“Just your word and a handshake is all I need.”

Image Source: https://www.shutterstock.com/video/clip-21301288-detailed-close-up-business-partners-closing-deal-handshake - accessed 6/2/20.

What do you do for a living?

Image source- http://bit.ly/2Ixc5KC via https://blog.ipleaders.in/all-you-need-to-know-about-identity-theft-in-cyberspace-in-india/ - accessed 6/2/20.

Is it real?

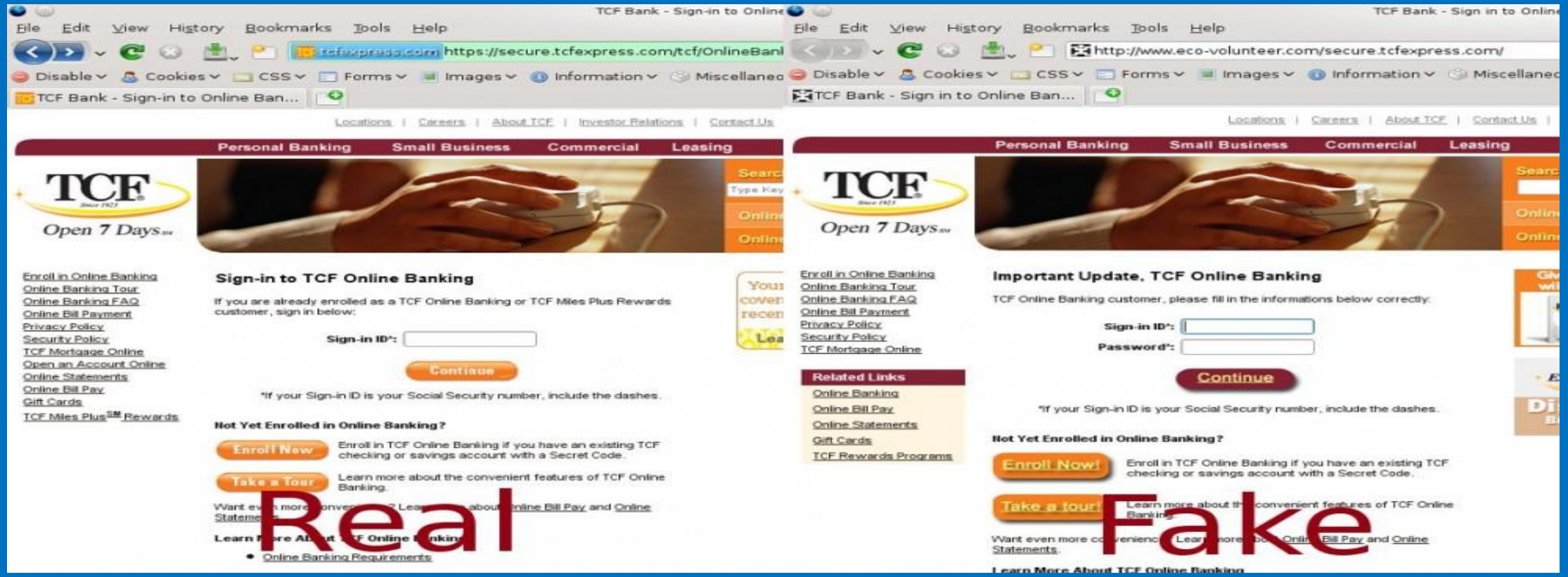


Image source: https://mtekk.us/archives/enemy-of-the-spammers/stupid-phishers-im-still-not-an-idio/attachment/real_fake_tcf/ - accessed 6/2/20.

“Trust, but verify!”

