or membership directories.
- If you open an unwanted message, send a stop or opt out message in response.
- Check the privacy policy when submitting your wireless phone number or e-mail address to any Web site. Find out if the policy allows the company to sell your information.
- Contact your wireless or Internet service provider about unwanted messages.

GET THE FACTS ABOUT NCUA DEPOSIT INSURANCE

Your savings federally insured to at least $250,000 and backed by the full faith and credit of the United States Government. Click here for more detailed information.

AWARENESS KEY TO AVOIDING PHISHING, VISHING SCAMS

Awareness. Awareness. Awareness. This is the strongest weapon consumers can have to avoid falling victim to phishing and vishing scams. Example: Unfortunately, many North Texas consumers were unaware and as a result, got scammed. Pamela Stephens, CEO of Security One FCU (Arlington) is warning other credit unions of a recent attack that compromised the personal identity of several Security One FCU members, as well as non members.

According to Stephens, an email began circulating on May 29. The message informed recipients that Security One FCU was conducting a short online survey of "customers" to determine how well the credit union is meeting their expectations. They were driven to a web site that appeared to be that of Security One FCU. Of course it was a fraudulent web site, which Stephens says has now been taken down. Recipients were told that the data collected from this survey would assist the credit union in improving and expanding its products and services. As an incentive to take the five-question survey, the "customer" would receive $20. In order to receive the $20, the survey participant must provide personal identifying information, as well as a credit card number.

Of course, the email was not actually from Security One FCU. It was a phishing attack. Phishing is the act of sending a deceptive email to look like an authentic email from a well established firm in an attempt to scam the user into surrendering private information that could be used in an identity theft.

Unfortunately for Security One, the attack didn't stop with the one email. The following day, another email began circulating. This time, recipients were warned, "due to the recent increase in phishing scams, your account has been temporarily suspended." In order to re-activate their account, the e-mail recipient was told they must call an (800) number provided in the email and follow the instructions. Again, the recipient was asked to divulge personal identifying information and again, provide a credit card number.

This type of scam is known as vishing, which operates like phishing by persuading consumers to divulge sensitive information, claiming their account was suspended, deactivated, or terminated. Recipients are directed to contact their financial institution 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…" and then requested to enter their card number in order to resolve a pending security issue.

According to Stephens, those that did not respond to the email received a text message the following day! The content of the text message was similar to the e-mail…"in order to re-activate your account, you must call…" This tactic, according to the Internet Crime Complaint Center (IC3), is a newer version of vishing.

Stephens is sharing her story in the hopes that it will help create greater awareness, and prevent others from falling prey.

In addition to awareness, following are other tips to avoid falling victim to phishing and vishing scams:

- Never give any personal information on phone or via email. All the popular online companies like PayPal, eBay and other institutions, like credit unions etc., clearly warn users through their websites or other ways that they never ask for any personal information on email or automated phone calls. This should make it a lot easier to tell phishing attacks out.
- When in doubt, delete. Delete any email you have doubts about, especially one that requests you to give up your personal, private information.
- Be cognizant and protect your identity. Beware of e-mails, telephone calls, or text messages requesting your personal identifying information.
- If you feel the email looks suspicious, report the email to the 'real' company.

For additional tips and helpful information, visit the IC3 web site at www.ic3.gov or Anti-Phishing Working Group's web site at www.antiphishing.org. Additionally, the National Credit Union Administration (NCUA) has a brochure available on its web site for download, which explains what is phishing and how to avoid falling victim. To access the brochure, please visit the NCUA website.

WATCH OUT FOR THE MASTERCARD SCAM

MasterCard users must be on their guard for any e-mails claiming to come from the company following the discovery of a phishing campaign which attempts to entice victims with the promise of money off future purchases, says Brett Myroff, CEO of regional Sophos distributor, Sophos South Africa.The content of this phishing e-mail is unusual since it attempts to lure users to sign up to SecureCode and receive extra security protection for their MasterCard accounts, by offering a 16% discount on future purchases made with the card, says Myroff.
"In contrast, typical phishing campaigns ask users to confirm details for maintenance purposes or because of database corruption."In reality, users that click on the link contained within the e-mail are redirected to a phishing site, set up to look almost identical to the genuine MasterCard Web site, Myroff says. "Visitors are then asked to supply confidential information including credit card expiration date, date of birth and the three-digit security code located on the back of the card – ample information for the cyber-criminals to then access and use the account in question to steal money," he adds."Phishers are putting a lot more effort into their scams these days and to the undiscerning eye, it's almost impossible to tell this isn't the real MasterCard site," Myroff says.

