



One Step Ahead

Strategies to Secure Personal
Information and Prevent Fraud

One Step Ahead

Data breaches, identity theft, credit card fraud, robocalls and spam text messages are increasingly commonplace in our daily lives. There are often simple actions you can take to help minimize your risk and prevent fraud. Learning these actions can put you in a better position to stay **One Step Ahead** with **Strategies to Secure Your Personal Information and Prevent Fraud**.

D.I.P. – Deter. Identify. Protect.

To stay one step ahead, it is important to **DETER** cyber criminals. **IDENTIFYING** how and where common scams happen will help you spot them before you fall victim. Finally, in the event you fall victim of fraud, ensure you know the steps to **PROTECT** yourself.



DETER



IDENTIFY



PROTECT

The Value of Your Information

The amount criminals are willing to pay for your information depends on the data they buy. Fraudsters may purchase your Social Security number for as little as **\$4** all the way up to over **\$1,000** for a full range of documents and account details.¹



Value of Your Data

- Social Security number: **\$4**
- Online banking logins: **\$40**
- Credit card details: **\$14-30**
- A full range of documents and account details: **\$1,000**
- Hacked Facebook account: **\$35**

1 in 50

children were victims of identity theft last year with victims losing

\$918 Million



DETER

One of the most impactful precautions you can take to help prevent becoming a victim of fraud is deterrence. The better you deter, the more likely criminals will redirect their efforts. To effectively deter, consider these three areas of general vulnerability where you can make a difference.

No-Tech

- Mail Theft
- Paper Statements
- Wallet/Purse

Low-Tech

- Credit Cards
- Passwords
- Social Media

High-Tech

- Hacked Smartphone
- App Data
- Online Data
- Wi-Fi Network

No-Tech

One of your greatest risks is the amount of paper containing your personal information.³ Frequently, mail or other documents end up in the trash where they are susceptible to falling into the wrong hands. Fortunately, there are resources that can reduce your paper trail.

Go to optoutprescreen.com
to reduce preapproved credit card offers
or call **1-888-5-OPT-OUT (1-888-567-8688)**

Go to catalogchoice.org
to cancel specific catalogs/paper mail

Low-Tech

Credit cards, social media and passwords are among the many areas targeted by cyber thieves. The good news is there are simple steps you can take to protect yourself.

Credit Card Best Practices

Most of us have had our credit card comprised at some point. While thieves sometimes target your physical card, the greater risk is accessing your personal credit card data. While cards are an area of risk, there are steps you can take to protect and monitor your credit card accounts.

Credit Card Tips

- Do not sign card - Ask for ID
- Designate one card for online/risky purchases
- Watch for skimmers
- Explore virtual account numbers

Credit Card Apps allow you to

- View transactions in real time
- Lock/Pause/Freeze your card
- Set custom alerts/thresholds

Social Media Best Practices

Many of us utilize social media to stay in touch with our community, family, friends and professional colleagues. While there are benefits to using these platforms, they come with risks. The information you post on social media can be used to exploit your personal information. For example, something as simple as sharing your vacation photos the same day they are taken alerts criminals that your home may be unoccupied. The best course of action is to think before you post.

Active social media users are **30%** more likely to be affected by identity fraud.