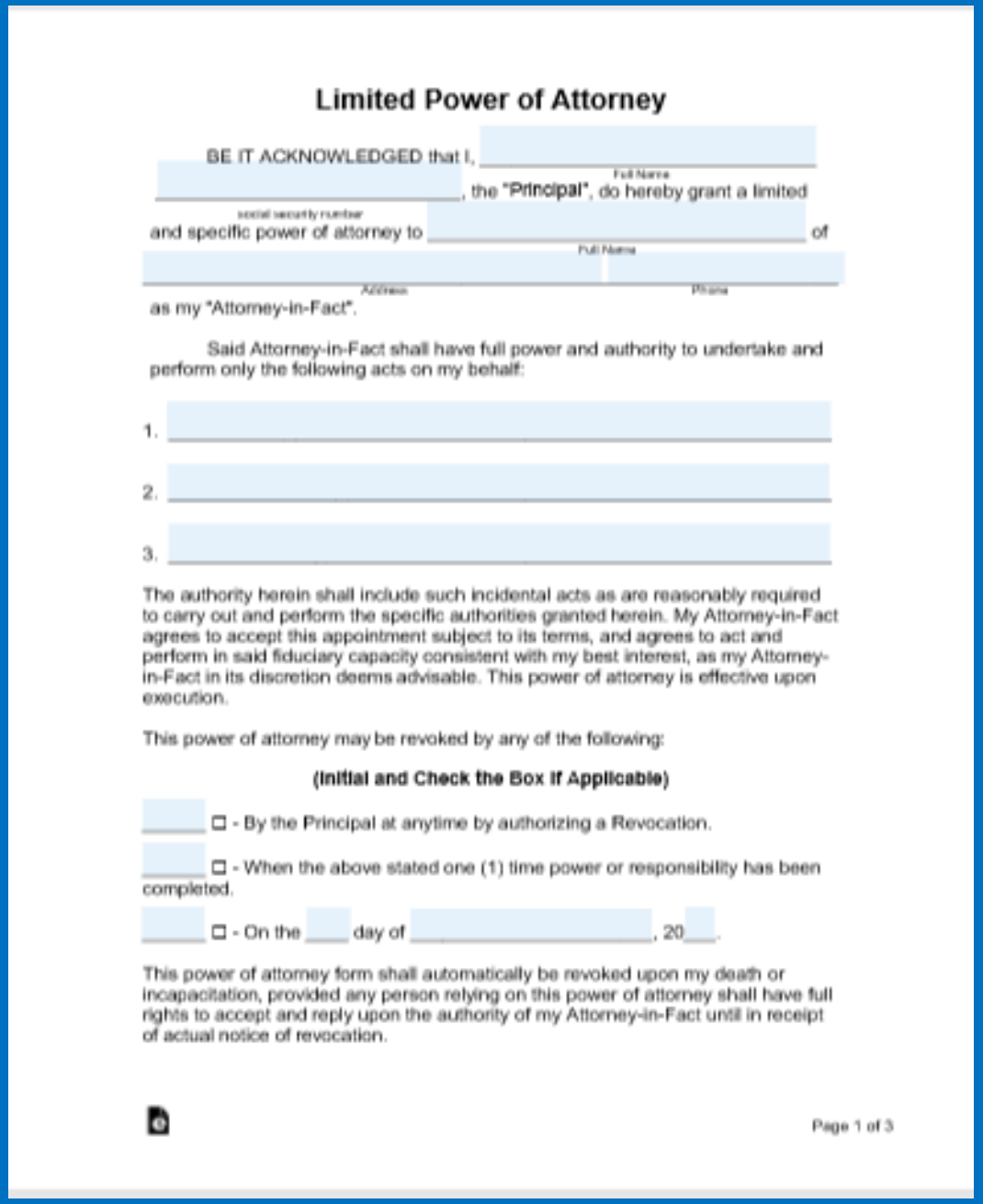
Image source: https://www.amazon.com/Ronald-Reagan-Framed-Photo-Verify/dp/B01LCJYCBU#ace-g0160871354 - accessed 6/2/20.

Undocumented transactions

Image source: https://www.pinterest.com/pin/705657835347014610/ - accessed 6/2/20.

AT HOME CARE & ASSISTANCE

- Just because you invited them to come to your home does not mean you should trust them.
- Ask the business/agency assisting you for a copy or where to access the rules and regulations with which their employees must abide.
- If they are shopping for you:
  - Order and pay online via a secure website
  - Utilize gift cards
  - Confirm purchases/expenditures
- If you want to give them a gift – give it through the business or organization.