Trojan attack
This week also saw the emergence of yet another spate of low to medium prevalence Trojans. Troj/DwnLdr-HCM is a downloader and information-stealing Trojan for the Windows platform.Another Trojan for the Windows OS, Troj/Busky-FB, installs itself in the registry and creates the following entry: HKCUSoftwareRR0OKt5hEC.The Troj/Dloadr-BKR Trojan, again affecting Windows users, has also been noted. The W32/Netsky-BS worm is also spreading via e-mail and affecting the Windows platform. W32/Xorer-D, another worm for the Windows platform, includes functionality to access the Internet and communicate with a remote server via HTTP."Following the MasterCard scam, computer users must be wary of simply clicking on links in unsolicited e-mails and should take time to verify the site address first – it may take a little longer, but will protect your money and identity from preying

cyber criminals in the long run. Also, everyone needs to use a little common sense – if it seems too good to be true, it probably is," Myroff says.

SOUTHLAND FEDERAL CREDIT UNION ACCOUNT SUSPENDED PHISHING SCAM ALERT

This is a Phishing attempt. If you ever receive an email that is asking for you to enter or provide them with your personal/account information. Don't! Other financial institutions have seen their members/customers receive request where someone is attempting to get them to follow the link and enter personal information. Southland Federal Credit Union would not ask for personal/account information in this format. Members should not click on the link; any member that has surrendered personal or account information should do the following: Close accounts, report to Law Enforcement Agency and contact Credit Agencies.

Dear Southland Federal Credit Union Member,

You have one new security message at Southland Federal Credit Union.

INBOX (1)

From: Southland Federal Credit Union Member Service
Subject: Southland Federal Credit Union Account Suspended

To go to your Southland Federal Credit Union Inbox please click on the link:

DO NOT GO TO THIS WEBSITE
http://www.shivae.org/shop/Southland Federalcu.org/index.htm

Thank You

Southland Federal Credit Union Team

IC3 WARNS OF STORM WORM VIRUS

With the Valentine's Day holiday approaching, the Internet Crime Complaint Center (IC3) urges consumers to be on the lookout for spam e-mails spreading the Storm Worm malicious software (malware). The e-mail directs the recipient to click on a link to retrieve the electronic greeting card (e-card). Once the user clicks on the link, malware is downloaded to the Internet connected device and causes it to become infected and part of the Storm Worm botnet. A botnet is a network of compromised machines under the control of a single user. Botnets are typically set up to facilitate criminal activity such as spam e-mail, identity theft, denial of service attacks, and spreading malware to other machines on the Internet. The Storm Worm virus has capitalized on various holidays in the last year by sending millions of e-mails advertising an e-card link within the text of the spam e-mail. Valentine's Day has been identified as the next target. Consumers should be wary of any e-mail received from an unknown sender, and should not open any unsolicited e-mail and do not click on any links provided. If you have received this, or a similar e-mail, please file a complaint at www.ic3.gov

WHEN IS A CREDIT REPAIR OFFER A SCAM?

By the end of 2007, Americans owed more than $915 billion in credit card debt, and the credit crunch is clearly impacting consumers as lenders are becoming more choosey about who gets loans and who doesn't. Given, stricter loan and credit requirements, the Better Business Bureau (BBB) is warning that some companies are using the credit crunch to take advantage of consumers by promising bogus credit repair services that can be costly and in some cases illegal. Complaints to BBB about credit repair companies have risen for three straight years, topping more than 1,400 in 2006. "With the economy slowing and lenders becoming increasingly picky, many people are

looking for fast, easy ways to fix or even erase damage to their credit history" said Steve Cox, spokesperson for the BBB. "People need to be very careful when searching for or using a credit repair agency. In some cases consumers are being charged for work they could have done on their own for free, and in the worst case scenarios, consumers are unwittingly encouraged to engage in illegal activities. "BBB advises anyone using a credit repair service to beware of companies that:

- Do not tell you your legal rights and what you can do – legally – for free; Recommend that you not contact a credit bureau directly; Want you to pay for credit repair services before any services are provided; Advise you to dispute all information in your credit report; Take any action that seems illegal, such as creating a new credit identity by obtaining a federal employer identification number to use instead of a social security number, and
- Offer to let you "piggyback" on other consumer's good credit.

