How to Protect Yourself from Identity Theft and Cybercrime

RECOGNIZE AND FIGHT BACK AGAINST IDENTITY THEFT, CYBERCRIME, AND SCAMS

Goals

- Encourage open dialogue around cybercrime and identity theft concerns for consumers in Georgia
- Help participants identify red flags to avoid becoming victims of scams, identity theft, and cybercrime
- Help participants understand proactive steps they can take to minimize their risk of becoming victims of scams, identity theft, and cybercrime
- Encourage participants to utilize available resources if they know or suspect they are a victim of a scam, identity theft, and/or a cybercrime
- Encourage participants to report suspected scams and cases of identity theft to the appropriate state and federal agencies

This module was produced by Georgia Watch under award #2016-XV-GX-K004, awarded by the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this module are those of the contributors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Identity Theft, Cybercrime, and Consumer Scams:

KNOWING THE SIGNS AND RED FLAGS

GEORGIA WATCH™
PROTECTING CONSUMERS SINCE 2002

Total Complaints in Georgia (2017-2018)

Type	Number - 2017	Percent - 2017	Number - 2018	Percent - 2018	% Change
Debt Collection	42,590	37%	28,447	23%	-14%
Identity Theft	12,547	11%	23,874	20%	+9%
Imposter Scams	10,064	9%	12,352	10%	+1%
Credit Bureaus, Information Furnishers and Report Users	8,539	7%	9,891	8%	+2%
Banks and Lenders	6,549	5%	5,945	5%	0%
Television and Mobile Services	4,316	3%	4,721	4%	+1%
Auto-Related	4,004	3%	4,470	4%	+1%
Shop-at-Home and Catalogue Sales	3,457	3%	3,727	3%	0%
Prizes, Sweepstakes, and Lotteries	3,704	3%	3,520	3%	0%
Credit Cards	n/a	n/a	2,045	2%	n/a
Television and Electronic Media	1,870	1%	n/a	n/a	n/a
TOTAL	114,202		119,054		+4%

Source: Federal Trade Commission

GEORGIA WATCH™ PROTECTING CONSUMERS SINCE 2002

Georgia Identity Theft Complaints (2018)

Identity Theft Type	Complaints	Percentage
Other Identity Theft*	9,632	40%
Credit Card Fraud	8,563	36%
Loan or Lease Fraud	4,833	20%
Phone or Utilities Fraud	3,435	14%
Bank Fraud	2,010	8%
Employment or Tax-related Fraud	1,870	8%
Government Documents or Benefits Fraud	712	3%
TOTAL	**23,874**	

**Includes theft related to email, social media, insurance, medical services, online shopping, etc.*

Source: Federal Trade Commission

GEORGIA WATCH
PROTECTING CONSUMERS SINCE 2002

What is Identity Theft?

- **Identity theft occurs when someone steals your personal information to commit fraud.**
  - Stealing your identity could mean using personal identity information (such as your name, Social Security number, bank account information, or credit card number, etc.) without your permission.

GEORGIA WATCH™ PROTECTING CONSUMERS SINCE 2002

Identity Theft 101

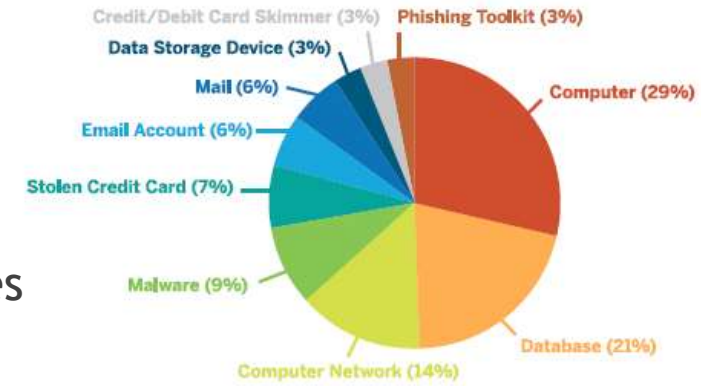
WHAT DO IDENTITY THIEVES WANT?

