COMPLIANCE
& Risk Management

LSCU
League of Southeastern Credit Unions & Affiliates

IDENTITY THEFT

RED FLAGS AND HOW TO PROTECT YOURSELF

OBJECTIVES

By the end of this presentation you should be more familiar with...

1. Common Identity Theft Tactics
2. Red Flags to look out for
3. Ways to protect yourself from identity theft
4. What to do if you fall victim to identity theft

WHAT IS IDENTITY THEFT?

USA.GOV DEFINES IDENTITY THEFT AS SOMEONE USING YOUR PERSONAL OR FINANCIAL INFORMATION WTHOUT YOUR PERMISSION

IN 2022, THERE WERE OVER 1.1 MILLION REPORTS OF IDENTITY THEFT REPORTED TO THE FEDERAL TRADE COMMISSION

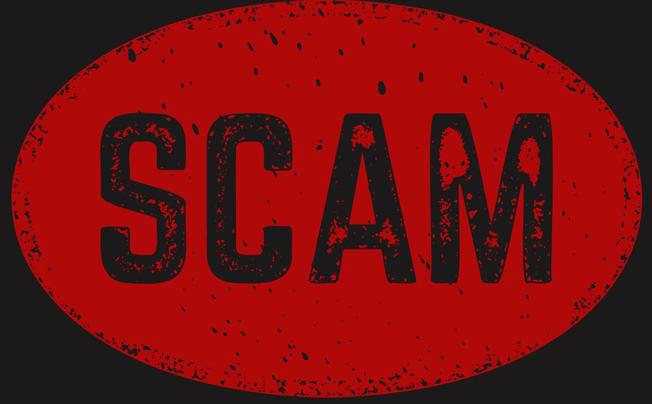
A RED FLAG IS A PATTERN, PRACTICE, OR SPECIFIC ACTIVITY THAT INDICATES THE POSSIBLE EXISTENCE OF IDENTITY THEFT

COMMON TACTICS OF IDENTITY THEFT

Here are some of the most common tactics of identity theft. Click ahead to get details about how each of these scams work...

- Student Loan Forgiveness Scams
- Phone Scams
- Gift Card Scams
- Employment Scams
- Imposter Scam
- Email Scams
- Debt Collection Scams
- Medicare Verification Scams
- Fake Online Shopping Sites
- Tech Support Scams

*** Ofcourse, there are many other scam tactics, these are just some of the most common today!



01 STUDENT LOAN FORGIVENESS

A scammer may pressure a victim with fake urgent messages encouraging you to apply for debt relief and then request a payment for an application fee. They may attempt to access your social security number and account numbers.
For information about your student loan, contact your student loan provider or find information on the Department of Education's Website

02 GIFT CARD SCAMS

Congratulations! You have won a gift card giveaway- all you need to do to redeem your gift card is click here and answer this short survey about all of your financial and personal information.

Remember, if it seems to good to be true, it probably is.

03 EMPLOYMENT SCAMS

Employment scams prey on those eager for work. Would be "employers" may ask for money up front to pay for job equipment or pressure you to give them your personal information. They may also ask you to work for a period and send you a fake check, or no check at all.
The Better Business Bureau found that 76% of employment scam victims felt that something was off and pursued the job offer anyways. Always listen to your gut!

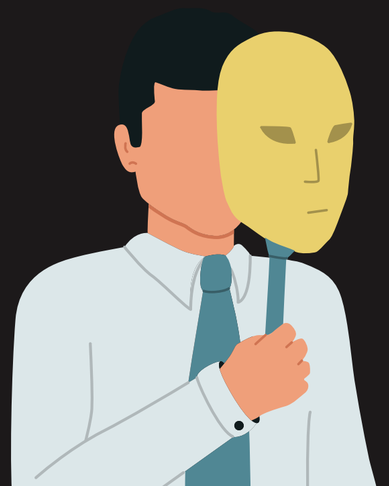
04 FAKE EMAIL SCAMS

"Phishing" emails look as if they come from a legitimate source. They may appear to be from your financial institution, credit card provider, a known retailer, or a government agency. These emails carry software called malware, which can be used to steal your digitally stored information, such as health records, passwords, and personal identifitaion numbers.
The Interstate Technology and Regulatory Council reported that in 2021, 1/3 of cyberattacks were a result of phishing.

05 IMPOSTER SCAMS

This occurs when someone calls or emails you claiming to be a government official or friend requesting personal and/or financial information.

A form of this happens in Debt Collection Scams, where an individual poses as a debt collection employee and claims that they are contacting you to collect a debt. They often ask for your personal information and will request payment by wire transfer or credit card.



06 MEDICARE SCAMS

A scammer will call, email, or even show up in person telling a victim that they need to verify their Medicare. They ask for verification of a Medicare Identification Number. The Medicare info the victim provides is used to fraudulently bill Medicare and collect money or even receive healthcare services.

