



# How to protect yourself from identity theft

Your ultimate cheat sheet

Sharing personal data today means giving up control of it in hope that everything will turn out OK. Although, the risk of data theft and abuse never goes away. Here's what happens:



01

## PERSONAL DATA SHARING

You safely provide your details to a governmental or private organization. You may even share something on social media.



02

## PERSONAL DATA THEFT

Someone gets your personal information without your consent.



03

## IDENTITY THEFT

Someone uses your personal data to impersonate you for financial gain or other benefits.

## How to minimize your risk of data theft

Unless you live in social isolation, your data is shared across many different organizations. If your data hasn't been leaked, it's still safe. Here's what to do to keep it that way.

### DATA THEFT PREVENTION CHECKLIST

- Check if your online accounts were affected by data breaches  
Get regular checkups with MacKeeper's ID Theft Guard tool. Learn more on [mackeeper.com/privacy/](https://mackeeper.com/privacy/)
- Set up strong, unique passwords for all your accounts  
Change passwords quarterly
- Add multifactor authentication to your accounts wherever possible
- Delete unused accounts
- Check your sent folder for unusual outgoing emails  
Repeat weekly
- Install and use a reliable antimalware app
- Secure your home Wi-Fi with a strong, unique password
- Secure all devices with strong, unique passwords, PINs, or biometric protection  
Change passwords and PINs quarterly
- Enable mobile bank notifications
- Store paper documents securely
- Shred unnecessary documents  
Repeat quarterly
- Check your credit reports  
Review them three times a year
- Set reminders in your calendar for regular security review

### TIPS FOR MAXIMUM PROTECTION

- Don't use free public Wi-Fi; if you must, use a VPN
- Don't leave devices unlocked or unattended
- Upgrade your devices and get technical support only from trusted vendors
- Don't let strangers use your devices
- Don't use others' devices unless necessary; stay cautious
- Track, lock, or wipe your device if it's lost or stolen
- Be careful using social media and smart devices
- Share as little of your personal information as possible
- Request removal of your personal information from people search websites, like Whitepages
- Shop only from reliable websites; look for "https"
- Don't use autofill for payment details
- Don't open suspicious emails; if you do, don't follow the links or open attachments
- Set up a password manager
- Don't carry around documents you don't actually need
- Educate your kids and parents about data and identity theft



# How to protect yourself from identity theft

Your ultimate cheat sheet



01

## PERSONAL DATA SHARING



02

## PERSONAL DATA THEFT



03

## IDENTITY THEFT

### How to act in case of data theft

If your personal information is stolen, it's time to act quickly and attentively.

#### PERSONAL DATA THEFT CHECKLIST

If your personal data was exposed or stolen, but there are no signs of misuse, **use this list to minimize your risks.**

- Get breach details from the affected company or organization  
Be careful about email and phone data breach notifications—they can be fakes initiated by scammers
- Notify relevant organizations according to what data was stolen:
  - Your bank and creditors
  - Your health insurer
  - Credit reporting agencies
  - The Internal Revenue Service
  - The Department of Motor Vehicles
  - Utility companies
  - Other \_\_\_\_\_
- Request a new credit or debit card from your bank
- Place a fraud alert or a credit freeze on your credit report
- Check your bank statements for suspicious records  
Repeat weekly
- Request a credit report and check it for unusual records
- Review your Social Security statement
- Sign up for credit monitoring
- Update passwords and security questions for your accounts
- Request your medical records and check them for suspicious items  
Repeat quarterly
- File your taxes early  
Do so every year
- Set reminders in your calendar for regular security review

#### IDENTITY THEFT CHECKLIST

If someone is using your stolen records to impersonate you, **use the personal data theft list and these additional measures to regain your privacy.**

- Contact the Federal Trade Commission at [identitytheft.gov](https://www.ftc.gov) or the police to get an identity theft report
- Report Medicare or Medicaid fraud at [oig.hhs.gov](https://www.oig.hhs.gov)
- Provide your identity theft report to all relevant organizations
  - Your bank and creditors
  - Your health insurer
  - Credit reporting agencies
  - The Internal Revenue Service
  - The Department of Motor Vehicles
  - Utility companies
  - Other \_\_\_\_\_
- Apply for a new Social Security number
- Get a new driver's license

#### If your private data has been compromised, stay alert!

Data thieves can crop up, using your personal information months or even years after it was stolen.