APOLLON

Cyber Security
&
Fraud Prevention

Cybersecurity

PREVENT

1. ***Strong Passwords:*** Use a combination of numbers, symbols and letters to form a long, complex password. Use unique passwords for each online login and regularly change all passwords.
2. ***Multi-Factor Authentication:*** If available, enable two-factor authentication for email, social media, financial accounts, etc. This functionality sends a one-time code to a mobile device to verify access, thus preventing unauthorized parties from accessing your account without the code.
3. ***Secure Wi-Fi Network:*** Avoid unsecure access to public Wi-Fi networks, such as in coffee shops, airports, hotels, etc. A virtual private network (VPN) creates a personal, private network across public networks.
4. ***Cautiousness with targeted telephone calls:*** Avoid divulging any banking or personal information to a caller over the phone and do not give in to pressure to take immediate action. The IRS and law enforcement agencies will not call you. Beware of the question "can you hear me" which leads to the recording of you saying "yes" to authorize unwanted charges, etc.
5. ***Safe Surfing*:** Only open emails, attachments, and links from people you know. Pay attention to a website's URL; hover over any links to see where they lead.

DETECT

1. ***Account Review*:** Open your credit card bills and bank statements right away. Check carefully for any unauthorized charges or withdrawals and report them immediately.

2. ***Review Your Credit Report:*** By law, you can obtain a free credit report every 12 months from www.annualcreditreport.com. According to the Federal Trade Commission, this is the only authorized source for the free annual credit report (though it will not include your FICO score). You should review your credit report for any discrepancies (unauthorized accounts, etc.).

REACT

If you have been a victim of identity theft:

- File a report with the local law enforcement agency.
- File Form 14039 (Identity Theft Affidavit) with the Internal Revenue Service.
- Contact one of the three credit bureaus (Equifax, Experian, TransUnion) to report the crime and freeze credit. Once one of the credit bureaus issues a fraud alert, the other two bureaus are automatically notified.

Fraud Prevention

Excerpts from “10 Things You Can Do to Avoid Fraud” by the Federal Trade Commission (FTC)

Spot imposters	Scammers often pretend to be someone you trust, like a government official, a family member, a charity or a company you do business with. Don’t send money or give out personal information in response to an unexpected request — whether it comes as a text, a phone call or an email.
Talk to someone	Before you give up your money or personal information, talk to someone you trust. Con artists want you to make rushed decisions. They might even threaten you. Slow down, check out the story, do an online search, consult an expert — or just tell a friend.
Don’t believe caller ID	Technology makes it easy for scammers to fake caller ID information, so the name and number you see aren’t always real. If someone calls asking for money or personal information, hang up. If you think the caller might be telling the truth, call back to a number you know is legitimate.
Consider how you pay	Credit cards have significant fraud protection built in, but some payment methods don’t. Wiring money is risky because it’s nearly impossible to get your money back; that’s also true for reloadable cards (like MoneyPak or Reloadit) and gift cards (like iTunes or Google Play). Government offices and honest companies won’t require you to use these payment methods.
Be skeptical of free trial offers	Some companies use free trials to sign you up for products and bill you every month until you cancel. Before you agree to a free trial, research the company and read the cancellation policy. Always review your monthly statements for charges you don’t recognize.
Sign up for scam alerts: *ftc.gov/scams*	Get the latest tips and advice about scams sent right to your inbox. If you spot a scam, report it at ftc.gov/complaint. Your reports help the FTC and other law enforcement investigate scams and bring criminals to justice.

APOLLON

Apollon Wealth Management, LLC (Apollon) is a registered investment advisor This document is intended for the exclusive use of clients or prospective clients of Apollon. Any dissemination or distribution is strictly prohibited. Information provided in this document is for informational and/or educational purposes only and is not, in any way, to be considered investment advice nor a recommendation of any investment product or service. Advice may only be provided after entering into an engagement agreement and providing Apollon with all requested background and account information. Please visit our website for other important disclosures.
http://apollonwealthmanagement.com

June, 2022