Snapchat, Facebook and Instagram users are at a **46%** higher risk.⁵

Password Best Practices

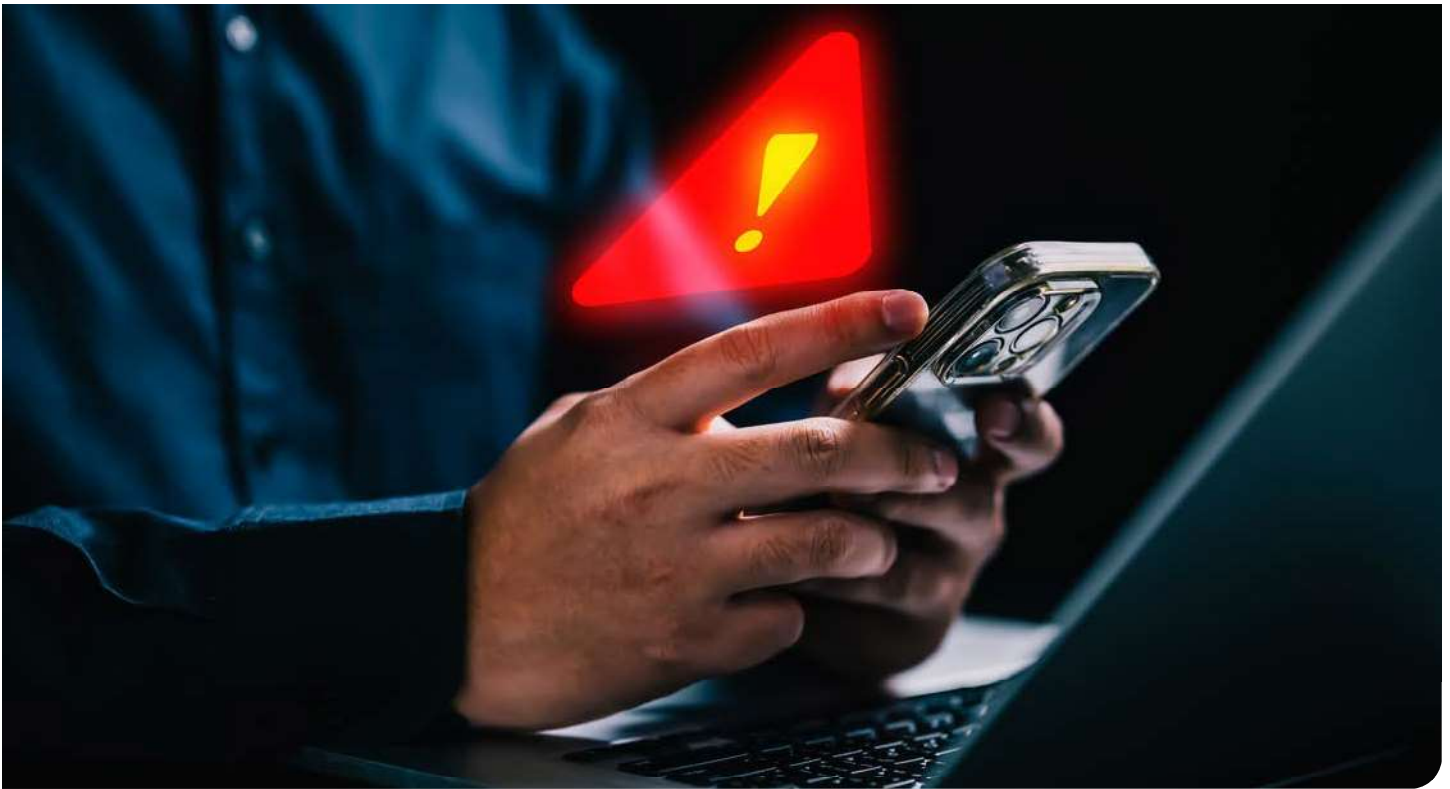
Criminals use technologies to crack passwords, which is why having a strong password is crucial as your first line of defense to protect your electronic information.

- Use unique passwords
- Minimum 12 characters and multiple character types
- Use phrasing: Ice-Cream4Dinner!
- Utilize multi-factor authentication when available
- Use encrypted password storage applications

Time it takes a hacker to brute force your password in 2024

Numbers of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481 k years	126bn years	2tn years	26tn years

Information provided by www.hivesystems.io/password



High-Tech

Cell phones are among the most utilized device that we own. They provide us with directions, keep our schedules, take pictures and allow us endless use of applications. Many of us have our passwords, credit card and personal information stored in some form on our mobile devices. Follow the critical steps below to protect your mobile phone.

Mobile Phone Best Practices - Securing your Device

Passwords

- Ensure you have a device password or fingerprint/eye scan
- Limit what can be accessed on the lock screen
- Be cautious with autofill

Location and Privacy

- Disable location history
- Enable locations services on apps where location is needed
- Limit ad tracking and delete browser history

Securing Physical Device

- Utilize Find My iPhone or Android Device Manager
 - Allow remote wipe and erase data after exhausting password attempts
 - Consider third-party security tools
-

Understand the apps on your phone

At this very moment, your smartphone is likely filled with apps that collect details about you, including you age, gender, political leanings, GPS data, internet browsing, social media activity and much more.⁶ Be cognizant of apps with the capabilities listed below.

- | | | |
|---------------------|---|-----------------|
| • Microphone access | • Audio recording | • Camera access |
| • Location tracking | • Ability to read call logs and text messages | |

