Dear New Yorker,

Your identity is at risk. Online, over the phone, and even in person, it's easier than ever for scammers to steal your personal information and use it to commit fraud.

Identity theft affects millions of people every year. Scammers apply for credit cards in your name, receive your medical benefits, and even use your social security number for tax fraud, damaging your credit status and costing time and money to fix.

You can safeguard your personal information and prevent most forms of identity theft with a little diligence, and we're here to help you learn how.

For more details on how to keep your identity safe, or what to do if you believe your identity has been stolen, please go to our website ag.ny.gov.

Sincerely,

Letitia James

Attorney General of New York
Letitia James

Resources

Office of the New York State Attorney General, Consumer Frauds Bureau

Report scams or file a complaint.

(800) 771-7755 / ag.ny.gov

Federal Trade Commission

Report scams or identity theft.

877- 382-4357 / ftc.gov

Credit Report

To check or freeze your credit reports.

877-322-8228 / annualcreditreport.com

Major Credit Reporting Agencies

Experian:
(888) 397-3742 / experian.com

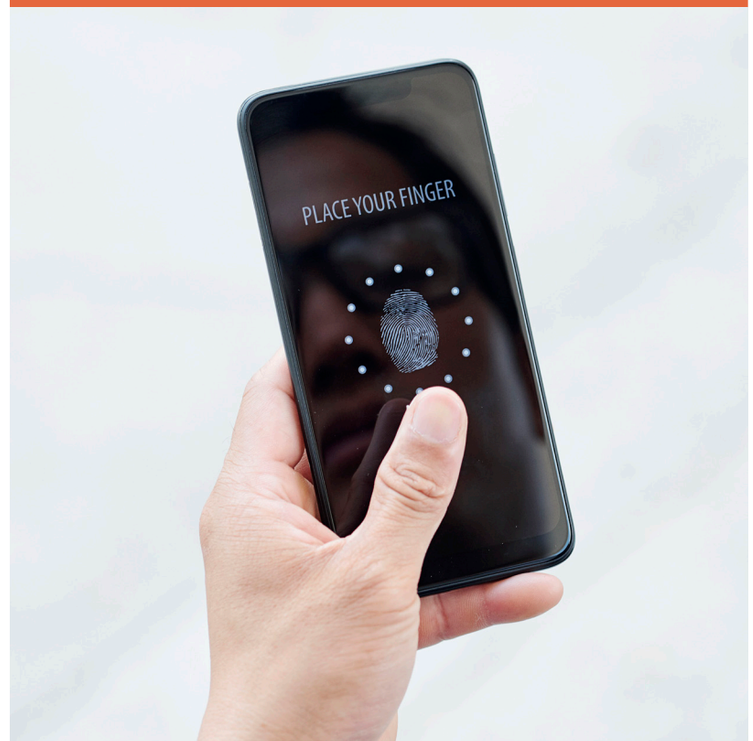
TransUnion:
(800) 888-4213 / transunion.com

Equifax
(800) 685-1111 / equifax.com

Innovis
innovis.com

Protect Your Identity

Tips to Keep Your Identity Safe



Office of the New York State Attorney General
Letitia James

Secure Your Personal Information

While it's generally safe to provide your name or phone number, telling someone your date of birth, social security number, or any account numbers can expose you to identity theft. You should also avoid disclosing any information you use as a "backup" answer for websites when you've forgotten a password.

Never give your personal information to someone who contacts you randomly: unless you've reached out to them, there's a chance you're being "phished."

Phishing is an attempt to get a victim to provide personal information such as their username, password, or credit card number. Scammers can contact you by text, phone, or email, and often pose as a government agency, bank, or well-known company. They'll demand your personal information to resolve some problem or emergency, or say they just need to "confirm your information" before they can give you something.

None of these organizations would actually contact you this way for important information. If you are unsure, call the company — using published numbers — to verify whether it's actually them. Some phishing attempts tell you to go to a website or open an attachment. ***Don't download attachments or click on links from people you don't know.*** These may contain viruses that will infect your computer and steal your personal information.

Suspicious Messages

Even if a message appears to come from a trusted source like a relative or known company, it could still be a phishing attempt: scammers might have taken over the account or created a new account with a similar name. If you get a message that doesn't sound like the sender, contains just a link or attachment without any explanation, or otherwise seems suspicious, double check the "from" field to make sure it's the correct address or call the sender to verify it's really them. This can happen on social media as easily as over email or text, so don't trust a suspicious message just because it comes from a "friend."

Social Security Number

There is very little need for a company to ask for your social security number. If they do, ask why they need it, especially if it isn't a government agency, employer, bank, or financial institution. ***And, again, never give it out to someone who contacts you unsolicited.***

Use a Firewall, Update your Operating System

Browsing the web can expose your computer to viruses. Keep your Operating System and antivirus program updated and keep your firewall running to stay safe.

Create Strong Passwords

If you use the internet, you need strong passwords, and you need several of them. A strong password is one that:

- Is long. It should be at least eight characters, but the more the better.
- Can't be guessed by someone researching you, so no birthdays or names of relatives.
- Is something you can remember. Combining long, uncommon words ("batterystapler") can be useful here.
- Is only used once. If you repeat a password and someone learns it once they can get access to all your accounts.

Password Managers

Modern browsers have "password managers" you can install that remember your passwords for you: just download a manager and everything else gets done automatically. Keep the password for your manager as secure as possible: if a scammer gets access to it they can access all your accounts.

Password-Protect Devices

Treat cell phones and computer accounts just like accounts on a website: give them unique, strong passwords.

Default Passwords

Some devices, like your router or modem, come with a default password. Default passwords are rarely secure, so you should change them immediately.

Regularly Change Passwords

Even if you follow this advice, the longer you use a password the more likely it is that a bad actor will get it: websites can have their security breached. Always change a password if the relevant website is breached, and periodically change passwords anyway to stay safe.

Secure Connections

An insecure website or Wi-Fi network can expose your personal information. Never conduct personal or financial business on a public network, and check to make sure that a website is "secure" before giving it anything sensitive. Secure websites will begin with **"https://"** instead of **"http://"**

Delete Unneeded Data

Destroy any records of personal information once you no longer need them. Shred physical documents like receipts, tax returns, and financial or medical records; delete or deactivate digital accounts and delete digital files. Remember that even deleted files can still be on your hard drive, so you'll need special security software to erase all your personal data if you're getting rid of an old computer.

Monitor Statements

Check credit card and bank statements carefully for any activity you did not authorize.

Carefully check medical bills and health insurance to be sure you actually received the treatment described.

Credit Reports

Everyone is entitled to one free copy of their credit report each year from each of the major credit reporting agencies. If you see accounts or inquiries that you didn't initiate or you don't recognize, it may indicate that someone else is using your identity. You can schedule reports from different agencies at different times of the year to obtain regular coverage at annualcreditreport.com or (877) 322-8228.

Child Identity Theft

Children's identities are the most commonly stolen, sometimes by family members with bad credit ratings. Protect your children's personal information as you would your own. Be sure to ask questions and take action if they receive bill collection calls or credit offers in their names, are denied benefits because someone else is using their number, or receive notices from the IRS about taxes due.