



FRAUD NEWS & UPDATES

Zelle® Scam

Zelle is a great service to have available, but it is also a target for scammers. One of the most common scams in an effort to get access to your account involves password change requests. Never give out your password to anyone. Fraudsters may also try to call or text pretending to be your credit union stating you have had a number of suspicious transactions on your account. And then they will ask a series of questions or send you a verification password to prove your identity. These are scams to access your funds. If you believe you are being scammed, hang up and call WESLA Federal Credit Union.

Online/Mobile Banking Scam

Watch out for phone calls from individuals posing as “Fraud Reps”. The “rep” asks for your username and passwords to online banking and the “rep” logs into your online banking account and conducts external transfers (taking money from your account). We will not call, text or email you requesting your online banking username and password.



Main Office
2921 Williamson Way
Shreveport, LA 71118

(318) 687-8700

Auto Mall Branch
8650 Fern Avenue
Shreveport, LA 71105

1-800-828-6647

Bossier City Branch
2600 Melrose Avenue
Bossier City, LA 71111

www.wesla.org





WHAT IS..

- **VISHING** - Fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers.
- **SMISHING** - Short for SMS Phishing, smishing is a variant of phishing email scams that instead utilizes Short Message Service (SMS) systems to send bogus text messages.
- **PHISHING SCAMS**- lure account holders into providing personal or financial information to scammers posing as a legitimate business. Most phishing scams are conducted through email, with messages containing links that ask for your personal data or download spyware to your computer or mobile device. Other phishing scams are conducted by phone call, text messages and social media. Navy Federal will never solicit your personal information via phone or email.

Don't Be A Victim!!

The number and sophistication of phishing scams sent out to consumers is continuing to increase dramatically. While online banking and e-commerce is very safe, as a general rule you should be careful about giving out your personal financial information over the Internet. The Anti-Phishing Working Group has compiled a list of recommendations below that you can use to avoid becoming a victim of these scams.

- Be suspicious of any email with urgent requests for personal financial information!
- Phishers typically include upsetting or exciting (but false) statements in their emails to get people to react immediately
- They typically ask for information such as usernames, passwords, account numbers, credit card numbers, social security numbers, etc.
- Phisher emails are typically NOT personalized, while valid messages from your bank or e-commerce company generally are
- Don't use the links in an email to get to any web page if you suspect the message might not be authentic. Instead, call the company on the telephone, or log onto the website directly by typing in the web address in your browser.
- Avoid filling out forms in email messages that ask for personal financial information. You should only communicate personal information (such as credit card numbers, PIN number, social security numbers, or account information) over the telephone or via a secure website. When submitting credit card or other sensitive information via your web browser, always ensure that you're using a secure website.

•



Main Office
2921 Williamson Way
Shreveport, LA 71118

(318) 687-8700

Auto Mall Branch
8650 Fern Avenue
Shreveport, LA 71105

1-800-828-6647

Bossier City Branch
2600 Melrose Avenue
Bossier City, LA 71111

www.wesla.org





- Regularly log into your online accounts – don't leave it for as long as a month before you check each account.
- Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate. If anything is suspicious, contact your financial institution and all card issuers.
- Always report 'phishing' or 'spoofed' e-mails to the following groups:
 - Forward the email to the Federal Trade Commission at spam@uce.gov.
 - Forward the email to the "abuse" email address at the company that is being spoofed.
 - When forwarding spoofed messages, always include the entire original email with its original header information intact
- **IDENTITY THEFT** – Identity theft is a crime in which an imposter obtains key pieces of personal information, such as Social Security or driver's license numbers, in order to impersonate someone else. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials. In addition to running up debt, an imposter might provide false identification to police, creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen.
- **SKIMMING**- Skimming is a huge problem for financial institutions and its members in the United States. It involves stealing the magnetic strip information off a members debit card and using a hidden camera to gather their PIN number information. The information is then used to make a duplicate debit card. In 2012 alone, criminals were able to use these cards and steal 11.3 billion dollars.

