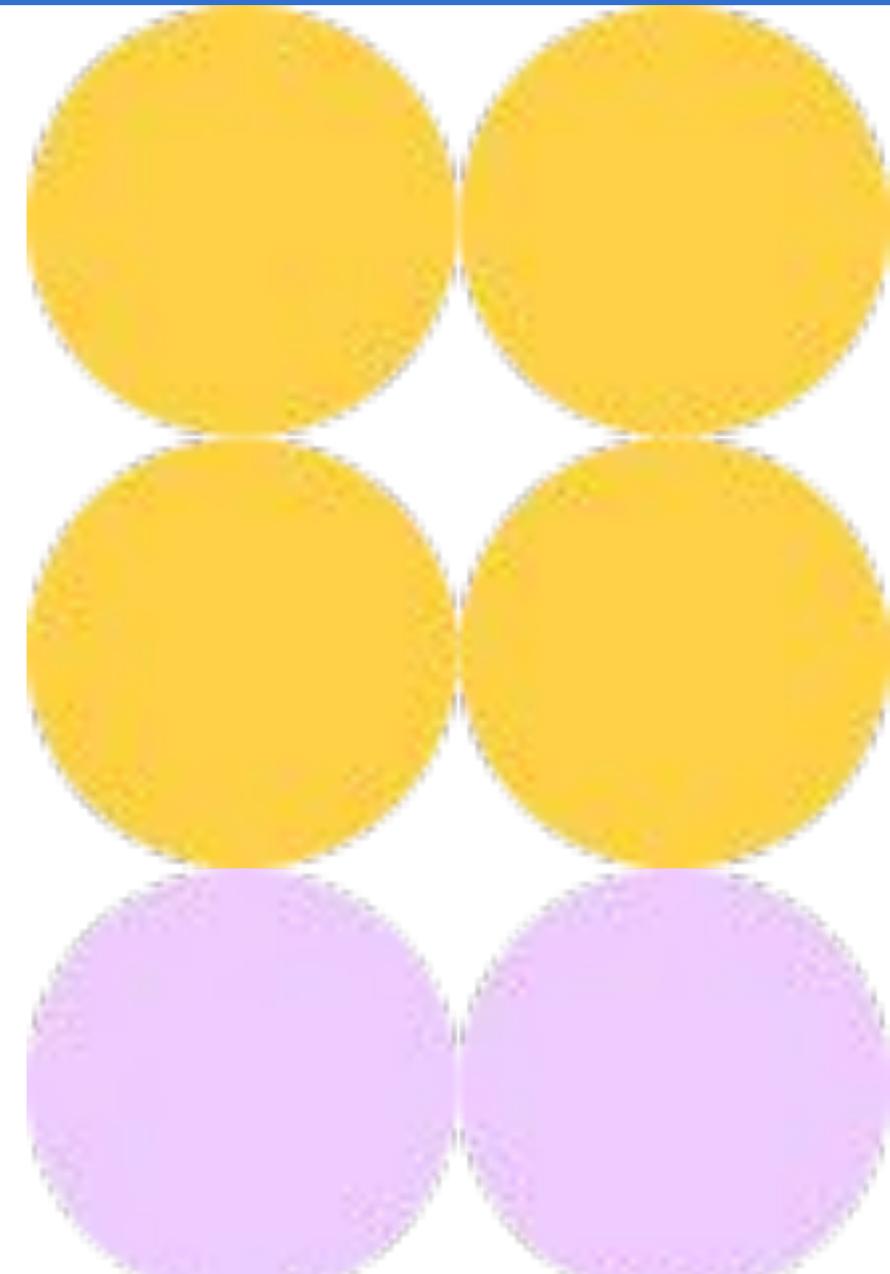


Identity Theft: What to know



Identity Theft: What You Don't Know Can Hurt You

+ **What is identity theft?**

- Someone uses your personal information without permission- They pretend to be you for money, services, or access- It can affect your credit, medical records, and finances

+ **With the Rise of AI**

- Identity theft is at an all-time high- It's not just online-Instead of just being a bad guy, they are lifting people's identities and using them.



Why Do Scammers Steal Identities?

Open Credit Cards in your name

Open loans in your name

File fake Tax Returns

Collect government benefits

Get medical care under your name

Get Medicaid resources under your name

Get rental agreements under your
name for housing

How They Get Your Information



- Phishing emails and texts

Be wary of unsolicited emails or messages requesting sensitive information.