- **Name***
- **Social Security number***
- **Date of birth***
- **Address***
- **Credit card information***
- Telephone number
- Account numbers
- PINs and passwords
- Mother's maiden name
- Financial records
- Email address

WHERE DO THEY GET IT?

- ***Directly from you***
- Family members
- "Dumpster diving" or your mailbox
- Email account
- Stolen credit card
- Shoulder surfing
- Social networking sites
- Large scale commercial data breaches
- Your computer files and network
- Changing your address

Top resources identity thieves use:



Source: ITAP 2018 Report

Source: ITAP 2018 Report, *UTCID Report #1606*

Identity Theft 101

COMMON TYPES OF SCAMS, FRAUD, AND IDENTITY THEFT

- Credit card fraud
- Fake job and work from home scams
- Fake sweepstakes or lottery scams
- IRS Imposter Scams
- Tax identity theft
- Social security scams
- Online dating scams
- Reshipping and payment processing fraud
- Tech support scams
- Phishing emails and malware
- Medical identity theft
- Medicare scams
- Social media scams

Source: Fraud.org

GEORGIA WATCH™ PROTECTING CONSUMERS SINCE 2002

Identity Theft 101

WHO IS AT GREATEST RISK OF IDENTITY THEFT?

- College-educated
- Adults and Seniors
- Georgians (we are a leading state in identity theft reports)

TYPES OF LOSS VICTIMS OF ID THEFT COMMONLY EXPERIENCE

- Emotional distress
- Financial
- Property
- Reputation
- Intellectual property

Source: ITAP 2018 Report, *UTCID Report #1606*

Most Frequent Ways Criminals Target You for Scams, Fraud, and Identity Theft

SOMETHING GOOD:
YOU'VE WON SOMETHING OR ARE ELIGIBLE FOR A JOB

SOMETHING BAD:
YOU WILL BE PENALIZED OR FINED FOR NOT RESPONDING OR PARTICIPATING

SOMETHING EMOTIONAL:
SOMEONE NEEDS YOUR HELP

GEORGIA WATCH™
PROTECTING CONSUMERS SINCE 2002

Pick 5

You can realistically cover only five of the following topics on the following slide in a 60-minute presentation. Choose the five topics that are the most present in your community.

- IRS Imposter Scams
- Social Security Scams
- Medical Identity Theft and Medicare Scams
- Online Dating Scams
- Social Media Scams
- Reshipping and Payment Processing Fraud
- Tech Support Scams
- Fake Offer Scams

GEORGIA WATCH™ PROTECTING CONSUMERS SINCE 2002

IRS Imposter Scams

The Internal Revenue Service (IRS) is the government agency that collects federal taxes. Scammers will pretend to be IRS officials to get you to send them money.

- A recent scam: consumers receive an email claiming to be from the IRS's Criminal Investigation division. The email says the consumer is the subject of a criminal investigation and instructs them to click on a link or open an attachment to find out more about the complaint against them. Clicking on the link allows scammers to remotely access the consumer's hard drive
- **The IRS will never send out unsolicited emails or ask for a person's personal or financial information. They will never threaten to arrest or deport you.**
- Never send money to anyone who asks. Requests for you to wire money or to send prepaid cards/gift cards are always scams. Always pay the IRS directly, and nobody else.
- Call the IRS at 1-(800)-829-1040. Check your account balance at IRS.gov/balancedue

Source: Federal Trade Commission and GA Department of Law

GEORGIA WATCH™ PROTECTING CONSUMERS SINCE 2002

Social Security Scams

Scammers may also pretend to be from the Social Security Administration and request personal information.

- Like the IRS, no government agency will call or email you unexpectedly to ask for personal information.
- Verify the identity of anyone who asks for personal information over the phone, and say you will respond through the entity's customer service channels. *If anyone pressures you to provide information or money over the phone, it's a scam.*
- Store your Social Security card in a safe location; do not carry it with you. Shred documents listing your SSN and banking information.
- Report any suspicious activity or communications claiming to be from the SSA to the Social Security Fraud Hotline: https://oig.ssa.gov/report

Source: Office of the Inspector General - SSA

Medical Identity Theft and Medicare Scams

Identity thieves may use your name or health insurance information to see a doctor, get prescription drugs, file claims with your insurance providers, or seek other care. They may also claim to be from Medicare and ask for personal information.

