Scams & Cyber Threats

In the classic musical production The Music Man, con man Harold Hill frightens a town’s folks into believing that they’ve got “trouble, right here in River City!” Once he has them quaking in their boots, he’s right there with a solution, for a price. Grifters and con men show up everywhere, including the world of technology. There are many different types of scams that try to convince you to send money or enable access to financial accounts. Scammers today use phone calls, emails, text messages, websites, pop-up ads, and postal mail. Most scams do not have a happy ending like the movies.

Common Scams

- #1 Phishing - Use an official-looking email, phone, or website saying your account has a problem, been hacked, or will be shut down immediately. They get victims to click on a link, call, or open an attachment to get your account, password, and financial information. Tip: Hang up and do not click on any link. Use an alternate method to contact the company that sent you the email and ask if your account has been compromised. Don’t use the phone number in the email that was sent to you or in a pop-up message. Check a past bill or statement for accurate contact information.
- #2 Tech support scams - You receive an unexpected call or pop-up message on your computer warning of an issue, such as a virus, malware, or a device is not protected. The caller or pop-up claims to be from tech support and asks for access to your computer to fix the issue. Typically, the scammer will ask you to type a specific command to enable this access. Once they have control of your computer, they may require payment for technical assistance, install malicious software, change settings to leave your computer vulnerable, sell you unneeded software, or ask you to log on to your bank account to steal your financial information. Tip: Beware of scammers impersonating a tech support company, fraud department, or a government agency. Never give them control to your computer or logon info.
- Friend/family member imposter - You receive a call or email from someone that appears to be legitimate because the scammer knows specific information about you, your family, and friends. Scammers trick you into believing they are a friend or family member, claiming to need money for an emergency, such as posting bail, paying a hospital bill, or being detained at an airport. Scammers pressure you to send money immediately through an online wire or other payment service. Tip: Contact your friend or family member directly to confirm the caller's story.
- IRS scam – You receive a phone call claiming to be the IRS that you owe money. They demand you pay immediately or you will be arrested. Tip: The IRS never calls and demands money or gift cards.
- Online dating - Scammers use online dating sites, social networks, and chat rooms to meet potential victims. They create fake profiles to build online relationships and eventually request you send money due to a hardship. Tip: Do not give personal information, account numbers, or credit card information to someone you recently met online.
- Online loan scams - Beware of loan offers on social media or online ads. It usually is a scammer impersonating a loan company who is looking to empty your bank account once you share your financial data. Watch out for warning signs, such as the lender demanding a prepaid debit card or pressuring you to act immediately. When applying for a loan, go to a trusted website instead of clicking on a link in an ad.
- Ransomware - You unknowingly download a type of malicious software to your computer. This software is designed to block access to your operating system and all the information stored on your PC until you pay a sum of money to an online criminal. Tip: Back up your data regularly by syncing your files to a secure external drive or backup service such as cloud storage.
- Lottery or sweepstakes - You receive a phone call, email, or letter stating you have won a lottery or sweepstakes. Scammers require you to pay a fee to receive the prize to avoid taxes or additional fees, or may even threaten to report you to the IRS or police if you don’t make the requested payment. Tip: Legitimate lotteries pay taxes directly to the government rather than being reimbursed from winners’ proceeds.
- Check or account deposit - Scammers send you a fake check or make a deposit into your account. Once the money is deposited, you are asked to send all or a part of it back. After you send the money, you find out that the check bounced or the deposit is fraudulent. Note: You are responsible for the full amount of the check you deposited and associated check fees if it bounces. It may typically take up to 10 business days for a check to be discovered as fraudulent and returned to your bank.

Tips to Protect Yourself

It's easy to feel that scams and threats are beyond hope, but don't give up hope.