Fake websites or login pages

Confirm the legitimacy of communications and links before responding or providing details.

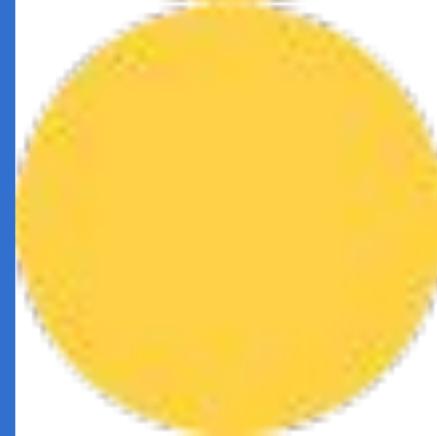
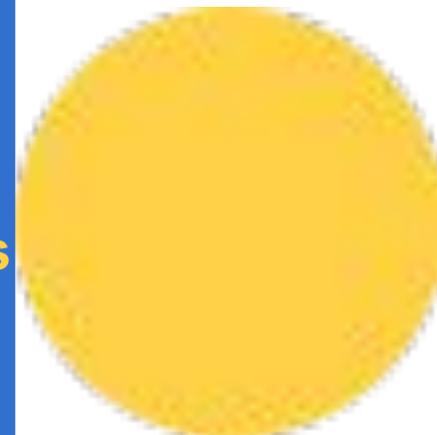


Public Wi-Fi traps & Phone scams or robocalls

Regularly update training for family members and individuals on recognizing and handling phishing threats.



Hacked Corporate Databases



Identity Theft Isn't Just Online

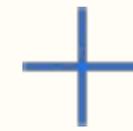


**- Stolen mail or
trash**

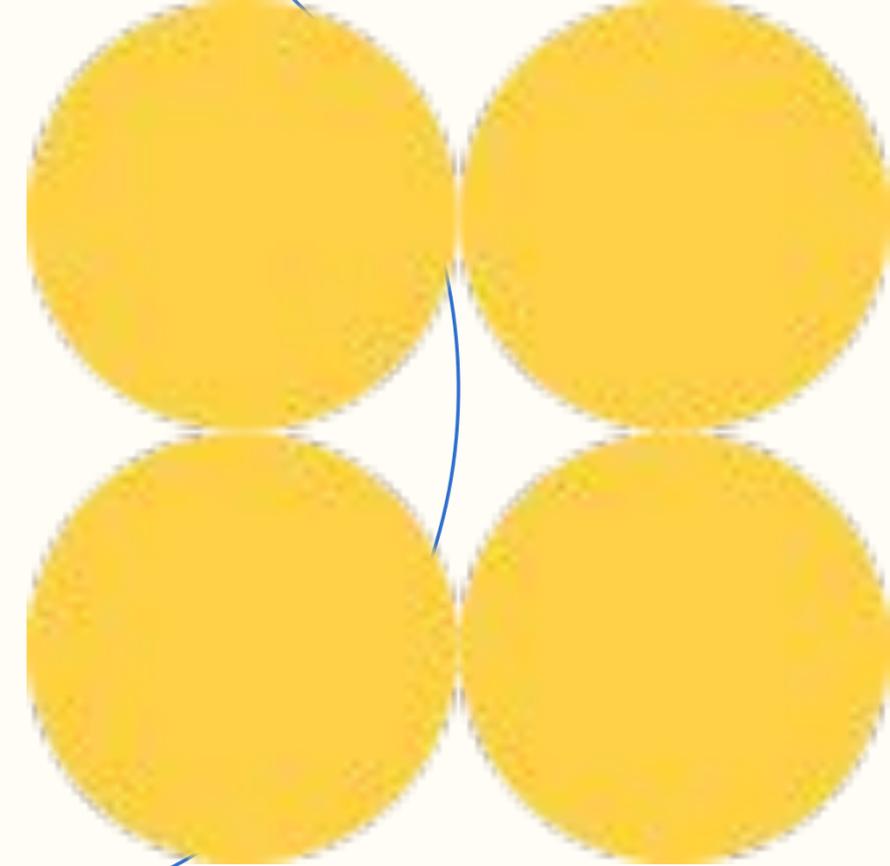
Age old scam, but people
still get sensitive information
via the mailbox.



