Oakdale

Community Newsletter

Would You Know a Scam If You Saw One?

Scammers are constantly finding new ways to steal your money and or your identity. You can protect yourself by knowing what to look out for.
This month, we have highlighted some of the most common types of fraud and scams, what to watch for and what steps to take to keep yourself, your loved ones, your identity and your money safe.

FIRST, SOME GOOD NEWS!!!

oakdale oakdale oakdale oakdale oakdale oakdale oakdale oakdale oakdale oakdale oakdale

Coming Soon!

to

Oakdale!

J*A*B PROPERTY MANAGEMENT IS PLEASED TO ANNOUNCE THAT WE ARE OPENING AN OFFICE IN OAKDALE FOR YOUR CONVENIENCE!!

Five RED Flags to Watch Out For

UNEXPECTED CONTACT:
A person or company contacts you out of the blue by phone, text, or email about an invoice, order, delivery, or charge you didn't know about.

EVERYTHING IS "URGENT!":
Scammers will create a false sense of urgency and use pressure tactics like rude or pushy language to get you to act immediately.

VERY SPECIFIC OR UNUSUAL WAY TO PAY:
Someone is asking you to pay or send money using gift cards, cryptocurrency, a payment app, or even an online wire - to pay for something, resolve an "issue," get "sweepstakes winnings," or stave off your imminent arrest.

THREATENING LANGUAGE:
Scammers may tell you that you owe money, then threaten to call the police if you don't pay immediately. They may also coach you on what to tell the bank to withdraw or transfer money, or ask you to keep a "secret."

THE "ROMANTIC EMERGENCY":
A new online love interest bombards you with "sweet talk" but doesn't seem to want to meet you in person. Suddenly a hardship or emergency strikes and they want you to send them money.

Six Common Scams & How To Avoid Them

CHARITY SCAMS:
A charity scam is when a thief poses as a real charity or makes up the name of a charity that sounds real in order to get money from you. These kinds of scams often increase during the holiday season as well as around natural disasters and emergencies, such as storms, wildfires, or earthquakes. Be careful when any charity calls to ask for donations, especially ones that suggest they're following up on a donation pledge you don't remember making.
What to do: Ask for detailed information about the charity, including address and phone number. Look up the charity through their website or a trusted third-party source to confirm that the charity is real.

DEBT COLLECTION SCAMS:
Most debt collectors will contact you to collect on legitimate debts you owe. But there are scammers who pose as debt collectors to get you to pay for debts you don't owe or ones you've already paid.
What to do: Don't provide any personal financial information until you can verify the debt.

DEBT SETTLEMENT AND DEBT RELIEF SCAMS:
Debt settlement or relief companies often promise to renegotiate, settle, or in some way change the terms of a person's debt to a creditor or debt collector. Dealing with debt settlement companies, though, can be risky and could leave you even further in debt.
What to do: Avoid doing business with any company that guarantees they can settle your debts, especially those that charge up-front fees before performing any services. Instead, you can work with a free or nonprofit credit counseling program that can help you work with your creditors.

GRANDPARENT SCAMS:
If you get a call from someone who sounds like a grandchild or relative asking you to wire or transfer money or send gift cards to help them out of trouble, it could be a scam.
What to do: Read more about other ways to protect older adults from fraud and financial exploitation.

FORECLOSURE RELIEF OR MORTGAGE LOAN MODIFICATION SCAMS
Foreclosure relief or mortgage loan modification scams are schemes to take your money or your house, often by making a false promise of saving you from foreclosure. Scammers may ask you to pay upfront fees for their service, guarantee a loan modification, or ask you to sign over the title of your property, or sign paperwork you don't understand.
What to do: If you are having trouble making payments on your mortgage, a HUD-approved housing counseling agency can help you assess your options and avoid scams. If you think you may have been a victim of a foreclosure relief scam, you may also want to consult an attorney. Learn more about mortgage loan modification scams.

IF IT SOUNDS TOO GOOD TO BE TRUE, IT PROBABLY IS.

ROMANCE SCAMS:
A romance scam is when a new love interest tricks you into falling for them when they really just want your money. Romance scams start in a few different ways, usually online. Scammers may also spend time getting to know you and developing trust before asking you for a loan or for access to your finances.
What to do: Be smart about who you connect with and what information you share online. Don't share sensitive personal information, such as bank account or credit card numbers or a Social Security number, with a new love connection. Learn more about how to avoid romance scams.