Limited Power of Attorney

BE IT ACKNOWLEDGED that I, _____ (Full Name) _____ (social security number), the "Principal", do hereby grant a limited and specific power of attorney to _____ (Full Name) of _____ (Address) _____ (Phone) as my "Attorney-in-Fact".

Said Attorney-in-Fact shall have full power and authority to undertake and perform only the following acts on my behalf:

1. _____

2. _____

3. _____

The authority herein shall include such incidental acts as are reasonably required to carry out and perform the specific authorities granted herein. My Attorney-in-Fact agrees to accept this appointment subject to its terms, and agrees to act and perform in said fiduciary capacity consistent with my best interest, as my Attorney-in-Fact in its discretion deems advisable. This power of attorney is effective upon execution.

This power of attorney may be revoked by any of the following:

(Initial and Check the Box if Applicable)

_____ ☐ - By the Principal at anytime by authorizing a Revocation.

_____ ☐ - When the above stated one (1) time power or responsibility has been completed.

_____ ☐ - On the ____ day of _____, 20___.

This power of attorney form shall automatically be revoked upon my death or incapacitation, provided any person relying on this power of attorney shall have full rights to accept and reply upon the authority of my Attorney-in-Fact until in receipt of actual notice of revocation.

Page 1 of 3

Image source: https://eforms.com/power-of-attorney/limited/ - accessed 6/2/20.

LIVING ONLINE

Image source: https://learnenglishteens.britishcouncil.org/zh-hans/node/3801 - accessed 6/3/20

COMPUTERS

Image source: https://media.buzzle.com/media/images-en/photos/gadgets/computers/1200-22174724-tablet-and-desktop-with-laptop.jpg - accessed 6/2/20.

SMARTPHONES

Image source: https://www.androidheadlines.com/2014/11/samsung-apple-lg-top-smartphone-vendors-3q14.html - accessed 6/2/20.