**Skimming your
credit card**



**Shoulder surfing
at the ATM**





Caregivers or family members

Create a structured plan to address and manage incidents effectively. Especially, have a code word for verification



Misusing checks or bank cards

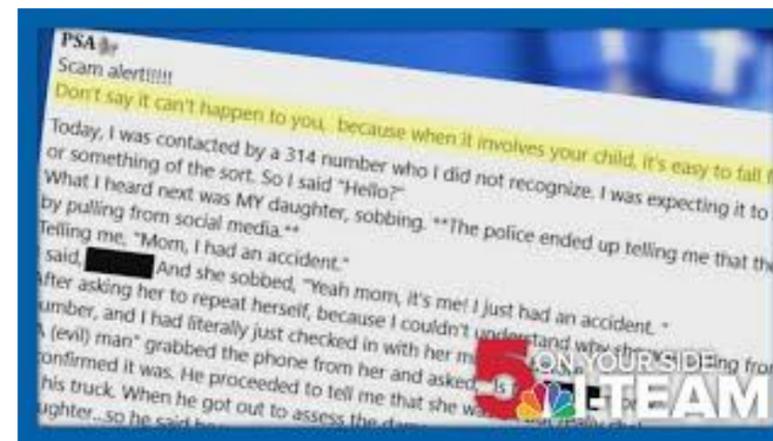
Always check your statements



Stealing Social Security numbers

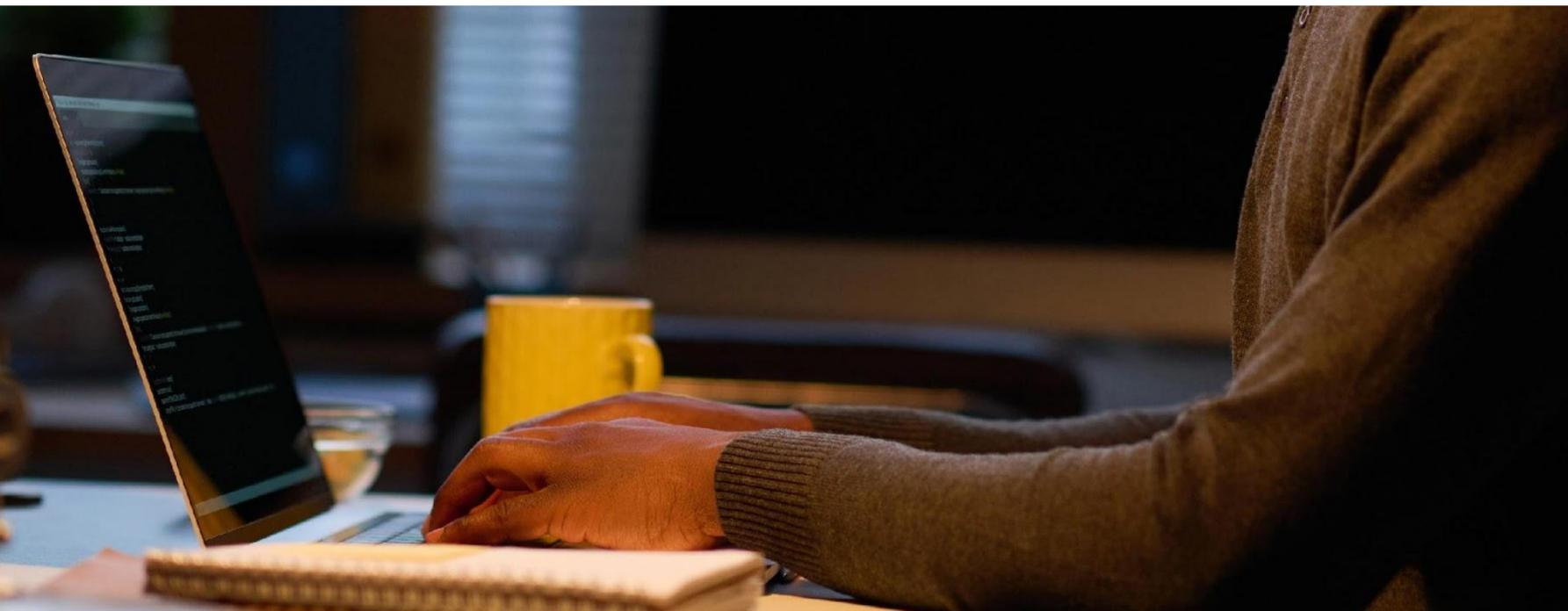
This is more difficult to monitor, but you can report fraud to the IRS in case you believe your Social Sec was compromised.