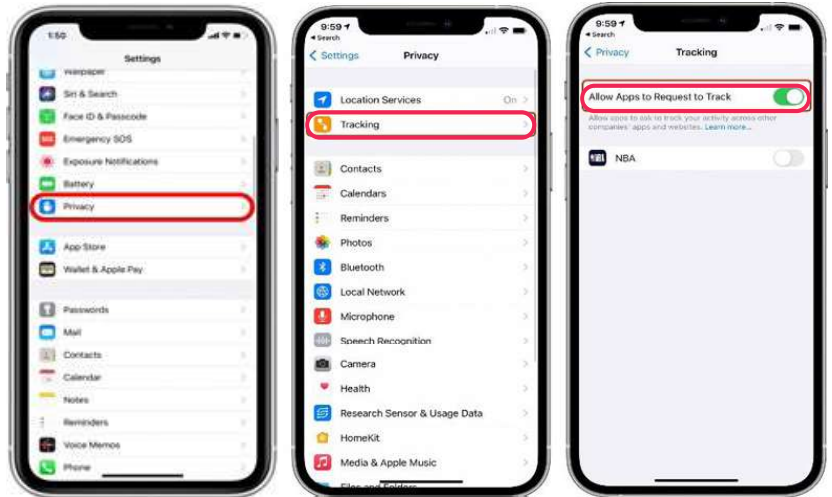
How to turn off app tracking

iPhone

- Go into Settings
- Choose Privacy
- Choose Tracking
- Turn off “Allow Apps to Request to Track”

Android

- Go into Settings
- Choose Apps
- Tap three dots on screen’s upper right corner
- Choose Special Access
- Choose Usage Data Access
- Turn off Data Tracking for apps



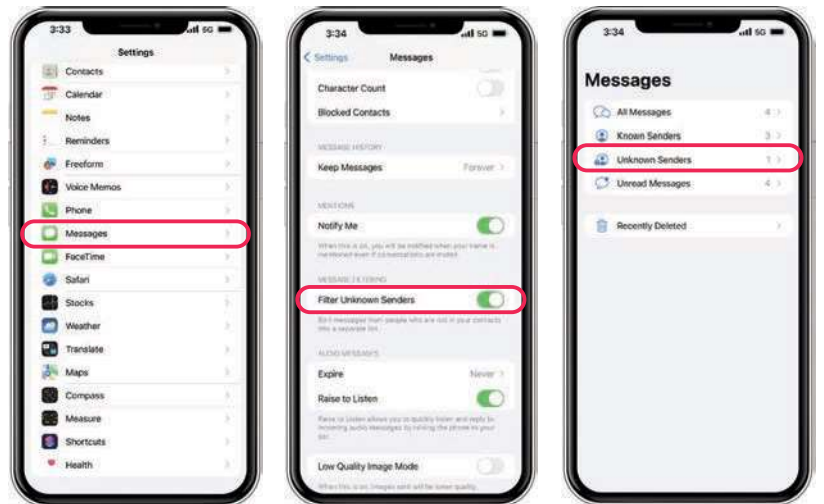
How to limit spam text

iPhone

- Go into Settings
- Choose Messages
- Turn on “Filter Unknown Senders”
- Go into Messages
- Select Known Senders list

Android

- Go into messaging app
- Tap three dots icon in upper right corner
- Tap Settings and then Spam Correction
- Select Enable Spam Protection



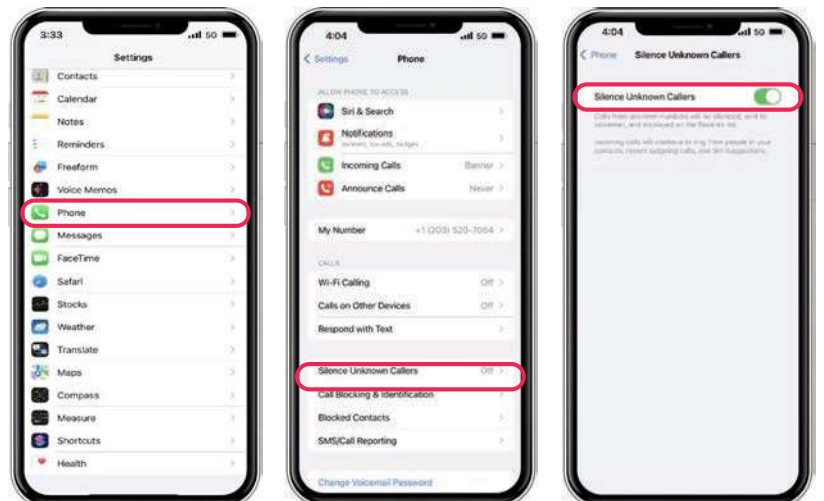
How to silence unknown callers

iPhone

- Go into Settings
- Choose Phone
- Choose Silence Unknown Callers
- Turn on

Android

- Go into Phone app
- Then Settings
- Blocked Numbers
- Turn on “Unknown”





IDENTIFY

Being proactive and alert concerning suspicious activity will help you identify attempts to defraud you. Here are the tools to help you identify fraud and protect yourself.

usps.com

Informed Delivery® – a free service

- Sign up to receive a daily email with images of your incoming mail
- Track and manage your packages in one convenient place

haveibeenpwned.com

- The primary function of haveibeenpwned.com is to provide the public with a means to check if their private information has been leaked or compromised. Visitors to the website can enter an email address and see a list of all known data breaches with records tied to that email address.

annualcreditreport.com

- The only authorized site where you can order the free credit report you are entitled to each year from each reporting agency. When asking for a credit report, you may need to provide certain personal information, including a Social Security number and information about monthly bills.