We take the good with the bad

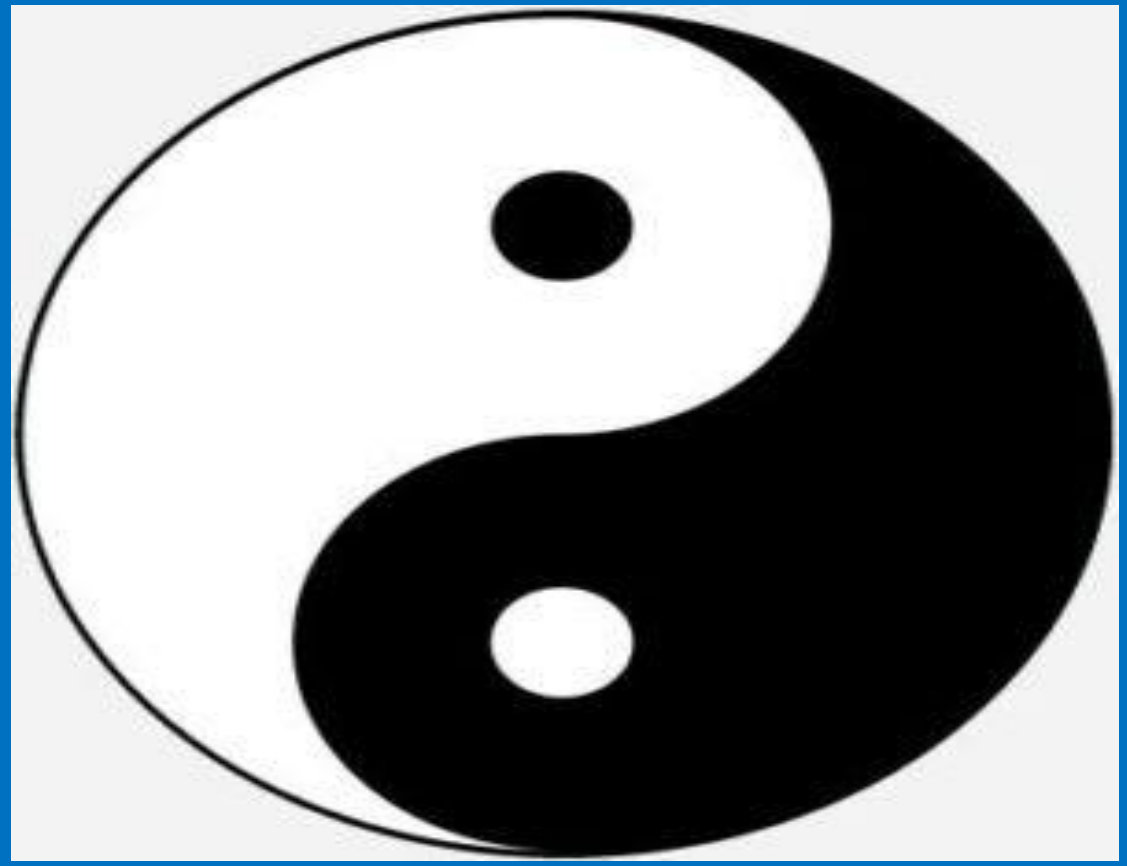


Image source: https://www.dictionary.com/e/pop-culture/yin-yang/ - accessed 6/3/20

Online Scams

2019 Online Crime By the Numbers

- FBI's Internet Crime Complaint Center – IC3 Report
  - 2019 revealed both the highest number of complaints and dollar losses
    - 467,361 Complaints (approx. 1300 a day)
    - $3.5 Billion in losses (individuals/businesses)

Source: https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 - accessed 6/5/20

Most Frequently Reported Complaints

- Fake emails trying to fraudulently obtain information
- Non-payment/Non-delivery scams
- Extortion

Source: https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 - accessed 6/5/20

Most costly type of complaints

- Business email compromise
- Romance/confidence fraud
- Spoofing

Source: https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 - accessed 6/5/20

An Ever Expanding Crime

- IC3 reported it is harder to tell the real from the fake when it comes to internet crime

- Result:
  - Drawing more criminals into this type of crime
  - Leading to more sophisticated attempts
  - Making internet crimes more successful
  - And therefore, more profitable

Source: https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 - accessed 6/5/20

Fake Site Contact Increasing

- People report arriving at fake sites with greater frequency
  - From search engine results

- IC3 warns users to be extremely skeptical/double check everything

Source: https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 - accessed 6/5/20

IC3's Recommendations

"In the same way your bank and online accounts have started to require two-factor authentication—apply that to your life."

"Verify requests in person or by phone, double check web and email addresses, and don't follow the links provided in any messages."

-Donna Gregory, Chief of IC3

Source: https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 - accessed 6/5/20

Lifewire.com's Top 10 Online Scams for 2020

1. Phishing Scams
2. Nigerian 419 Scams
3. Mystery Shopping Scams
4. Reshipping/Payment Processing Fraud
5. Pump and Dump Stock Scams
6. Hitman Scams
7. Ransomware Scams
8. Crowdfunding Scams
9. Technical Support Scams
10. Greeting Card Scams

Categories of Scams

- Three Basic Types
  - 1. Unsolicited requests to provide information or money
    - “I thought it was my bank”
    - “I thought I was giving money to . . .”
    - “They said I won money”
  - 2. Act now or . . .
    - Something bad will happen
    - Lose the chance/Limited opportunity
  - 3. I am looking for an accomplice, witting or unwitting
    - Cash this check/take this payment or accept this transfer for me and you can keep some
    - Do you want to make some extra cash fast?

Ex. #1 - PHISHING EMAILS

- Purpose: Have you voluntarily provide login credentials to a third party.
- Method: Email you from an apparent legitimate company
  - One you conduct transactions with
  - Inform you there is a problem with your account
  - Explains the need for security and what you need to do
  - Provide you a link to reset your password
  - Which requires you to provide your username and current password
- Problem: The site you provided your username and password to are fake
- Result: The scammer takes your current username and password, you provided, and accesses your legitimate account.