The Scam Could Come from Someone You Know



The Real Cost of Identity Theft

Impostor Scams ranked highest



- Lost money or savings

In 2024, Americans reported losing over \$12.5 billion to fraud and scams. This represents a 25% increase compared to 2023. Specifically, investment scams were the leading cause of losses, with \$5.7 billion reported stolen, according to the Federal Trade Commission (FTC)

xxx



Denied credit or services

Data from the Federal Trade Commission (FTC) indicates that 449,076 complaints of credit card fraud (including both new account fraud and existing account fraud) were filed in 2024.



Stress, fear, and wasted time- Legal issues or debt collectors



Famous Corporate Cases

- AT&T (2023): 70 million customers' data exposed
- 23andMe (2023): Genetic + ancestry info leaked
- Anthem Blue Cross (2015): 80 million medical records stolen
- Equifax (2017): 147 million Social Security and credit files breached



Famous People Hacked

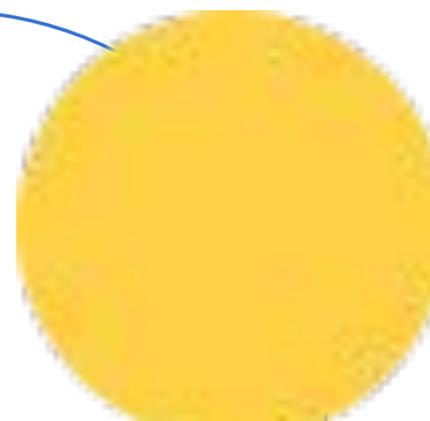
- Arup Conglomerate Zoom Call was the largest call in history: \$25million



- A Near theft of Elvis' Mansion



Famous Hacks That Changed the Game



What Criminals Do with Your Data



Sell it on the dark web



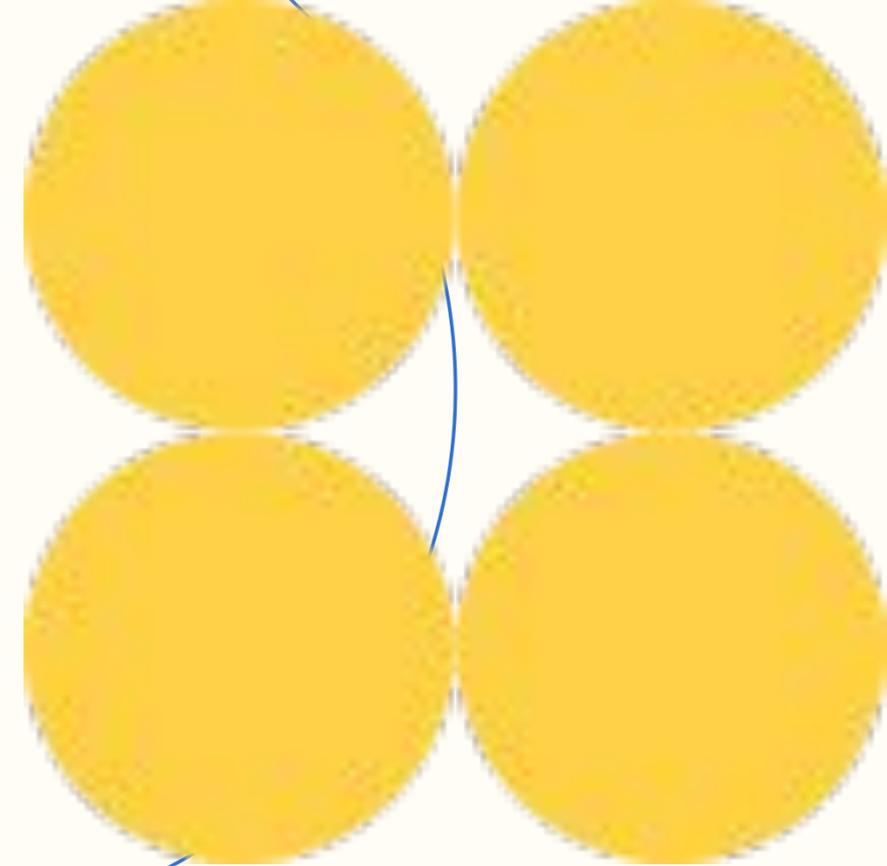
Create fake identities



**Commit tax and
insurance fraud**



**Rent apart
or buy cars
your name**



Identity Theft Isn't Just Online



Avoid Suspicious Links

Do not click on unfamiliar links or download attachments from unknown sources.