- Be wary of get-rich-quick schemes, huge discounts, or low prices. If an offer seems too good to be true, it probably is.
- Watch for language that creates unnecessary urgency action. Their goal is to get you to act without first thinking it through carefully.
- Don’t send money or giving your account information to anyone you don’t know. Be wary of an unexpected request for payment for a good, service or fee through any form of communication.
- Don’t send money back to someone who has provided a check or overpayment for goods or services.
- Use secure websites and apps for payments and shopping, and only with merchants you trust.
- Don’t trust your caller ID or an email address, the name and number can be faked/spoofed.
- Keep security patches and anti-virus software up to date for your computer, internet browsers, and mobile devices.
- Don’t automatically download any attachments – be sure to turn off this setting.
- Don’t click on links, open attachments, or provide sensitive information through a suspicious email or text message, even if the sender appears to be a reputable company or someone you know. Access a company’s website by using a reputable search engine, an old Bookmark you have in your browser, or your Password Manager.
- Never give control of your computer to anyone who contacts you.
- Don’t rely on caller ID. Scammers can spoof the name of a company to make the call seem legitimate.
- Never pay or donate using a gift card, prepaid card, Zelle, Venmo, or Crypto currency, it’s a scam.
- Protect your passwords and create strong passwords that are different for each site/app, change them routinely, and never reuse old ones. Strong passwords should be impossible for a hacker to guess. Never use family names, phone numbers, birth dates, or other social info that can be found on Facebook or other sources. Use a password manager like BitWarden (free version), https://bitwarden.com/, to manage passwords across all your devices. It auto-fills forms, performs auto-logins, and secures your data, and it's all ruled by one master password. DO NOT use the save password feature in most browsers.
- Enable two-factor authentication (2FA) where you will use a secondary form of authentication like a Text message, phone call, or eMail. This is especially important on financial and banking sites.
- Use a mobile-based payment system like Apple Pay or Android Pay, which is more secure than using physical credit card numbers that might be stolen. PayPal can also be used instead of providing your credit card.
- Watch your credit card and bank statements for unexpected charges and payments. Turn on alerts/notifications from your bank, brokerage, and credit cards. Most also let you set transaction limits if you get too many alerts.
- You can request one free credit report a year from the three credit services: Equifax, Experian and TransUnion at: https://www.annualcreditreport.com Look for unusual activity, such as the appearance of new accounts. Space out the three requests so you check every four months from a different service.
- Freeze your credit to stop anyone from opening credit and requesting loans and services in your name. You can unfreeze your credit as needed. Experian: https://www.experian.com/freeze/center.html
  Equifax: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
  TransUnion: https://freeze.transunion.com/sf/securityFreeze/landingPage.jsp
- Check if your info has been stolen. The site https://haveibeenpwned.com/ (an Internet slang term used to describe defeat) provides a comprehensive list of major data breaches.
- Install the Google Chrome extension “Password Checkup” to tell you if your passwords were hacked. It looks at the username and password you’re using and warns you if the data is already exposed.
  https://bgr.com/2019/02/05/google-password-checkup-chrome-plugin-will-identify-hacked-passwords/
- Sign up for a credit monitoring service that constantly monitors your credit report on major credit bureaus and alerts when it detects unusual activity. To help with the monitoring, you can set fraud alerts that notify you if someone is trying to use your identity to create credit. A credit-reporting service like LifeLock can cost $10 to $30 a month or you could use a free service like the one from Credit Karma: https://www.cnet.com/news/best-identity-monitoring-services/
- Make sure to have an Anti-Virus installed, updated, and configured correctly.
- Keep device OSs and apps updated. Old versions have vulnerabilities.
- For your tablet or phone, never download apps from outside Google Play or Apple App Store. They do the work of screening apps for you.
- Be mindful of every app you install and what permissions you give it like data/files, contacts, or photos.
- Encrypt your laptop and use a password to login.
- Assume Texts/SMS and eMails are public, DO NOT SEND passwords, Social Security number, or other confidential info. If security is needed use encrypted/secure apps, sites, and services.

- Public Wi-Fi networks at a coffee shop or Doctor's office are PUBLIC and may expose personal information like IDs and passwords. Use your SmartPhone hotspot if you need a secure network.
- If you use a public or Carondelet PC, log off when you are finished and close the browser completely.
- Use an eMail account like Gmail that notifies you when your account has been used on a new device. If it was not you using a new device, you should immediately change your password.
- Consider one email dedicated to signing up for apps that you want to try, but which might have questionable security or which might spam you. After you've vetted a service or app, sign up using your permanent email account. Many sites use your email address as the account username, but some let you select your own username. Consider using a different username every time. A password manager has no trouble using the right username and password. You can get free eMails accounts from sites like Gmail.com, Microsoft Mail, etc.
- Phone Scams – Block numbers, hang-up, never give account info, and never send money or gift cards. Only answer calls from businesses and people in your contact list. Others can leave a voicemail.
- Facebook data – Any friends or companies you "Like" have access to all your personal info, contacts, location, etc. Limit what you "Like". Only fill out required fields in your account and consider using false info for dates like a birthday. You can limit some exposure in the Privacy Settings. Do not use your Facebook as a login for other apps. Setup a new account and password for each app so they do not get access to your info.
- Browser – To limit tracking use the Private/Incognito mode found in most browsers.
- A virtual private network "VPN" can help protect your privacy especially when you're on a public Wi-Fi. I do not see a need other than a public Wi-Fi connection and the overhead and problems it can cause it not worth the trouble for other connections.
- As they say, if you're not paying for a site, app, or service, then you are the product. Those sites, apps, and services work hard to monetize your info.
- Be cautious in downloading browser extensions, and delete ones they no longer need. Eight widely used browser extensions have been caught harvesting data from an estimated 4 million consumers who used the browsers Chrome and Firefox. The extensions collected a host of information that wasn't authorized by either browser, exposing not only complete browsing histories but also access to files such as tax returns, medical records, credit card information, and other highly sensitive data. All the extensions have been remotely removed from or disabled in consumers' browsers and are no longer available for download, but hackers are always working on new attacks with new extensions.

Additional Links and Information

Carondelet Tech Help Resources: https://carondeletvillage.org/tech-help-resources/
Questions or comments can be sent to TCKreuzer@gmail.com