Before contacting a credit repair service, consumers can check them out first with BBB by easily accessing BBB Reliability Reports free of charge at www.bbb.org

IRS WARNS OF NEW E-MAIL AND TELEPHONE SCAMS USING THE IRS NAME; ADVANCE PAYMENT SCAMS STARTING

The Internal Revenue Service (IRS) is warning taxpayers of several current e-mail and telephone scams that use the IRS name as a lure. The IRS expects such scams to continue through the end of tax return filing season and beyond. The IRS cautions taxpayers to be on the lookout for scams involving proposed advance payment checks. Although the government has not yet enacted an economic stimulus package in which the IRS would provide advance payments, known informally as rebates to many Americans, a scam which uses the proposed rebates as bait has already cropped up. The goal of the scam is to trick people into revealing personal and financial information, such as Social Security, checking account or credit card numbers, which the scammers can use to commit identity theft. Typically, identity thieves use a victim's personal and financial data to empty the victim's financial accounts, run up charges on the victim's existing credit cards, apply for new loans, credit cards, services or benefits in the victim's name, file fraudulent tax returns or even commit crimes. Those who have received a questionable e-mail claiming to come from the IRS are encouraged to forward it to a mailbox the IRS has established to receive such e-mails, phishing@irs.gov. Those who have received a questionable telephone call that claims to come from the IRS may also use the phishing@irs.gov mailbox to notify the IRS of the scam.

CUNA Phishing Alert

If you receive an email stating that your credit union has joined America's Credit Union, please disregard. This is an attempt to retrieve your account information maliciously. Below is a sample of the malicious email.

Dear FCU/CU account holder This notice informs you that your CREDIT UNION bank has joined our AMERICA'S CREDIT UNION (NCU/FCU/CU) network. For both, ours and your security, we are asking you to activate an online account on our database. Fill the form to activate your online account by clicking on the link bellow.https://cuna.org/update_profile/index.asp In accordance with AMERICA'S CREDIT UNION User Agreement, you can use your online account in 24 hours after activation. We thank you for your prompt attention this matter. Sincerely AMERICA'S CREDIT UNION review Department In accordance with AMERICA'S CREDIT UNION User Agreement, you can use your online account in 24 hours after activation. We thank you for your prompt attention to this matter. Sincerely AMERICA'S CREDIT UNION review Department This site is directed at or made available to persons in the United States and Credit Union customers only. Persons outside the United States may visit Credit Unions on line. Products and services described, as well as associated fees, charges, interest rates, and balance requirements may differ among geographic locations. Not all products and services are offered at all locations.

Spoof Credit Union E-Mails Could Ruin Consumers' Holidays

A new, dangerous identity theft scheme is targeting credit union customers across the country. According to consumer and credit union groups, spoof e-mails are directing credit union customers to call a telephone number and confirm their personal information. Consumers who make the call do not reach their credit union, but instead end up on the telephone with a scam artist who wants to steal their identity. Savvy consumers have increasingly learned to identify and delete spoof e-mails that falsely appear to originate from legitimate banks or credit card companies. Known as "phishing," these e-mails direct consumers to a decoy Web site that allows the scammers to collect all the information they need to empty the customers' bank accounts and ruin their credit. "Phishing" scams have been around for years, but increasingly sophisticated criminals now send e-mails instructing consumers to call a telephone number instead of clicking on a link. This tactic, known as "vishing," can be especially effective because consumers who encounter a live person are much more likely to let down their guard. The latest "vishing" scam immediately disarms consumers by specifically warning about similar schemes. One recently circulated e-mail reads:

Dear Credit Union Customer, We regret to inform you that we have received numerous fraudulent emails which ask for personal account information. The emails contained links to fraudulent pages that looked legit. Please remember that we will never ask for personal account information via email or web pages. Because of this we are launching a new security system to make Credit Union accounts more secure and safe. To take advantage of our new consumer Identity Theft Protection Program we had to deactivate access to your card account.

To activate it please call us immediately.

The e-mail provides a telephone number with a U.S. area code, adding to its air of legitimacy. In an especially brazen move, the e-mail offers identity theft tips and links to the Federal Trade Commission's identity theft prevention Web site. Consumers who think the e-mail is legitimate call the number and furnish sensitive information to a person they believe is a trusted credit union employee. Only when their identity is stolen do they realize it was all a scam. These "vishing" scams combine the "phishing" ploy with a Web-based telephone scheme. The telephone numbers that appear in these e-mails are set up through VoIP, which is an Internet-based telecommunications service. Even though the phone number appears to be based in a familiar U.S. area code, the scammers are most likely in other countries and impossible to track down. Consumers who receive this or any other unexpected e-mail or phone call seeking personal information should not respond. Consumers who have concerns about their account should contact their credit union by calling the telephone number that appears in the local directory or on their periodic statements. Never click on a link or call a telephone number that appears in an unexpected e-mail.Greg Abbott
Attorney General of Texas

