Avoiding Financial Scams and Identity Theft Slams

Provided by Joseph D'Urso, AIF®

WHO ARE THEY?

- ***Financial fraudsters*** are after your assets.
- ***Identity thieves*** steal your personal information (often to then commit financial fraud).

WHAT DO THEY WANT? YOUR MONEY AND YOUR LIFE

- Social Security Numbers, passports, driver's licenses, and similar identifying information.
- Financial account and credit card numbers.
- Passwords (or insights about you that help them guess at weak ones).
- Your and family members' contact information (name, address, phone, e-mail).
- Your and family members' birth dates.
- Details about your life (interests, travel plans, relationships, your alma maters, etc.).

HOW WILL THEY GET IT? HOWEVER THEY CAN!

- Real or virtual strong-arm theft; breaking and entering; and scams to trick you.
- Strangers, strangers posing as someone you know, or someone you do know.
- Online, by phone, in the mail or in person.
- ***Phishing*** emails and deceitful or compromised websites (tricking you into clicking on bad links or opening infected attachments).
- ***Malware*** infects your device with pranks, viruses and security breaches.

WHAT SHOULD YOU LOOK FOR? TEN RED FLAGS

1. An offer that sounds too good to be true.
2. A stranger who wants to be your real or virtual best friend.
3. When someone you know is behaving oddly via email or phone. (It may be an identity thief.)
4. Someone claiming to represent a tax agency, financial or legal firm, police department or other authority contacts you out of the blue, demanding money or information.
5. You're feeling pressured into responding RIGHT AWAY to a threat, temptation or curiosity.
6. You're prioritizing easy access over solid security (weak or absent locks and passwords).
7. You're sharing personal information in a public venue (including social media).
8. Facts or figures aren't adding up; bank statements, reports or other info is missing entirely.
9. Your defenses are down: You're ill, injured, grieving, experiencing dementia or feeling blue.
10. ***Your gut feel is warning you: Something seems off.***

WHAT CAN YOU DO? QUITE A LOT!

Online Protection

- **Software:** Keep your anti-malware, anti-spyware and operating system software current!
  Backups: Use multi-version backup software for system and/or file recovery as needed.

- **Passwords:** Create long, strong, unique passwords; periodically change them, and use a reputable password manager to store them more securely.
- **Extra security:** Use it when available, such as two-step verification or fingerprint access.
- **Phishing:** Be careful about clicking links or opening attachments, especially from strangers.
- **Social media:** Privatize your profiles and activities so only those you allow in can see them.
- **WiFi:** Be extra careful using public WiFi; assume the world can see what you're doing.

Suspicious Phone Calls

- **Identify:** Legitimate callers don't call unannounced and entice or threaten you.
- **End the call:** Your best line of defense is to immediately hang up.
- **Don't cooperate:** Never share your credit card number or any other sensitive information.
- **Investigate:** End the call and contact the alleged source directly to inquire further.
- **Report:** Report the suspicious number to federal authorities.

Credit and Records Management

- **Watch for inconsistencies:** Look for odd transactions in your financial statements.
- **Watch for missing statements:** In case your account has been redirected elsewhere.
- **Monitor your credit reports:** Request and review your free AnnualCreditReport.com.
- **Consider a credit freeze:** If you rarely apply for loans, you may want to freeze your credit.
- **Follow up promptly:** If something seems "off," immediately change any login passwords, and promptly contact the service provider and appropriate federal authorities.

Personal Security

- **Remain on guard:** There is still plenty of old-fashioned theft going on.
- **Secure it:** Lock up your desk, files, car, mailbox and trash bins.
- **Shred it:** Use a micro-cut shredder to destroy any paperwork you do not need to keep.
- **When you're out and about:** Keep a close eye on your purse or wallet everywhere you go.
- **Filling in forms:** Don't provide your Social Security Number unless actually required.
- **Banking:** When using an ATM machine, look for others around you or signs of tampering.

WHAT IF THEY SUCCEED? ACT PROMPTLY

- **Online**: Promptly change passwords on any affected accounts; recover backups as needed.
- **In general**: Check in with any bank or other institution involved, and the government agency responsible for overseeing the breach: the IRS for tax fraud, or the FTC for anything else.
- **Financial**: If you feel your financial security has been compromised, we'll want to hear from you as well! We'll do all we can to help you fix the breach and minimize any damage done.

Joseph D'Urso, AIF® may be reached at 410-991-0252, joed@thinkpwm.com, or www.joedurso.net.