With the advent of EMV chips, criminals are aware that the switch to the more secure card is coming in October of 2015, and are in turn trying to commit as much fraud as they can before that. Because of this, both the member and the financial institutions have to take extra precautions when using ATMs.

In an effort to keep you informed, we have a few tips of what you can look for when using your debit/ATM card.

- Look for changes in the ATM or card reader -extra plastic -bulkier card reader -any pieces that weren't present before - changes in the card reading method
- Look for changes in the keypad look and feel.
- Make sure to look around for any cameras place in a position where your hand can be seen in putting your PIN number. They can be very small or placed in pieces of plastic.
- If you suspect a skimmer is being used, contact the financial institution that owns the ATM or the local police department.
- With your heightened awareness, you are not only helping yourself, but you are helping financial institutions fight fraud all over the country.



Main Office
2921 Williamson Way
Shreveport, LA 71118

(318) 687-8700

Auto Mall Branch
8650 Fern Avenue
Shreveport, LA 71105

1-800-828-6647

Bossier City Branch
2600 Melrose Avenue
Bossier City, LA 71111

www.wesla.org



How to Protect Your Identity Steps to Minimize the Risk of Your Identity Being Stolen

Identity theft occurs when someone uses another person's identity. It can be an account takeover or posing as a financial institution member to obtain the members personal financial information - pretexting.

Although you only have to pay the first \$50 of fraudulent charges, the average identity theft victim spends many hours and over \$1,000 to have their credit restored.

Prevention Techniques

1. Before allowing anyone access to personal information (e.g. Social Security Number (SSN), mothers maiden name, bank account numbers, etc.) ask how it will be used and if it can be kept confidential. Never give this information out over the telephone. Only give out your SSN when necessary. Ask to use another form of identification, if possible. DO NOT carry your Social Security card in your purse or wallet.
2. Place the contents of your wallet on a photocopy machine. Do both sides of each license, credit card, etc. That way, you will know what you had in your wallet, including all of the account numbers and phone numbers you need to call and cancel. Keep the photocopy in a safe place. Carry a minimum number of credit cards and identification.
3. Shred or destroy credit and debit card receipts, cancelled checks, expired credit cards, pre-approved credit card solicitations, convenience checks, insurance forms, financial statements, and any other documents you are disposing of that contain personal information or account numbers. To stop receiving prescreened credit offers, you can call 888-5-OPTOUT. You can prohibit use of information in your credit bureau report from being used to determine if you qualify for offers not initiated by you by calling toll-free 1-888-567-8688. You can reduce junk mail and telemarketing calls by going to the Direct Marketing Association website at <http://www.dmaconsumers.org/consumerassistance.html>.
4. Mail all outgoing mail from post office collection boxes, from your work, or the local post office. Do not let your personal mail sit in the mailbox after it as been delivered.
5. Keep a record of all the credit cards and accounts you have, including issuing company information, card or account numbers, expiration dates, and telephone numbers to call if the card or account is lost, stolen, or fraudulently accessed. This record should be kept in a safe place. Be aware of when in the month you should receive credit card bills and immediately report bills not received. Review bills thoroughly for unauthorized charges.
6. Notify your credit union if your checks are stolen and close that account. Stop payment on your checks. Ask your credit union to notify the check verification service with which it does business. Do not have your SSN or drivers license number preprinted on your checks.
7. When assigning passwords to accounts, avoid using your mothers maiden name, your birth date, the last four digits of your SSN, your phone number, address, your drivers license number, or any series of consecutive numbers.