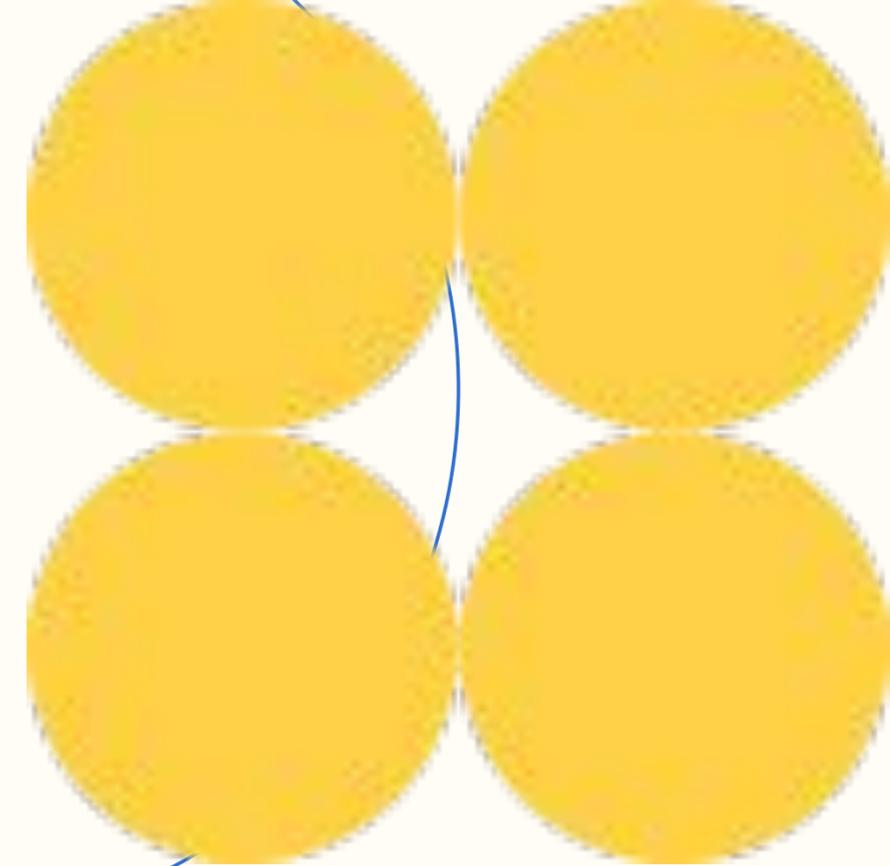
Verify Sources

Ensure the legitimacy of websites and emails before entering personal or financial information.