Combatting Phishing Emails

- Be wary of unsolicited emails from government agencies/companies you interact with
- Never click a link provided in an unsolicited email to comply with the sender's request
  - Access the government agency/company from your usual web address
    - Ie., from a bookmark/type known address in the browser/search engine search
  - Exception: Sometimes when you are logging on to a government agency/company site, they require you to click a link in an email
    - In this situation, you initiated the communication
    - So, it is less suspicious
    - Do so cautiously

Combatting Phishing Emails

- So, you are curious . . .
- If you want to check the legitimacy of a link
  - There are ways to do so without clicking on it
    - Hover over it without clicking on it
    - Use Checkshorturl.com
- Remember, if it is asking for personal identifying information
  - Does the address start with the secure tag HTTPS?

Ex. #2 – HITMAN SCAM

- Purpose: Have you pay a large sum of money.
- Method: Contact you with information they have been hired to kill you.
  - They provide personal information about you.
  - Likely obtained from social media platforms
  - Express willingness to not kill you in exchange for money.
- Problem: They are not a hitman, just a savvy scammer using fear to control your behavior.
- Result: You pay a large sum of money to prevent something that was never going to happen.

Combatting Hitman Scam

- Don’t panic.
- Re-read the communication multiple times.
- Do not reply to the communication.
- Report the communication to :
  https://www.ic3.gov/media/default.aspx
- If it persists, notify law enforcement

Ex. #3 – MONEY MULE SCAM

- Purpose: Have you pay a sum of money.
- Method: Contact you with information they need assistance with a transaction.
  - This scammer may be a newer online acquaintance.
  - They claim they need your help because they do not have a bank account.
  - Take their funds and deposit them in your account.
  - They then ask you to get pre-paid gift cards or wire an amount to cover the obligation.
  - Before the deposited amount clears your account.
- Problem: They never had legitimate funds for any transaction.
- Result: The amount your new “friend” paid to you is found to be fraudulent and you are out whatever money you fronted, as well as any fees your bank charges you.

Combatting Money Mule Scam

- Never accept money or a “job” from an online/social media acquaintance.
- Never send advance money to claim a prize or inheritance.
- Don’t trade funds with an online associate, due to some claimed necessity by the other party.
  - Or a promise you get to keep some of the funds.

KEEP CALM and Avoid Coronavirus Scams

Here are **5 things** you can do to avoid a Coronavirus scam:

Ignore offers for vaccinations and home test kits.

Scammers are selling products to treat or prevent COVID-19 without proof that they work.

Hang up on robocalls.

Scammers use illegal sales call to get your money and your personal information.

Watch out for phishing emails and text messages.

Don't click on links in emails or texts you didn't expect.

Research before you donate.

Don't let anyone rush you into making a donation. Get tips on donating wisely at ftc.gov/charity.

Stay in the know.

Go to ftc.gov/coronavirus/scams for the latest information on scams. Sign up to get FTC's alerts at ftc.gov/subscribe.

Federal Trade Commission

If you see a scam, report it to **ftc.gov/complaint**

GUIDELINES FOR PROTECTING YOURSELF IN AN ONLINE WORLD

- Regularly Update Your Software
- Protect Your Personal Information
- Protect Your Passwords
- Consider Turning On Two Factor Authentication
- Give Personal Information Over Encrypted Websites Only
- Back Up Your Files Regularly
- Proceed Cautiously

Source: https://www.consumer.ftc.gov/articles/0009-computer-security - accessed 6/2/20.

Two-factor Authentication

Source: https://swoopnow.com/how-does-two-factor-authentication-work/ - accessed 6/2/20

Encrypted Websites

- Examples:
  https://www.walmart.com/
  https://www.target.com/
  https://www.amazon.com/
  https://www.ftc.gov/
  https://www.irs.gov/

External Storage Devices

Image source: https://cdn.shoppers-bay.com/img/073ebcb28ee71112572cd434d3bea24d.jpeg - accessed 6/2/20.

Image source: https://www.everyusb.com/how-much-are-custom-usb-drives - accessed 6/3/20.

Cloud Storage

- What is the cloud?