FOR MORE INFORMATION ON SCAMS, VISIT CONSUMERFINANCE.GOV

& Some NOT-So-Common Scams

Student Loan Forgiveness Scams:

When student loan forgiveness applications opened in 2022, the FBI warned borrowers to watch out for scams targeting applicants. Student loan forgiveness scammers may contact you via phone or create phony application sites aimed at stealing your Social Security number or your bank account information. They may put pressure on their victims with fake urgent messages that encourage you to apply for debt relief before it's too late. Then they'll charge you a hefty application fee. In reality, it's a scam.

It costs nothing to apply for student loan forgiveness, so anyone who asks you to pay a fee is committing fraud. In addition, the U.S. Department of Education won't contact you by phone. You can stay safe and avoid student loan forgiveness scams by going directly to the Department of Education website for information about applying for forgiveness.

PHONE SCAMS:

Scammers may try to get in touch with you by phone, and some phone scams rely on smartphones' capabilities to access the internet and install malware.

- Robocalls: Robocalls have people's phones ringing nonstop with increasingly natural-sounding recorded voices. They may offer everything from auto warranties to vacations, or issue a threat to try and get your attention. Some robocalls can even respond to your questions.
- Texts: You may receive a text message from an unknown number or email address. Often, these smishing attempts include a link to a scammer's website or app.
- Impersonators: Scammers impersonate IRS personnel, police, survey takers, relatives, delivery people and well-known companies to threaten you or gain your trust. They use scare tactics related to your Social Security number, criminal record or account before asking for your personal, account or credit card information.
- Apps: Scammers may try to get you to install a malicious app to steal your information. Or, they might create a nearly identical copy of an existing app and then make money from in-app purchases.
- QR codes: QR codes have gained popularity as a touchless option to do things like read a restaurant menu or make a payment. However, scammers place their QR codes in inconspicuous spots, and scanning the code could prompt you to make a small purchase or enter your credentials on a look-alike website.

SIM SWAPPING:

SIM swapping happens when a thief steals your number and assigns it to a new SIM card in a phone they control. It's the same process you go through when you get a new phone and the mobile carrier gives you a new SIM card. The scammer uses your SIM card to steal your information to log in to your accounts and either enter a verification code or reset the account password using the code or link sent to the phone.

You might be able to contact your mobile phone operator and add extra security or temporarily freeze number porting to help protect yourself from SIM swapping. Also, see if your accounts let you use a non-SMS multifactor authentication option, in which you provide two pieces of proof to verify your identity.

YOUR BANK WILL NEVER ASK YOU FOR YOUR PASSWORD NEVER!!!

One-Time Password (OTP) Bots:

An alternative to SIM swapping, some scammers are using so-called OTP bots to trick people into sharing the authentication codes that are sent to them via text or email, or that they have to look up in an authentication app or device.

The bots may initiate a robocall or send you a text imitating a legitimate company. For example, the robocall may look and sound like it's coming from a bank. The voice asks you to authorize a charge and tells you to input the code you're texted if it's not one you made. In reality, the bot is attempting to log in to your account, which triggers the system to send you the code. If you share the code, the scammer can then log in to your account.

Don't Let It Be

GAME OVER

For You!!

Lock it Down!

Protecting Your Personal Information is No Game.

1: KEEP YOUR MAIL SAFE

Keep your mail in a locked mailbox or consider using a PO Box at the post office. Put a stop order on mail delivery when you are traveling.

2: READ YOUR ACCOUNT STATEMENTS

Each month open all of your statements for bank accounts, credit cards, etc. to check for purchases that you do not recognize. Or better yet, set up your account on the company's secure website and check your account there every few days.

3: CHECK YOUR CREDIT REPORTS

You are entitled to one free credit report per year from each of the three credit reporting agencies (Equifax, Experian, Trans Union). Access them by going to www.annualcreditreport.com. Read them completely and look for errors in your personal information or accounts that you do not recognize.

4: SHRED!

Some thieves have been known to go through garbage cans and dumpsters looking for your financial information. Once you are finished with a financial document use a crosscut shredder to dispose of it.

5: STORE PERSONAL DOCUMENTS AT HOME

Some people like all of their important things in one place -- like a purse or wallet -- but this can be disastrous if your purse or wallet is stolen or lost. Leave your Social Security card, and any credit cards that you don't use on a regular basis, at home. Keep important documents, as well as birth certificates, immigration documents; insurance policy information, and bank account information in a fireproof lockbox or another secure location.

6: BE WARY OF UNKNOWN PHONE CALLS AND EMAILS

Never give out personal information via phone or email—even if they claim to be your bank. Unsolicited phone calls and emails could be scams, so watch out for them. You can stop phone calls through the National Do Not Call Registry at https://www.donotcall.gov/. Never click on links within emails whose addresses you do not recognize. Some are "phishing" scams that are trying to access personal information on your computer. Identify them as "junk" in your email or forward them to spam@uce.gov.

