THE FINANCIAL SERVICES NETWORK

TIPS FOR PREVENTING FRAUD

Cybercrime and fraud are serious threats and constant vigilance is key. While the financial institutions you do business with play an important role in helping protect your assets, you can also take action to protect yourself and help secure your information. This checklist summarizes common cyber fraud tactics, along with tips and best practices. Many of these suggestions may be things you're doing now, while others may be new. We also cover actions to take if you suspect that your personal information has been compromised.

WHAT YOU CAN DO

- Be aware of suspicious phone calls, emails, and texts asking you to send money or disclose personal information. If a service rep calls you, hang up and call back using a known phone number.
- Never share sensitive information or conduct business via email, as accounts are often compromised.
- Beware of phishing and malicious links. Urgent-sounding, legitimate-looking emails are intended to tempt you to accidentally disclose personal information or install malware.
- Don't open links or attachments from unknown sources. Enter the web address in your browser.
- Check your email and account statements regularly for suspicious activity.
- Never enter confidential information in public areas. Assume someone is always watching.

EXERCISE CAUTION WHEN MOVING MONEY

- When dealing with your investment advisor, call their office so they can help you directly.
- When working with your bank or other financial accounts, review and verbally confirm all disbursement request details thoroughly before providing your approval, especially when sending funds to another country. Never trust wire instructions received via email.

ADHERE TO STRONG PASSWORD PRINCIPLES

- Don't use personal information as part of your login ID or password and don't share login credentials
- Create a unique, complex password for each website. Change it every six months. Consider using a password manager to simplify this process.

MAINTAIN UPDATED TECHNOLOGY

- Keep your web browser, operating system, antivirus, and anti-spyware updated, and activate the firewall.
- Do not use free/found USB devices. They may be infected with malware.
- Check security settings on your applications and web browser. Make sure they're strong.
- Turn off Bluetooth when it's not needed.
- Dispose of old hardware safely by performing a factory reset or removing and destroying all data storage devices.

USE CAUTION ON WEBSITES AND SOCIAL MEDIA

- Do not visit websites you don't know, (e.g., advertised on pop-up ads and banners).
- Log out completely to terminate access when exiting all websites.
- Don't use public computers or free Wi-Fi. Use a personal Wi-Fi hotspot or a Virtual Private Network (VPN).
- Hover over questionable links to reveal the URL before clicking. Secure websites start with "https", not "http".
- Be cautious when accepting "friend" requests on social media, liking posts, or following links.
- Limit sharing information on social media sites. Assume fraudsters can see everything, even if you have safeguards.
- Consider what you're disclosing before sharing or posting your résumé.

THE FINANCIAL SERVICES NETWORK

HOW YOU CAN WORK WITH YOUR FINANCIAL ADVISOR TO PROTECT YOUR INFORMATION AND ASSETS

- **Keep them informed** regarding changes to your personal information and financial status.
- **Expect them to call you to verbally confirm electronic requests** to move money, trade, or change account information.
- **Expect them to ask for personal information** to verify your identity if there are suspicious activities regarding your accounts.
- **Help them by identifying trusted contacts or family members** in case they have concerns about financial manipulation.

WHAT TO DO IF YOU SUSPECT A BREACH

- Call your financial advisor immediately so that they can watch for suspicious activity and collaborate with you on other steps to take.

LEARN MORE

- Visit these sites for more information and best practices:
- StaySafeOnline.org: Review the STOP. THINK. CONNECT™ cybersecurity educational campaign.
- OnGuardOnline.gov: Focused on online security for kids, it includes a blog on current cyber trends.
- FDIC Consumer Assistance & Information, https://www.fdic.gov/consumers/assistance/index.html.
- FBI Scams and Safety provides additional tips, https://www.fbi.gov/scams-and-safety.

CONSIDER FREEZING YOUR CREDIT

1. If you are not going to be making any utilizations of your credit, consider freezing your credit with all of the major branches
2. To place a freeze on your credit reports, you need to call the credit reporting companies. There are three main ones: Equifax, Experian and TransUnion — and one smaller one, Innovis.

Keep in mind, credit freezes take time and cost money. To change the status, generally it can take upwards of 5 business days to process. A credit freeze CAN be lifted, however, that lift will cost money, and generally takes 3-5 business days to process. Keep this in mind if you are moving, buying a car, or applying for a new credit card.

Here are the numbers to call:
- Equifax — 1-800-349-9960
- Experian — 1-888-397-3742
- TransUnion — 1-888-909-8872
- Innovis — 1-800-540-2505

ADDITIONAL INFORMATION ON CREDIT FREEZES:

If you would like to know more about credit freezes with each of the major branches, please use the links below to gain a better understanding of each of their procedures.
- For Equifax. - https://www.equifax.com/personal/credit-report-services/
- For Experian - https://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/security-freeze/
- For TransUnion - https://www.transunion.com/credit-freeze
- For Innovis - https://www.innovis.com/personal/securityFreeze