Beware of JQ Bank Grant Scam

According to the Better Business Bureau, law enforcement and other agencies, a new type of online scam for grant money has surfaced. This scam appears to be another version of the "overpayment scam". Victims are solicited online regarding grants that may be available to them. These grants may be for education, debt relief, low income subsidy, or any other type of "financial aid". Responding victims apply for their grant and are sent printed information along with a check, typically for $4,975.00. They are then directed to a website for instructions. The site instructs the victim to purchase a specific variety of stored value credit card (*GREENDOT Reloadable/MoneyPak) and load it with the grant broker's "commission". They are promised a second, larger check after the stored value card number is e-mailed to the broker. Of course, the card is quickly liquidated and the original check is later returned as counterfeit, or account closed. The websites reportedly used in the scam are: www.jqbank.com, www.grantchecks.com, www.beverlyhillsgrants.com, and www.grantoutlet.com. The scammers move their operation to a new website when they start attracting too much scrutiny. * GREENDOT Reloadable/Money Pak stored value credit cards are legitimate cards but are being used as part of this scam. **Scam Details:**

- A grant seems like a reasonable explanation for receiving a large sum of money and is very attractive to college students. The counterfeit checks are often drawn on an active and verifiable account, typically at

Wells Fargo. Convincing printed information is provided to the victim with a plausible explanation for why funds need to be sent back to the broker. (Conflict of interest, regulations, etc…)

- Money is transferred back to the scammer via stored value credit card. Thus, avoiding the suspicion often generated by wire transfers. This method also facilitates further laundering of the stolen funds.

OR:

- Grant money is received for a mere commission of 10% of the check amount. The receiver of the grant money deposits the check, and then via Electronic Funds Transfer, sends 10% of the check amount back through a given website.
- The check is returned as counterfeit and the thief now has the depositor's good money along with their bank account information.

Loss Prevention Recommendations:

- Inform your members about this type of scam. Question your members if they request to purchase a specific variety of stored value credit card (GREENDOT Reloadable/MoneyPak). Place holds on check deposits in accordance with Regulation CC and credit union policy. Verify the authenticity of the checks with the institution on which they are drawn. Use a telephone number of record, not the number on the document. Another option would be to choose to accept it for collection only, rather than deposit, and not credit the member's account until the credit union receives payment. Perform periodic training/audits (i.e. monthly) to verify tellers are complying with your check hold and check cashing policies and procedures. If your members have been victimized by this scam, they should contact your local law enforcement, US Postal Inspector, or FBI.
- Report the incident to Better Business Bureau at www.bbb.org and to the Internet Crime Complaint Center at www.ic3.gov.

"Evil Twin" Wi-Fi Attacks Trend Raise Identity Theft Fears

As more and more American workers go mobile, demand for quick, efficient wireless access to the Internet is booming. Major retail chains like Starbucks and McDonald's offer paid Wi-Fi networks; wireless internet is offered at almost all major airports in one form or another. That makes it easier than ever to find an Internet connection. But this convenience may come with a hidden cost, IT security experts warn. Now technology experts believe that the prevalence of comparatively secure, password-enabled wireless access points and Web sites has opened the door for a separate and lesser-known type of cyber-attack: The Evil Twin. An evil twin attack occurs when a hacker sets up a clone Wi-Fi access point that mimics an existing wireless gateway - for instance, one of the "hotspots" commonly found at hotels, airports and coffee shops. With the right equipment, the hacker can capture any and all data submitted by an unsuspecting user via the cloned wireless hub.

Evil twin fraud can also extend beyond the initial login page, once the victim has connected to the fraudulent access point. In this scenario, the hacker remains a middleman between the scam victim and the legitimate signal, intercepting all data transmitted between the two. Worse yet, the evil twin could control the web pages that appear in the user's web browser when they enter a given domain name. Unfortunately, like many things identity theft-related, data on real-world evil twin attacks is hard to come by. No single agency keeps tabs on the phenomenon. But that's not to say evil twin attacks aren't taking place. In cases of credit account takeovers, victims often have no idea how a perpetrator might have acquired their account numbers. There are a few simple ways for consumers to protect themselves from evil twin attacks.

- the most important is to recognize the hallmarks of an authentic secure web site, knowing better than to submit sensitive data to sites that are not authentic and secure.
- consumers should pay close attention to the warnings their browsers provide before they transmit data to unsecured Web sites.

Though users typically ignore these warnings, they are there for a reason.