- Read your medical and insurance statements regularly and completely to detect any possible identity theft. Check any treatment summaries received to make sure the name of the provider, date of service, and service provided are accurate.
- Other signs of medical identity theft:
  - Bill for medical services you didn't receive
  - Call from debt collector about medical debt you don't owe
  - Medical collection notices on your credit report you don't recognize
  - Denial of insurance because your medical records show a condition you don't have
- Be wary if someone offers you "free" health services but asks for your health plan ID number. Don't share medical or insurance information by phone or email unless you initiated the contact. Keep all copies of medical and insurance records in a safe place.

Source: Federal Trade Commission

Online Dating Scams

Scammers create fake online profiles using photos of other people, then later exploit your romantic interest to get your money.

- They will ask for you to talk to them off the online dating site – usually through text or email. They will claim to be traveling, living/working abroad, in the military, etc., which is why they will never meet up with you in person.
- Despite never having met you, they will profess their love for you. After gaining your trust and romantic interest in return, they will tell you they urgently need money and ask you to send some.
- *If an online date asks you to send money, it's a scam.*
- Be suspicious if an online date is getting very serious but will not meet up in person.
- *Never agree to open a bank account, transfer money, or re-ship goods sent to you for an online date. These are signs of money laundering, which is a criminal offense.*

Source: GA Department of Law

Social Media Scams

Scammers, virus writers, and other types of cybercriminals capitalize on the popularity of sites like Facebook, Twitter, Instagram, and more.

- Beware of clicking on shortened URLs – clicking on a link where you can't see the full site address may bring you to a site that can install malware on your computer.
- "Phishing" refers to a fraudulent attempt to obtain sensitive information (usernames, passwords, etc.) by disguising oneself as a trustworthy entity in an electronic communication. Be cautious when you receive an email from a popular social media site that asks you to click on a link and enter your login information.
- Hidden charges are everywhere on social media. By taking a quiz and having the results texted to you, you may unknowingly sign up for a phone subscription that charges you every month.
- Scammers will sometimes make fake profiles using your friends' photos and personal information. They will then contact you for money for an urgent situation. Always check with your friend via text, email, etc. to see if this profile is legit.

Source: AARP

Reshipping and Payment Processing Fraud

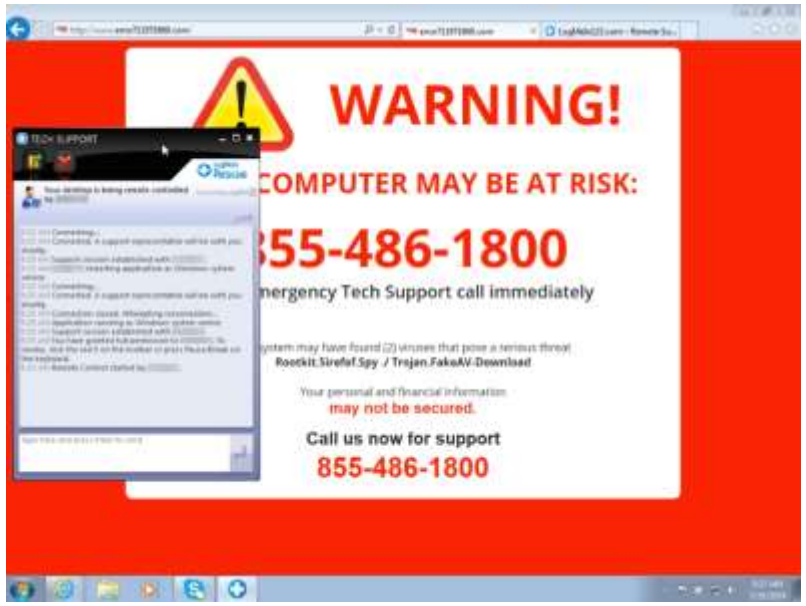
Payment processing scams are operated by scammers who specialize in money laundering. Funds and credit card information are stolen and then used to support luxurious lifestyles for the scammers and further other crimes.