Guard your Medicare ID Number as you would any other personal information.

Ignore calls, emails, and visitors purporting to offer you anything in exchange for your information.

07 FAKE ONLINE SHOPPING SITES

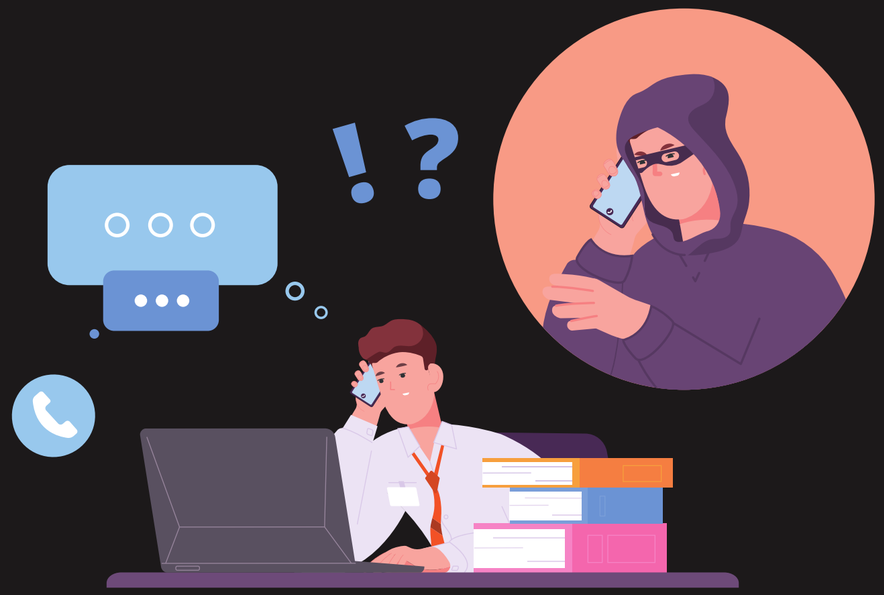
Be cautious when shopping online at social media based stores with prices too good to be true! These "stores" may be fabricated to lure victims in to steal their financial and personal information. Be especially wary if payment is demanded in the form of a wire transfer or other immediate means. Often, in these situations, terms and conditions; dispute resolution; and contact information may be scarce. Those who purchase from these fake sites often never receive any merchandise and attempts to reach the seller are unsuccessful.

08 TECH SUPPORT SCAMS

What should you do if you receive a phone call or pop-up on your computer warning you that your device has a virus or other problem and needs to be fixed? Remember that legitimate tech businesses will not contact you in this way to communicate an issue. Rather, these warnings are created by fraudsters pretending to be employees of Microsoft or other large tech companies. They typically ask to remotely access your computer and demand that you pay them to fix a nonexistent problem. Doing so gives the fraudster access to all of your personal and financial information that you may have stored on your computer.

It is wise to use someone you know or a reputable repair company when having your computer fixed!

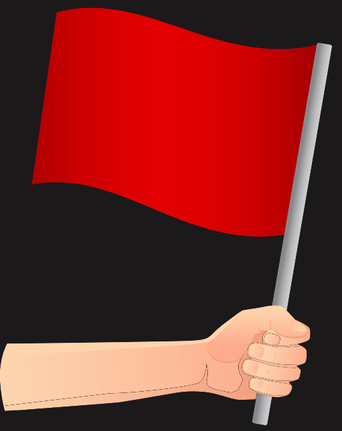
PHONE SCAMS



It seems like we all receive more robocalls and spam calls everyday. But did you know that some of these calls may be scams, attempting to access your personal information and steal your identity? Be wary of anyone calling and asking for your personal information for ANY reason.

Legitimate businesses and government organizations will not call and require you to provide your personal identification information.

To help reduce the number of telemarketer calls, place your number on the National Do Not Call Registry. Once your number is on the list for 31 days, you should stop receiving calls from most telemarketers. At that point, the ones that still call you are most likely scams.



CONSIDER THESE RED FLAGS

Each red flag indicates possible identity theft!

01 YOU RECEIVE DEBT COLLECTION CALLS FOR ACCOUNTS YOU DID NOT OPEN

02 YOU RECEIVE BILLS FOR ITEMS THAT YOU DID NOT PURCHASE

03 THERE IS INFORMATION ON YOUR CREDIT REPORT FOR ACCOUNTS YOU DID NOT OPEN

04 YOU NOTICE UNRECOGNIZED BANK/CREDIT CARD TRANSACTIONS

RED FLAGS

Red flags in phishing attempts are warning signs or indicators that help individuals identify potential scams. Some common read flags in phishing include:

1. Urgent or threatening language
2. Suspicious sender information
3. Requests for personal information
4. Misspellings or grammatical errors
5. Suspicious links or attachments
6. Generic greetings
7. Too good to be true

01 URGENT OR THREATENING LANGUAGE

Phishing attempts often create a sense of urgency or use threatening language to prompt immediate action. Phases like "urgent action required," "account suspended," or "your account will be deleted" may indicate a phishing attempt.