Identifying Common Scams

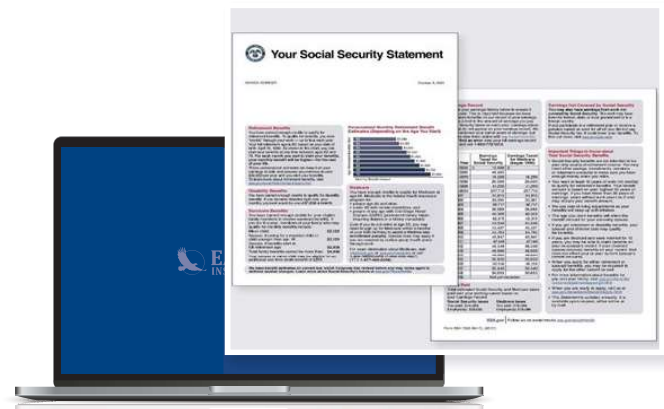
QR Codes

Criminals can replace legitimate QR codes with their own codes, often by simply printing one on a sticker and placing it over the real one. Parking meters and ticket vending machines are common targets of this scheme. When consumers scan this fake code, they are taken to a website that loads malware onto their devices or tries to trick them into entering credit card or other sensitive personal data.

Social Security Fraud

In recent years, Social Security fraud has been on the rise. With a full name, date of birth and Social Security number, thieves can claim Social Security benefits. For those waiting past age 62 to receive benefits and who do not check their statements, they may be unaware thieves are receiving their benefits.

ssa.gov/myaccount



Tax Return Fraud

By early March of the 2023 tax filing season, the IRS had already identified nearly 1.1 million tax returns with refunds valued at over \$6.3 billion as potentially fraudulent.⁷ Fraudsters will use real Social Security numbers and identities to file returns with fake data prior to the victim filing.

Tips on avoiding tax fraud⁸

- File your returns early
- Know your tax preparer
- Notify the IRS if you suspect tax fraud
- Know the IRS will NEVER call you about unpaid taxes





PROTECT

Deterring and identifying vulnerabilities will help you build a prevention strategy, but even the best strategies can be compromised. If you do become a victim, it is important to take action to limit the impact of identity theft and fraud.

Action Items for Fraud Victims

- **Place a fraud alert and freeze your credit**
 - Experian – **888-397-3742** – [experian.com](https://www.experian.com)
 - TransUnion – **800-680-7289** – [transunion.com](https://www.transunion.com)
 - Equifax – **888-766-0008** – [equifax.com](https://www.equifax.com)
 - Remember your PIN when you freeze your credit.
- **Close all affected accounts and/or change any relevant passwords**
- **File a police report**
- **Contact the Federal Trade Commission**
 - **IDtheft.gov**
 - **Reportfraud.FTC.gov**
 - **FTC: 877-438-4338**
- **Enroll in credit monitoring**
 - **LifeLock**
 - **Triple Alert**



Want to learn more?

Visit www.FTC.gov/idtheft for more information.

¹ www.prnewswire.com/news-releases/you-are-worth-1-000-on-the-dark-web-new-study-by-privacy-affairs-finds-301286467.html

² www.aura.com/learn/child-identity-theft#:~:text=According%20to%20Javelin%20Strategy's%202021,million%20to%20child%20identity%20theft.

³ www.41pounds.org/impact/c

⁴ www.cnn.com/2023/05/17/irs-flagged-more-than-1-million-tax-returns-for-identity-fraud-in-2023.html

⁵ www.security.org/digital-safety/credit-card-fraud-report/

⁶ www.identityguard.com/news/social-media-identity-theft#:~:text=In%20general%2C%20social%20media%20users,takeovers%20and%20fraud%20%5B*%5D.

⁷ www.washingtonpost.com/technology/2021/07/22/data-phones-leaks-church/

⁸ www.tigta.gov/sites/default/files/reports/2023-05/202340029fr.pdf

This material is for informational purposes only, and is not a recommendation to buy, sell, hold or rollover any asset. It does not take into account the specific financial circumstances, investment objectives, risk tolerance, or need of any specific person. In providing this information Eagle Life Insurance Company is not acting as your fiduciary as defined by the Department of Labor. Eagle Life does not offer legal, investment or tax advice or make recommendations regarding insurance or investment products. Please consult a qualified professional.

Not FDIC/NCUA Insured | May Lose Value | No Bank/Credit Union Guarantee | Not a Deposit | Not Insured by Any Federal Government Agency

6000 Westown Pkwy., West Des Moines, IA 50266 • 866-526-0995 • eagle-lifeco.com