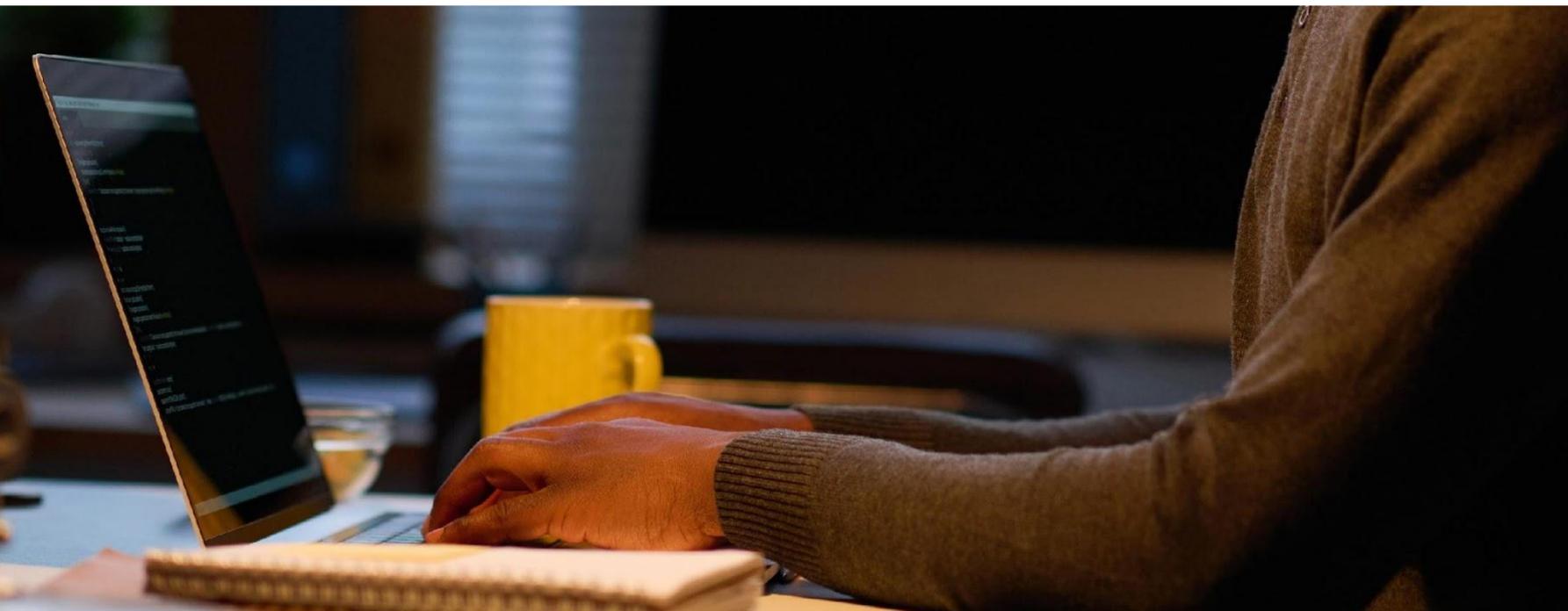


Use Secure Connections

Look for HTTPS in URLs and avoid conducting sensitive transactions over public Wi-Fi networks.



How to Spot Identity Theft Early



Check your statements

Unfamiliar bills or charges



Surprise Debt Collector calls

- Debt collectors calling
- Credit card denied unexpectedly



Missing Emails and Mail

If you still get paper statements, this one may be easier than identifying a missing Email.



Protecting yourself here will help with your Estate Planning Needs and the transfer of information not yet planned for, like logins.

enable 2 factor authentication

You're a Victim, what to do?

Create Strong Passwords

Enable Multi-Factor

Authentication (MFA)

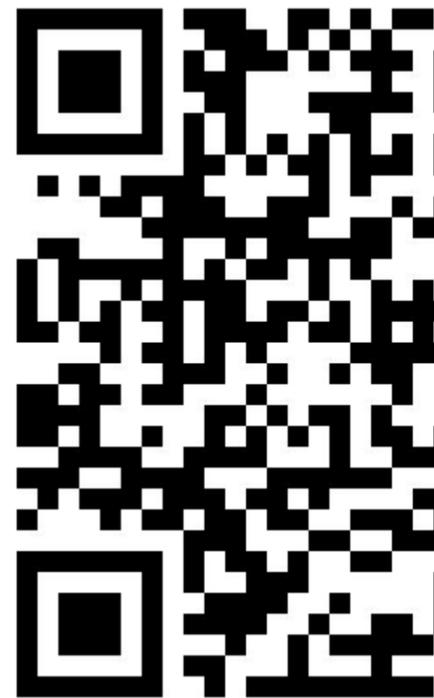
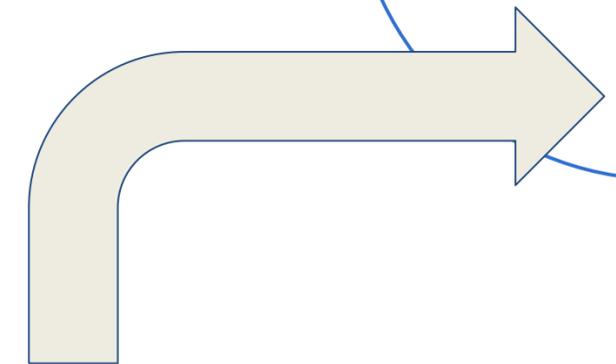
Password Management