New "Credit Repair" Scam Disguised as ID Theft Resolution

Abuse of ID theft resolution services is a new and more pernicious version of the notorious "credit repair" scams. A new breed of scammers is attempting to clean up their bad credit and unload their unpaid debts using fraudulent claims of ID theft. According to consumer activists, a growing number of fly-by-night "identity theft prevention" and

"credit repair" services are actually cons set up by scam artists to harvest information: Social Security Numbers, driver's license number, mother's maiden name, and credit and bank account numbers. Unfortunately, consumer victims of ID theft are likely to attribute any further problems to the original theft of their identity, not to the more current scammers.

Protect Yourself From Fraud: Get Informed

Whether it's telemarketing fraud, credit card fraud, a Nigerian letter scam or identity theft, the Federal Bureau of Investigations (FBI) says consumers can take measures to avoid being victimized. One such measure is to be informed – know the warning signs and how to protect yourself from being victimized. For example, a sure way to spot a telemarketing fraud is if the caller tells you something along the lines of "you must act now or the offer won't be good." Other signs include:

- "You've won a 'free' gift, vacation, or prize" but you have to pay for "postage and handling" or other charges. "You must send money, give a credit card or bank account number, or have a check picked up by courier."
- "You can't afford to miss this 'high-profit, no-risk' offer."

Consumers should understand that it's very difficult to get their money back if they've been cheated over the phone, so before they buy anything by telephone, the FBI suggests they adhere to the following:

- Don't buy from an unfamiliar company. Legitimate businesses understand that you want more information about their company and are happy to comply. Always check out unfamiliar companies with your local consumer protection agency, Better Business Bureau, state Attorney General, the National Fraud Information Center, or other watchdog groups. Unfortunately, not all bad businesses can be identified through these organizations. Always take your time making a decision. Legitimate companies won't pressure you to make a snap decision. Don't pay for a "free prize." If a caller tells you the payment is for taxes, he or she is violating federal law.
- Never respond to an offer you don't understand thoroughly and never send money or give out personal information such as credit card numbers and expiration dates, checking account numbers, dates of birth, or social security numbers to unfamiliar companies or unknown persons.

In any scam, the scheme relies on convincing an unsuspecting victim, that the offer is legitimate. An example of this is the Nigerian scam, which has been emptying the pockets of victims for decades. The Nigerian scam combines the threat of impersonation fraud with a variation of an advance fee scheme in which a letter - mailed from Nigeria - offers the recipient the "opportunity" to share in a percentage of millions of dollars that the author (a self-proclaimed government official) is trying to transfer illegally out of Nigeria. The FBI offers the following tips to avoid falling prey to the Nigerian letter scam:

- If you receive a letter from Nigeria asking you to send personal or checking account information, do not reply in any manner. Send the letter to the U.S. Secret Service or the FBI. Be skeptical of individuals representing themselves as Nigerian or foreign government officials asking for your help in placing large sums of money in overseas bank accounts. Do not believe the promise of large sums of money for your cooperation.
- And most importantly, guard your account information carefully.

While consumers can certainly avoid being victimized by the Nigerian scam – just don't respond to the letter - preventing identity fraud is more complex because the sources of information about you are so numerous. But the FBI says you can minimize your risk of loss by following a few simple hints:

- Never throw away ATM receipts, credit statements, credit cards, or checking account statements in a usable form. Never give your credit card number over the telephone unless you make the call. Reconcile your checking account monthly and notify your credit union of discrepancies immediately. Report unauthorized financial transactions to your credit union, credit card company, and the police as soon as you detect them.
- Review a copy of your credit report at least once each year, and notify the credit bureau in writing of any questionable entries and follow through until they are explained or removed.

Just as you guard personal information such as your social security number, you should also take care to protect your credit card numbers. For example, the FBI warns that consumers should never give out their credit card

number(s) online unless the site is a secure and reputable site. Additionally, consumers should keep a list of all their credit cards and account information along with the card issuer's contact information. If anything looks suspicious or if a credit card(s) is lost or stolen, consumers should contact the card issuer immediately.