7: Be social media savvy

Some identity thieves might be trolling around social media sites looking for identifying information or vacation pictures indicating that you are not home. Information on social media sites is often used to figure out passwords. Make use of social media privacy settings and save your "wish your were here" photos for once you return home.

8: CREATE DIFFICULT LOGINS AND PASSWORDS

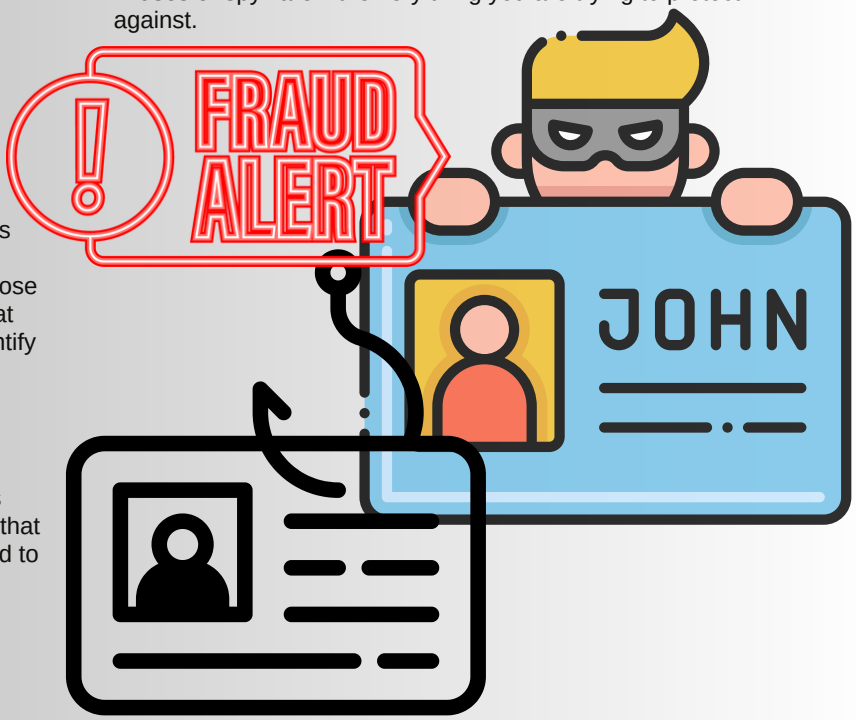
Identity thieves can access your information by hacking into your computer by decoding your passwords. Keep your passwords safe by avoiding family names, important dates, or any words that can be found in a dictionary; keep them long; use a combination of letters, number and symbols; and change them monthly. Also avoid using obvious keyboard patterns for your passwords: 1qazxsw2 or qwerty, for example. Do not store you passwords on your computer. The same applies to your cell phone. While it is a pain to enter a password every time you open your phone, this will provide you with some security in the event that your phone is lost or stolen. Also, take advantage of system updates to make sure your phone has the latest security systems.

9: USE ONE CREDIT CARD FOR ONLINE SHOPPING

Once a hacker is successful, he or she can start making use of credit cards that you use for online purchases. To reduce this risk designate one credit card for all purchases you make online. And remember; never use a debit card online.

10: KEEP YOUR SECURITY, VIRUS AND SPYWARE SOFTWARE UP-TO-DATE

It's easy to skip over the prompts to update software. Don't. Take the time to update your security, virus, and spyware software when prompted. Do not click on links that pop up when you are online claiming to be security updates. These may be links to viruses or spyware—the very thing you are trying to protect against.



Today's Lesson:

SCAM VOCAB 101

Pharming

When hackers use malicious programs to route you to their own sites — even though you've correctly typed in the address of a site you want to visit. The software stealthily diverts you to a look-alike destination, typically with the goal of gathering personal information for identity theft.

not to be confused with

Phishing

The use of authentic-looking emails, often purporting to be from a bank or government agency, to trick you into responding with sensitive personal data.

vishing

which rhymes with

Short for "voice phishing," it's the use of recorded messages to telephones — usually claiming to be from a bank — with the goal of tricking you into revealing personal or account information for identity theft.

smishing

aaaaaand.....

Named for the SMS (short message service) technology used to send text messages, it means phishing attempts made on cellphones.

Extra Credit Words

Cramming

The illegal placement of unauthorized charges on your telephone bill for unrequested services or calls not made.

Skimming

The capturing of information from the magnetic stripe on your ATM and credit card by use of portable "skimmer" devices that are secretly installed on card-reading machines.

Spoofing

Any situation in which scammers masquerade as a specific person, business or agency. The term is typically used to describe the manipulation of telephone Caller ID to display a false name or number for the caller.

*all verbs this week

*Test on Friday!