+ Call credit bureaus to freeze accounts

+ Report to the FTC:
identitytheft.gov

+ Contact your bank and insurance

+ File a police report if needed



Click to download
printable booklet





Review your bank and credit reports often

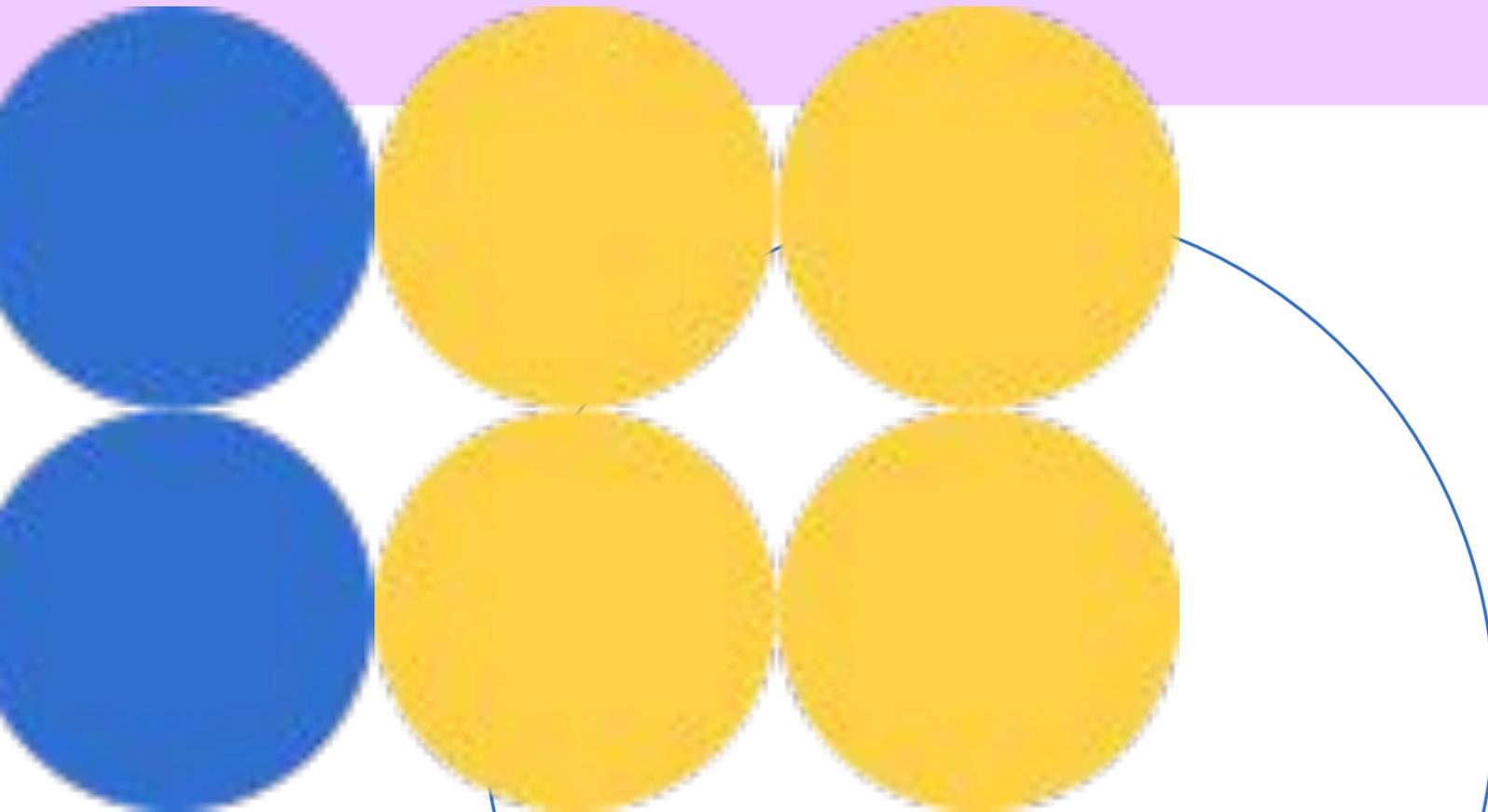


Store documents in a safe place



Talk about scams with friends

TIP: Use alerts for charges over \$20



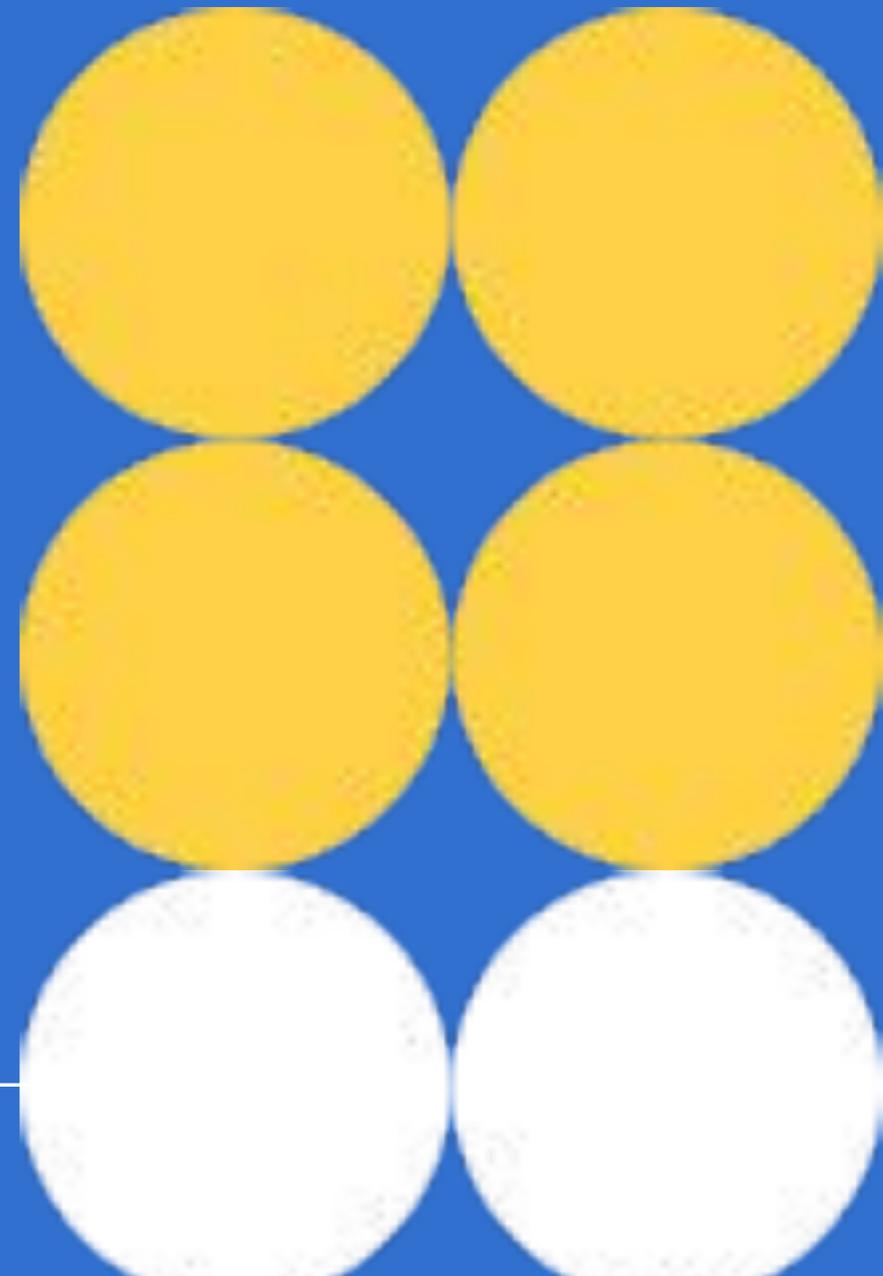
Summary and Key Takeaways



Thank You

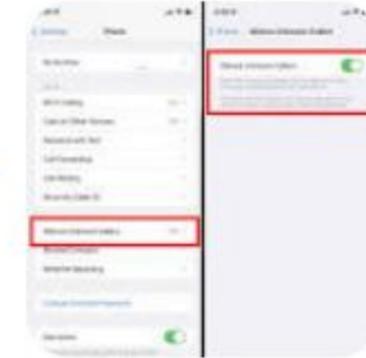


[LINK TO BOOKLET](#)



SILENCING UNKNOWN CALLERS

To silence unknown callers on your iPhone, navigate to Settings > Phone > Silence Unknown Callers and toggle the feature on. This will send calls from numbers not in your contacts, recent outgoing calls, or Siri Suggestions directly to voicemail, while still appearing in your call history. [🔗](#)



Here's a more detailed breakdown:

1. **Open Settings:** Locate and tap the Settings app on your iPhone's home screen.
2. **Go to Phone Settings:** Scroll down and tap on "Phone".
3. **Enable Silence Unknown Callers:** Scroll down to the "Calls" section and tap on "Silence Unknown Callers".
4. **Toggle the switch:** Turn the switch to the ON position to activate the feature. [🔗](#)

What this feature does:

Blocks Unknown Callers:

Silences calls from numbers not in your contacts, recent outgoing calls, or Siri Suggestions. [🔗](#)

Sends to Voicemail:

These calls are sent directly to voicemail. [🔗](#)