DETER / DETECT / DEFEND

BEST PRACTICES FOR SAFEGUARDING YOUR ONLINE PRESENCE AND DIGITAL FOOTPRINT

RETURN ON LIFE® WEALTH PARTNERS

Your Life. Your Money. Your Way.®

As the world becomes increasingly reliant on digital technologies, cybercrime is surging. Fortunately, there are steps you can take now to help deter, detect, and defend against identity theft, online fraud, scams, and more. Below are several tips 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. before discarding
- Leverage online statements and paperless options
- Visit optoutprescreen.com to sign up to reduce preapproved credit card offers

DID YOU KNOW?

The cost of cybercrime is projected to surpass $12.2 trillion by 2031.[1]

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 you don't use on a regular basis
- 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 Multifactor 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 use a device password, fingerprint, or facial recognition
  - 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 WPA2 or WPA3 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
- Digital Records:
  - 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
- Physically destroy the hard drive

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.

DID YOU KNOW?

74% of account takeover attacks start with phishing.[2]

2. Avoid phishing and email scams

- If something sounds too good to be true it probably is
- Don't click on links in emails from unknown sources or that look suspicious
- 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
- Report deceptive spam by filing a complaint at reportfraud.ftc.gov, phishing@irs.gov or reportphishing@antiphishing.org

DID YOU KNOW?

According to the IRS, they will not call you about unpaid taxes or penalties. Notify the IRS immediately if you suspect tax fraud at 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 , such as LIfeLock, NordProtect, or Identity Guard.
- 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 consumer.ftc.gov

[1]Cybercrime Security Ventures: Cybercrime To Cost The World $12.2 Trillion Annually By 2031

[2]First Business Bank: How To Prevent Account Takeover Fraud

RETURN ON LIFE® WEALTH PARTNERS

Your Life. Your Money. Your Way.®

To learn more about managing risk and helping to protect the people and the lifestyle you cherish, schedule time to speak with a member of our team today or visit us online at **ReturnOnLifeWealth.com.**

Let's talk / 440.740.0130
ReturnOnLifeWealth.com
7000 Fitzwater Road, Suite 300 • Brecksville, Ohio 44141