Seniors Scammed By Phony Checks

A dangerous new scam combines the counterfeit cashier's check with the phony lottery or sweepstakes. We are aware of several cases in which seniors have been scammed out of all their savings by this trick. Like the phony lottery or sweepstakes, this scam begins with an email, call or mailer that promises a large sum of money. The money may be a prize, winnings from a lottery, a once-in-a-lifetime "investment opportunity" or an inheritance. The tip-off is that before you can receive your "prize" you must first send in some money of your own, which is supposedly to cover transfer fees or taxes or some other made-up cost. You lose this money, and it turns out you never get the prize. Some savvy seniors just tell the scammer, "As soon as you send me the $40 million, I'll send you the 'fees' - Ha Ha!" The scammers have now addressed this problem. They trick the victim into thinking they have actually sent the prize by sending the victim a phony cashier's check. The counterfeits are very good, so good in fact that even banks are fooled. The victim then lets down his or her guard, believing that the whole thing is not a scam but the real thing. After all, it appears they've actually received the money. So the victim sends the money for the fees, or taxes or whatever. Then the check turns out to be worthless, and the victim's money is gone. In one variation that we are aware of, the scammer told the victim that he would help her by raising the money she needed to pay in order to collect a $2 million inheritance. He gave her a phony check for $61,000 and told her to deposit it in her account and then wire it overseas. Her bank initially told her the check was good. She did as she was told. When the check turned out to be worthless, she was liable for the money that she had wired to the scammer. Of course there was no inheritance. She lost her life savings.

Are You Ready for "Vishing"? Vishing Scams Use Phones Instead of Fake Websites

In a new twist, identity thieves are sending spam that warns victims that their credit union/bank account or PayPal accounts were supposedly compromised. However, unlike typical phishing emails, there is no website address in these phishing messages. Instead, the victim is urged to call a phone number to verify account details. The automated voice message says: "Welcome to account verification. Please type your 16-digit card number." The goal is to get the victim to enter their credit card number. In these reported scams, no mention of the credit union, bank or PayPal is made. Security experts tracking this scam and other instances of "vishing," short for "voice phishing," say the frauds are particularly despicable because they imitate the legitimate ways people interact with financial institutions. In fact, some vishing attacks do not begin with an e-mail. Some come as calls out of the blue, in which the caller already knows the recipient's credit card number. This increases the perception of legitimacy, the caller asks for the valuable three-digit security code on the back of the card. Vishing appears to be prospering with the help of Voice over Internet Protocol, or VoIP, the technology that enables cheap and anonymous Internet calling, as well as the ease with which caller ID boxes can be tricked into displaying erroneous information.
RECOMMENDATIONS:

- Never call a number you receive from a spam email, and if you do call by mistake, certainly do not enter any private information. If you want to call your bank, use the phone number you normally use, not a phone number you receive in an e-mail. Never click on the link provided in an e-mail you believe is fraudulent.Do not open an attachment to an unsolicited e-mail unless you have verified the source.Do not be intimidated by an e-mail or caller who suggests dire consequences if you do not immediately provide or verify information.If you believe the contact is legitimate, go to the company's website by typing in the site address directly or using a page you have previously book marked, instead of a link provided in the e-mail.
- Visit the FTC (Federal Trade Commission) website, www.onguardonline.gov. You will find interactive quizzes designed to enlighten you about identity theft, phishing, spam and online-shopping scams. The site also provides detailed guidance on how to monitor your credit history, use effective passwords and recover from identity theft.

Do You Know How To Put Your Identity Back Together Again?

A new online quiz offered by the Federal Trade Commission (FTC) will enable consumers to test their knowledge about protecting their personal information and responding if their identity is stolen. The quiz, available at www.onguardonline.gov/quiz, asks questions about getting a free credit report, using smart passwords, taking the right steps after an identity theft incident, and other topics. This comprehensive Web site has tips, articles, videos, and interactive activities. The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. For more information on the FTC, visit www.ftc.gov.

