DETER DETECT DEFEND

Best Practices for Safeguarding Your Online Presence and Digital Footprint

PLANNED FINANCIAL services
Your Life. Your Money. Your Way.®

In 2021, the FBI's Internet Crime Complaint Center (IC3) received a record 847,376 complaints from individuals, with potential losses exceeding $6.9 billion.[1] Fortunately, there are steps you can take now to help deter, detect and defend against identity theft, online fraud, scams and more—from securing your mobile devices, to backing up important data and keeping your Social Security number out of the hands of would-be criminals. Below are several tips and best practices you and your family members can use now to help safeguard your assets and your good name.

DETER identity theft by safeguarding your personal information

1. Reduce your paper trail – To avoid the theft of documents with personal information, such as pre-approved credit solicitations, medical and financial statements, etc.:

- Shred all documents, mail, cards, etc. prior to putting in the trash
- Leverage online statements and paperless options
- Visit **www.optoutprescreen.com** to sign up to reduce preapproved credit card offers

DID YOU KNOW?

The average American receives 41 pounds of junk mail each year, 44% of which is never opened.[2]

2. Carry only what you need – Consider removing the following from your wallet, purse or briefcase:

- Social Security card
- Blank checks
- Credit and debit cards that you don't use on a regular basis
- Receipts
- Passwords and pins
- Excess cash

3. Don't use obvious passwords – Your password is your first line of defense. Use multiple passwords and smart techniques:

- Minimum 8 characters and multiple character types
- Use phrasing, such as: Ilovemy2dogs!
- Utilize Multi-Factor Authentication (MFA) when available
- Use encrypted password storage applications
- Avoid using the same password for different apps or websites

4. Secure your mobile devices – The following tips can help you secure your smart phone, tablet or other mobile devices.

- Passwords:
  - Ensure you have a device password or fingerprint
  - Limit what can be accessed on the lock screen
  - Be cautious with autofill
- Location & Privacy:
  - Disable Location History/Significant Locations
  - Don't enable Location Services on all apps
  - Limit Ad Tracking and delete browser history
- Network Security:
  - Secure your home Wi-Fi network
  - Limit the use of unsecured networks when away from home or the office
  - Use WEP, WPA, or WPA2 wireless security protocols
  - Install Anti-Virus and Anti-Malware on your devices and networks
- Device Physical Security:
  - Utilize Find My iPhone or Android Device Manager
  - Allow Remote Wipe and Erase Data after password attempts
  - Consider third-party security tools

5. Keep information secure – Help protect your information from falling into the hands of scammers or thieves by backing-up important data on password-protected websites and destroying digital records before discarding or donating old devices.

- Social Media
  - Avoid posting personal information such as your age, date of birth, maiden name, relationship status, address or other unique identifying information where it can be viewed publicly on social media sites.

continued

Best Practices for Safeguarding Your Online Presence and Digital Footprint

DETER, continued

- Data Backup
  - Backup data to trusted sources, such as iCloud, Dropbox, Google Drive
  - Utilize local storage: external hard drive, CD/DVDs
- Digital Records:
  - Properly remove data from any device before selling or donating – smartphones, tablets, laptops, desktops, printers, copiers, etc.
  - Various software tools and methods are available to permanently remove data
    - Overwrite, erase, degauss, etc.
- Physically destroy the hard drive

DID YOU KNOW?

More than 95,000 people reported about $770 million in losses to fraud initiated on social media platforms in 2021.[3]

DETECT suspicious activity by monitoring accounts and billing statements

1. Be alert and proactive

- Immediately report lost or stolen credit/debit cards
- Review your credit reports annually
- Google yourself
- Regularly inspect financial statements for charges you didn't make
- Watch for credit card skimming devices on ATMs, gas pumps, etc.

2. Avoid phishing and email scams

- If something sounds too good to be true it probably is
- Don't click on links in emails that look suspicious or you weren't expecting
- Never send sensitive information via email – unless it's encrypted, it's not secure
- Turn off the preview pane in your email program to avoid opening suspicious emails
- Forward suspicious emails to **spam@uce.gov, phishing@irs.gov** or **reportphishing@antiphishing.org**

IRS
Department of the Treasury
Internal Revenue Service

DID YOU KNOW?

The IRS will not call you about unpaid taxes or penalties. Notify the IRS immediately if you suspect tax fraud at www.irs.gov.

DEFEND against identity theft as soon as you suspect a problem

1. Don't wait – Take immediate action when a problem occurs.

- Contact your bank or financial institution to report lost or stolen cards and/or fraudulent accounts or charges
- Enroll in credit monitoring
- Explore ID theft protection programs (LifeLock, Triple Alert)
- Freeze or place a fraud alert on your credit if you suspect fraudulent activity
- Close any accounts that have been tampered with or opened fraudulently
- File a police report if fraudulent accounts have been opened in your name
- Notify the Federal Trade Commission at **www.consumer.ftc.gov**

[1] FBI Internet Crime Report 2021
[2] www.41pounds.org/impact
[3] FTC.gov