02 SUSPICIOUS SENDER INFORMATION

Check the sender's email address or social media profile. Phishing emails or messages often use generic or suspicious email addresses that do not match the legitimate entity they claim to represent.

03 REQUESTS FOR PERSONAL INFORMATION

Legitimate organizations do not request personal information, such as usernames, passwords, or credit card numbers, via email, social media, or other online means. Be cautious of any request for personal information.

04 MISSPELLINGS OR GRAMMATICAL ERRORS

Phishing emails or messages may contain misspellings, grammatical errors, or awkward phrasing. Legitimate organizations usually have professional communications and do not contain obvious errors.

05 SUSPICIOUS LINKS OR ATTACHMENTS

Be cautious of links or attachments in emails or messages from unknown or untrusted sources. Hover over links to check their actual destinations, and do not click on suspicious links or download attachments that you were not expecting.

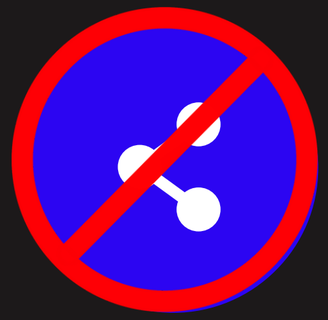
06 GENERIC GREETINGS

Phishing emails may use generic greetings like "Dear Customer" instead of addressing you by your name. Legitimate organizations often personalize their communications with your name or other relevant information.

07 TOO GOOD TO BE TRUE

Phishing attempts may lure individuals with enticing offers, such as winning a prize or getting a huge discount. If an offer seems too good to be true, it may be a phishing attempt.

PROTECT YOURSELF



Don't share your personal information with anyone! If someone calls asking for your personal information, question why they need it.

Remember, if someone calls you and asks for information, it is always okay to hang up and call a business back at a known number.

Protect yourself online!

Use strong passwords and multi-factor authentication when you can.

Be cautious when entering your personal information on websites.

Review your credit card and account statements regularly.

Store your personal information, including your Social Security Card, in a safe place. DO NOT CARRY IT IN YOUR WALLET.

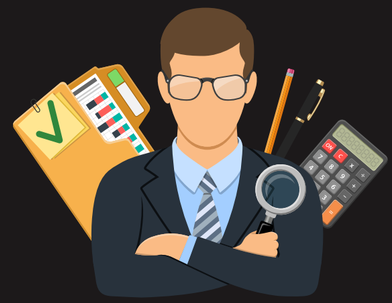
Review credit reports at least once a year and report any incorrect or suspicious activity.

WHAT TO DO IF YOU ARE A VICTIM

Report identity theft!

Notify the 3 major credit reporting agencies (Equifax, Experian, Transunion) and ask them to place a fraud alert and credit freeze on your accounts.

Contact your credit card issuers, credit union, other financial institutions, and anywhere else you have an account to alert them.



Close any new accounts that have been opened in your name, correct your credit report if needed, remove or dispute any bogus charges you may have on your accounts.

RESOURCES

- **FTC.GOV:** THE FTC'S FREE, ONE-STOP RESOURCE, *WWW.IDENTITYTHEFT.GOV* CAN HELP YOU REPORT AND RECOVER FROM IDENTITY THEFT. REPORT FRAUD TO THE FTC AT *FTC.GOV/ONGUARDONLINE OR WWW.FTC.GOV/COMPLAINT*

- **US-CERT.GOV:** REPORT COMPUTER OR NETWORK VULNERABILITIES TO US-CERT VIA THE HOTLINE: *1-888-282-0870* OR *WWW.US-CERT.GOV.* FORWARD PHISHING EMAILS OR WEBSITES TO US-CERT AT PHISHING- *REPORT@US-CERT.GOV.*

- **IC3.GOV:** IF YOU ARE A VICTIM OF ONLINE CRIME, FILE A COMPLAINT WITH THE INTERNET CRIME COMPLAINT CENTER (IC3) AT *HTTP://WWW.IC3.GOV.*

- **SSA.GOV:** IF YOU BELIEVE SOMEONE IS USING YOUR SOCIAL SECURITY NUMBER, CONTACT THE SOCIAL SECURITY ADMINISTRATION'S FRAUD HOTLINE AT *1-800-269-0271.*

- **CONTACT INFORMATION FOR CREDIT REPORTING BUREAUS:** TRANSUNION *800-916-8800;* EQUIFAX *888-378-4329;* EXPERIAN *888-397-3742*