Suspicious? Just hang up and call Social Security

December 19, 2005 - San Antonio Express-News (TX)
By Oscar Garcia

Question: I understand that Social Security may call Medicare beneficiaries to obtain additional information needed to process the Application for Extra Help with Prescription Drug Costs. How can beneficiaries know if a call is legitimately from SSA and not part of a scam? **Answer:** Social Security may call if some questions on the application were not answered or if we cannot read the answer. We may also call to resolve discrepancies between answers on the application and information we receive from other federal agencies about the applicant's income or resources. When a Social Security employee calls for more information, he or she should never ask you for bank account, credit card or life insurance policy numbers. In most cases, a Social Security employee will not ask for even a Social Security number; the only time we do so is if the number on the application is invalid and we need to know the correct one.If a person who receives a call from someone claiming to be a Social Security employee is at all suspicious, he or she should hang up and call Social Security at (800) 772-1213 to confirm that the call is legitimate. **Q:** I retired from teaching in June an I have been receiving an annuity from the Texas Teachers Retirement System. I used the "last day" rule to be exempt from the Government Pension Offset. What evidence is needed to document that I will qualify for the exemption form the GPO based on the fact that I paid into TRS and Social Security on my last day with TRS? **A:** When you file for Social Security benefits, you should provide documentation that includes the date(s) of your covered employment, a statement that these covered earnings were considered in computing your pension and a signature from your employer or pension-payer. The Teachers Retirement System generally uses Form 562 to provide this information. In addition, as the last day of employment was last year, you'll need to provide a Form W-2 as evidence that the employment was covered under Social Security. Social Security may contact your employer for confirmation. Oscar Garcia is a public affairs specialist at the Social Security Administration. Contact Garcia at oscar.h.Garcia@ssa.gov or at Social Security Administration, 4100 S. New Braunfels, Suite 101, San Antonio, TX 78223. For our area here is Lufkin contact the Social Security Administration offices at 701 N. 1st or 702 E. Denman, Lufkin, TX 75904 or call them at (936) 632-2999.

CONSUMERS SHOULD STAY ON ALERT TO AVOID BEING 'PHISHED'

The Federal Bureau of Investigations (FBI) advises consumers to stay on alert as phishing scams continue to increase. In the last several months, the FBI has issued numerous alerts, including its latest notice informing the public of a phishing scam that involves the Internal Revenue Service (IRS). The FBI warns consumers not to fall prey, as this e-mail scam lures them to a fake IRS web site. Unsuspecting consumers believe that by clicking on the link provided, they will be directed to the IRS web site where they can follow the necessary steps to receive their owed tax refund. In actuality, they are redirected to a fake web site where their personal data, including credit card information, is captured. The IRS is of course not the only organization to be exploited in this type of scam. The FBI has issued alerts warning consumers of phishing attacks imitating organizations such as the American Red Cross and even the FBI itself. As reported last week in the *LoneStar Leaguer*, even credit unions, leagues, the Credit Union National Association (CUNA) and NCUA have been impersonated. The Federal Trade Commission (FTC) suggests these tips to help consumers avoid getting hooked by a phishing scam:

- If you get an email or pop-up message that asks for personal or financial information, do not reply. And don't click on the link in the message, either. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization mentioned in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address yourself. In any case, don't cut and paste the link from the message into your Internet browser — phishers can make links look like they go to one place, but that actually send you to a different site. Use anti-virus software and a firewall, and keep them up to date. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically. A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Operating systems (like Windows or Linux) or browsers (like Internet Explorer or Netscape) also may offer free software "patches" to close holes in the system that hackers or phishers could exploit. Don't email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons. Be cautious about

opening any attachment or downloading any files from emails you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.
Forward spam that is phishing for information to spam@uce.gov and to the company, financial institution, or organization impersonated in the phishing email. Most organizations have information on their websites about where to report problems.

- If you believe you've been scammed, file your complaint at www.ftc.gov, and then visit the FTC's identity theft web site at www.consumer.gov/idtheft. Victims of phishing can easily become victims of identity theft. While you cannot entirely control whether you will become a victim of identity theft, you can take some steps to minimize your risk. If an identity thief is opening credit accounts in your name, these new accounts are likely to show up on your credit report. You may catch an incident early if you order a free copy of your credit report periodically from any of the three major credit bureaus. See www.annualcreditreport.com for details on ordering a free annual credit report.

You can learn other ways to avoid email scams and deal with deceptive spam at www.ftc.gov/spam.

Credit Unions Are The Target of "Phishing" Scams

Credit union Websites "Phished". Numerous credit union Websites are the subject of an illegal phishing messages e-mailed to credit union members and non-members to collect their User Name and Password information. Credit unions are warning people who receive the e-mail not to click on the link to the fake Web page and to instead delete the message. Do not click on the Website link in a message that's telling you that the organization's information is out of date or incomplete. The following credit unions and credit union organizations report being a target of a "Phishing" email or spoofed website:

CUNA, NCUA, The Credit Union at the University of Chicago, Chicago IL, Northern Schools Federal Credit Union, Fairbanks, AK, U of C Federal Credit Union, Bolder, CO, Redstone Federal Credit Union, Huntsville, AL. Alabama Teachers Credit Union, Gadsden, AL, UNO Federal Credit Union, New Orleans, LA, River Valley Credit Union, Ames, IA and Cedar Falls Community Credit Union, Cedar Falls, IA,

LOSS PREVENTION RECOMMENDATIONS:
If your member or your credit union is a victim of a "phishing" consider the following:

- Post a warning on your credit union's Website that it does not solicit personal/private information via e-mail. The member should not open but delete the message. Report the incident to Internet Fraud Complaint Center http://www.ifccfbi.gov/index.aspA good resource for this topic is Anti-Phishing Working Group at http://www.antiphishing.org/index.htmlMaintain a comprehensive and up-to-date domain portfolio. Register key brand names as well as the credit union's name. Register names under all relevant domain names, including all top-level domains and country codes. Use reputable domain name registration authority. Use tools provided by a reputable Internet brand protection service to conduct regular comprehensive internet monitoring. Monitor all web links to ensure proper authorization, content, privacy, and security. Ensure that appropriate written contracts are in place with all authorized third parties. Ensure that proper disclosure notices are posted on the credit union's Website. Take appropriate action against cyber squatters and other unauthorized operators to ensure continued control of domain names and web linking relationships. If you can determine the ISP hosting the imposter/spoofed website, contact the Internet service provider to request that the Website be immediately disabled and all information pertaining to it be preserved for law enforcement.
- If you have been victimized by spoofed e-mail or Website, you should contact your local law enforcement, US Postal Inspector, or FBI.

ALERT: New Phishing Attack Targets CU Members

The Texas Credit Union League (TCUL) has been advised of a new phishing attack that targets credit union members. The attacks come in as an email urging members to update their data online. When members access the fraudulent site, their user credentials and account details are requested. Phishing is a high-tech scam that uses spam or pop-up messages to deceive unsuspecting consumers into disclosing their credit card numbers, bank account information, Social Security number, passwords, and other sensitive information. Phishers send an email or pop-up message that claims to be from a legitimate business or organization, and the message usually asks that the recipient update or validate his/her account information. BEWARE of this scam and don't answer any questions about your account online!!

CUNA Website Subject of Illegal Phishing Message

SCENARIO/METHOD: CUNA (Credit Union National Association) Website Phished
The Credit Union National Association (CUNA) Website is the subject of an illegal phishing message e-mailed to credit union members to collect their User Name and Password information. CUNA is warning people who receive the e-mail not to click on the link to the fake Web page and to instead delete the message. Do not click on the Website link in a message that's telling you that the organization's information is slightly out of date or incomplete. The fraudulent message uses graphics from CUNA's Website. It uses the America's Credit Unions logo, contains the word "consumer" on the right side of the page and addresses the credit union member. It also has CUNA's copyright. The phish message says, "During our regular accounts verification, it has come to our attention that your credit union account may be slightly out of date or incomplete. This irregularity can and must be fixed through the Credit Union National Association Confirmation process that takes 10 minutes to complete and involves logging in and confirming your identity over a secure connection" at the link. CUNA does not have such a link on its CUNA.org Website, and there is no confirmation process for accounts at CUNA, which is a national trade association for credit unions. CUNA does not have access to credit union member accounts. The phish message also warns that disregarding the notification means the member's account might be restricted, and the member won't be able to access the account online, pay their monthly bill online, review and download monthly statements or request a credit line increase or change of address.

RECOMMENDATIONS:

- The member should not open but delete the message. Report the incident to Internet Fraud Complaint Center http://www.ifccfbi.gov/cf1.aspA good resource for this topic is Anti-Phishing Working Group at http://www.antiphishing.org/index.html
- If spoofed e-mail or Website has victimized the member, they should contact their local law enforcement, US Postal Inspector, or FBI.

Identity Theft - What You Should Know

Identify theft has become the fastest growing crime in both San Antonio and nationwide. Often times, the thief even knows the victims and uses their information to make illegal purchases of clothes, electronics, furniture and sometimes even cars.

These thieves get their information in many ways, including stealing mail for pre-approved credit offers. Checks, statements or bills provide them with information necessary to open accounts in a victim's name. They can also get information from the garbage, via the phone or through the theft of a wallet or purse. Many people don't realize they've become victims of identity theft for months and until much damage has been done.

How to Minimize Your Risk of Identity Theft

- Promptly remove mail from your mail box. Never give personal information over the phone unless you initiated the call and can ID the other party. Carry only essential ID and cards Never carry your Social Security card. Sign all new credit cards immediately. Shred bills and receipts. Destroy all carbon copies. Avoid writing PINs and other codes on your credit cards
- Memorize your PINs and passwords

If you feel that your identity has been stolen, contact the creditor and your financial institution to explain the details and send a certified letter as a follow-up. Secondly, contact all three of the major credit bureaus, Equifax, Experian, Trans Union. You can find links to them on our web site. In order to avoid surprises on your credit report, it is also recommended that you look at your credit report each year.