Public WI-FI Networks

- High risk from multiple threats
- Don’t
  - Allow your Wi-Fi to auto-connect to networks
  - Log into any account via an app that contains sensitive information. Go to the website instead and verify it uses HTTPS before logging in
  - Leave your Wi-Fi or Bluetooth on if you are not using them
  - Access websites that hold your sensitive information, such as such as financial or healthcare accounts
  - Log onto a network that isn’t password protected
  - File share

Source: https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html - accessed 6/5/20

Securing Your Home Wi-Fi Network

- Password Protect It
  - Make it complicated
  - Limit disclosing it to others
  - Change it frequently
- Also Make Changes To:
  - Router's admin credentials
  - Network name
    - Hide it
- Use Encryption/Firewall
- Don't utilize
  - Plug 'n play
  - Remote management
  - Wi-Fi protected setup (WPS)
- Update Router Firmware
- Many More Options

Source: https://www.comparitech.com/blog/information-security/secure-home-wireless-network/ - accessed 6/5/20

FRAUD PREVENTION

- Ways to further reduce your risk:
  - Credit freeze
    - Best protection against ghost accounts
    - Consider the impacts
    - No protection for existing accounts

Source: https://www.consumer.ftc.gov/topics/identity-theft - accessed 6/2/20.

FRAUD PREVENTION

- Ways to further reduce your risk:
  - Fraud alert
    - Options
      - Not a victim – protects for 1 year
      - Victim – protects for 7 years
    - Upon verification of your authorization
      - Creditors can get a copy of your credit report

FRAUD PREVENTION

- Ways to further reduce your risk:
  - Identity theft protection services
    - Monthly fee to have someone watch your back
    - If you choose to do this, do your homework before signing up

FRAUD PREVENTION

- Virtual Private Network
  - What is a VPN?
  - Why consider using a VPN?
  - What concerns are there with using a VPN?
  - What should you look for when shopping for a VPN?

Source: https://www.consumer.ftc.gov/articles/virtual-private-network-vpn-apps – accessed 6/2/20

PROTECT DATA FROM OFFLINE THIEVES TOO!

- Require Passwords to Access All Devices
- Use the Time Lock Feature on All Devices
- Remember to Back Up and Wipe Data from Phones/All Memory Devices before Disposal
- Shred/destroy anything containing personal identifying information when done with it
- Be wary of providing too much personal identifying information over the phone or in person

Source: https://www.consumer.ftc.gov/topics - accessed 6/2/20.

Remember:

- Scammers
  - Can be savvy.
  - They can make crazy reasons/situations sound believable.
  - They get paid when people fail to think before they act.

- When confronted with an unsolicited online interaction involving money
  - Do not act upon it or respond immediately.
  - Take some time.
  - Think rationally through the situation.
  - Discuss with someone you trust.
  - Take steps to protect yourself.

Fraud Related Informational Websites

- https://www.ftc.gov/
- https://www.ic3.gov
- https://www.ncoa.org/
- https://www.lifewire.com/internet-networking-security-news-4796476

NOTICES:

- Images were sourced for this presentation.
  - Just because an image or information was referenced/utilized in this presentation does not mean that the Frederick County State's Attorney's Office approves or promotes the content of that website.
- The slide containing Fraud Related Informational Websites are recommended to you as resources where you can access more information related to online scams and fraud.
- Again, this presentation is informational only.
  - Services mentioned herein requiring a monthly fee or purchasing a product are not being promoted or warranted.
  - You should conduct your own research, assess the options, discuss with people you trust, and then implement your own plan for how you can safely operate online.
- Always proceed cautiously when making decisions about your personal affairs.

Friendly Advice

- Do not let the risks scare you completely away from technology.
- Take reasonable precautions.
  - Don’t spend a fortune for protection
  - Don’t worry endlessly about this
- Credit and financial institutions are pretty generous with their reimbursement policies if you are victimized.
  - Beware apparent voluntary cooperation situations
- Warn others regarding fraud related scams

REMEMBER IT IS ALWAYS BEST TO **STOP!**

- **S**top – Don’t act or respond right away.
- **T**hink – Does this make sense?
- **O**thers – Reach out to someone you trust and talk to them.
- **P**lan – If and how you are going to respond.

Elder Fraud Presentation June 2020 Host and Attenders

THANK YOU!

Jason S. Shoemaker
Chief Assistant State's Attorney
Economic Crimes Unit
State's Attorney's Office for
Frederick County, Maryland
100 W. Patrick Street
Frederick, MD 21701
Phone: 301-600-1523