8. Find out how your employer safeguards your personal information. Employers are obligated to store documents with personal information, such as SSNs, in a secure format, whether the information is paper-based or electronic.
9. Get copies of your credit report annually from each of the three credit reporting agencies. Review the report to make sure it is accurate and includes only credit you have authorized. If you discover inaccurate information or a credit check conducted for an unfamiliar loan or lease, contact the credit bureau and report it immediately. The Fair and Accurate Credit Transactions Act requires that everyone must have access to their credit report for free on an annual basis. Individuals are able to receive their credit score; however they may have to pay a fee to receive the score. If you have been denied credit based on information from a credit report you are entitled to get a free copy of it.
10. Check your credit union and all other financial statements for discrepancies or unauthorized transactions.
11. Do not leave your wallet or credit cards in your car.
12. Do not give out personal or financial information over the telephone unless you know the caller and how the information will be used. The credit union will never ask for sensitive information unless you initiate the call.
13. Fraudsters are sending a fictitious IRS form and a fraudulent letter purporting to be from a bank by asking them to disclose personal and banking information. If a person returns the false IRS form to the fax number provided on the fake bank letter, the perpetrator of the fraud can contact the bank with enough information to appear credible, thereby gaining access to the victim's accounts, credit, and credit history. Contact the IRS to report the incident using the toll-free hotline number 800.829.0433.

Credit Reporting Agency Contact Information

Equifax <http://www.equifax.com/>

To request a report, call 800.685.1111

Or write:

PO Box 740241

Atlanta, GA 30374-0241

To report a fraud, call 800.525.6285

Or write the above address

Experian (formerly TRW) www.experian.com

To request a report or to report a fraud, call 888.397.3742

Or write:

PO Box 949

Allen, TX 75013-0949

Trans Union www.tuc.com

To request a report, call 800.916.8800

Or write:

PO Box 1000

Chester, PA 19022

To report fraud, call 800-680-7289

Or write:

Fraud Victim Assistance

PO Box 6790, Fullerton, CA 92634

Should You Become A Victim

If you believe you have been the victim of ID theft, immediately take the following steps:

1. Call the Federal Trade Commissions Identity Theft Hotline at 877.438.4338 (877 ID THEFT). Other tips are given at the FTC's website at www.consumer.gov/idtheft. You can write them at:

*Identity Theft Clearinghouse, Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580*
2. Report the fraud to the three major credit bureaus at the numbers given above and request a fraud alert placed on your name and SSN.
3. File a report with the police department in the locality where the fraud occurred.
4. Get new account numbers, ATM cards, and pin numbers.
5. It is a crime for someone to use your SSN to establish credit or open new accounts. Call the SSN Fraud Hotline at 800.269.0271.
6. Contact your creditors (credit card companies, phone companies, etc.) for any accounts that have been tampered with or opened fraudulently. Speak to someone in the fraud department. Follow up with written correspondence.
7. If an identity thief stole your mail or falsified a change-of-address form, that is a crime. Report it to your local postal inspector.
8. Report all stolen cards to the issuers immediately and get replacement cards with new account numbers. Ask that the old accounts be processed as "account closed at consumer's request" so that a "lost or stolen" notation cannot be interpreted as blaming you. Follow up with written correspondence.
9. Check the section of the report that lists "inquiries" and request that "inquiries" from companies that opened the fraudulent accounts be removed. Follow up each conversation with a letter detailing the exact circumstances and action requested. Include copies (not originals) of documents that support your position. Send your letter by certified mail and request a return receipt. Keep copies of your dispute letter and any enclosures. Do not forget to follow up in a few months by requesting a new copy of your report so you can verify that the corrections were made.
10. If someone has filed for bankruptcy using your name, you will need to write to the U.S. Trustee in the region where the bankruptcy was filed. A list of regions can be found at www.usdoj.gov/ust
11. Request that creditors call you before opening any new accounts or changing existing ones. Add a victim's statement to your report and find out how long the fraud alert is posted on your account and extend it if possible.

Keep a log of all conversations, including dates and names. Send correspondence by certified mail. Keep copies of all letters and documents and be sure to have your police report case number with this documentation.

Identity thieves can obtain your personal information by:

- Stealing wallets that contain personal identification information, credit cards, ATM cards, etc.
- Pretext calling (posing as an account holder or someone authorized to have account holder information in order to obtain confidential account holder data).
- Stealing mail to obtain credit card statements, monthly account statements, telephone bills, and tax information.
- Filling out change-of-address forms to divert a person's mail to another location.
- Rummaging through a person or company's trash for personal data.
- Purchasing copies of job or charge-card applications from store employees.
- Stealing personal information from workplace records
- Intercepting personal information transmitted electronically.