Phone Scams

Never provide a password, PIN number or account number over the phone
Never discuss your banking transactions with someone who calls from your bank

- even if they know the name of your bank
- even if the caller ID looks authentic

Never provide name, address, Social Security No., birthdate, etc. to any caller

- no matter how familiar or trusted the company or person is to you
- no matter how good their excuse is

Do not reply to a text from a number not saved in your phone contacts
Do not send financial or personal information by text
Never discuss your computer with a caller from "Tech Support"

- even if they know you have a certain computer such as Microsoft
- even if they are calling to help you avoid or fix a security breach
- even if you are having a computer problem

Never buy a gift card or send cash to someone who requests it on the phone

- even if they sound like a friend or family member
- no matter how desperate their excuse is

If a caller wants something from you, gets upset or makes you uncomfortable:

- hang up immediately and stop answering calls
- don't rely on caller ID; check the number in your own phone records
- once verified, call back if appropriate; a legitimate caller will understand

Email Scams

Never provide any information by email that you wouldn't give on the phone
Do not even open an email from a sender you do not recognize
Do not click on any links, download files or click on attachments sent by email

- even if you know the sender (call the sender first to verify)

Do not call phone numbers provided in emails

- even the email looks legitimate
- if an email requires you to make a call, get the number somewhere else

Before replying to an email, double-check the email address to see if it was faked
Never buy a gift card or send cash to someone who requests it by email

Credit Card Scams

Limit use of debit cards (since they expose your entire account to scammers)
Never use debit cards at gas station pumps or outside ATMs (to avoid skimming)
Never let your credit card out of your sight at restaurants or vendors
Completely destroy old credit and debit cards as soon you as replace them
Check your bank statements regularly for unauthorized charges
Enroll in alert notifications for mobile banking or credit card transactions

LOWENHAUPT & CHASNOFF, LLC
ATTORNEYS AT LAW

Social Media Scams

Do not accept friend requests from people you don't know
Remove "friends" who ask for anything (they are probably hackers)
Do not purchase items over social media
Never click on hyperlinks in social media posts
Do not tag your location in photos at home or on vacation
Set your social media profile settings to "private"
Do not profile your birthday, pet name, favorite teams, hometown, employer, etc.
Never accept direct messages from strangers

Internet Scams

Never use public or shared WiFi at coffee shops, airports, libraries, etc.
Only browse secure online websites that have a "lock" icon and start with https://
Never download software or apps unless you can verify the source
Never use your credit card on a webpage that offers low-cost products
Never make a purchase from a pop-up box
Never supply financial or personal information online
Never sign into an account using a link in an email or text
Check your online accounts regularly for unauthorized transactions
Use different passwords for different websites and accounts

Other Things You Can Do

Have a trusted person you call before you take any action out of the ordinary
Ask your bank to add safeguards to protect your accounts
Lock your devices with a passcode, and use Touch, Face or Voice verification
Use random, hard-to-guess passwords and change them often
Never store passwords or personal information on your phone, iPad or devices
Shred all documents with personal and financial data
Use secure mailboxes, collect your mail daily and set up mail forwarding
Factory reset and wipe any electronic device before selling or discarding
Lockdown your credit with the major credit bureaus; review your credit report
Hire a professional IT Technology company to:

- Install an Anti-Phishing Toolbar
- Keep your browser updated with security patches
- Use high-quality firewall desktop firewall and network firewalls
- Install antivirus software and keep it up to date
- Activate Two-Factor Authentication (2FA)
- Secure your home router with a strong password and WPA/2/3
- Consider using a VPN (virtual private network)

Call us if you need help at (314) 241-5950

LOWENHAUPT & CHASNOFF, LLC
ATTORNEYS AT LAW