- These scams often start through emails – you may receive one "recruiting" you to work for a business as a payment processor for their customers who live in your area, or an email asking to collect money for a charity and then forward it.
- The emails will ask for personal information like your name, address, and contact information. Sometimes they will even ask for your driver's license number, SSN, or a copy of your passport.
- You will be asked to receive and forward money/merchandise, to write checks on bank accounts other than your own, to receive and re-wire money, and more.
- *Any offer that asks you to serve as a "middle man" by receiving and then forwarding money, goods, etc., is a scam.*

Source: Better Business Bureau

Tech Support Scams

Scammers will pose as an employee of a well-known software company to fraudulently gain access to your computer.



- You receive a phone call or an email from one of these scammers, who will contact you with a sense of urgency – your computer is sending error messages, they've detected a virus, your computer is about to crash, etc., and you're going to lose all of your data!
- The scammer says that a tech support employee needs to access their computer remotely. Once they have gained access, they will tell you your computer is infected with viruses that they can remove for a fee.
- Scammers may also install software onto your computer that allows them to scan your files and potentially steal personal information.

Source: Federal Trade Commission

Fake Offer Scams

Scammers may contact you claiming that you have won something - the lottery, a sweepstakes, etc. - to get your attention.

- The scammers will ask you to pay some type of a fee – for example, processing, shipping, or service fees – or a tax before they receive their prize.
- After sending in your payment for the tax or fees, you will receive no prize in return, because the offer was fake. If you used a credit card or provided any other personal information to the scammer, this information may also be compromised and used for other purposes.
- Sometimes the scammer may send you a check as a way to help you pay for whatever they ask upfront, but when you go to cash the check (after already having paid the scammer), you discover the check is counterfeit.

Source: Federal Trade Commission

Identity Theft, Cybercrime and Consumer Scams:

TOOLS AND TIPS FOR PROTECTING YOURSELF

GEORGIA WATCH™
PROTECTING CONSUMERS SINCE 2002

How to Protect Yourself

- **Keep your private information safe and secure at all times.**
  - Keep important papers in a secure location. Shred documents with personal information before you throw them away. Make copies of everything that's in your wallet, in case it is stolen or lost.
- **Create strong, unique passwords for your various accounts.**
  - Make sure your passwords have a mix of letters, numbers, punctuation, both upper and lowercase letters, and at least eight characters long. Choose obscure security questions. Add 2-step authentication to all online accounts.
- **Monitor your credit cards, bank accounts, and credit reports regularly.**
  - Report any suspicious activity immediately. Have alerts sent to your phone when your credit or debit card is used.
- **Be wary when opening emails.**
  - Check the header, any embedded links, and the domain name. Read the body of the email carefully. Don't open attachments unless you are familiar with the sender.
- **Secure your mobile device and computer.**
  - Use your device's auto-lock feature. Don't broadcast your location. Don't share sensitive information via text. Check for secure Internet connections. Install anti-malware protection.

Source: The University of Texas at Austin & Consumer Ed

Sign up for the Opt-Out Prescreen and Do Not Call Registry

- The Do Not Call Registry and Opt-Out Prescreen are free services that can help you avoid becoming the victim of a scam or identity theft
- Opt-Out Prescreen
  - 1-(888)-567-8688
  - www.optoutprescreen.com
- Do Not Call Registry
  - 1-(888)-382-1222
  - www.donotcall.gov

GEORGIA WATCH
PROTECTING CONSUMERS SINCE 2002

Your Credit Score and Report

- Check your credit report at least twice per year for all three major bureaus
  - Equifax: 1-800-525-6285
  - Experian: 1-888-397-3742
  - TransUnion: 1-800-680-7289
  - AnnualCreditReport.com
- By federal law, you are entitled to one free credit report from each major bureau every year
- Georgians are entitled to an additional two reports each year from each major bureau – meaning you get a total of *9 free reports every year*

AnnualCreditReport.com

The only source for your free credit reports. Authorized by Federal law.

GEORGIA WATCH™ PROTECTING CONSUMERS SINCE 2002

Freeze Your Credit

- Freezing your credit prevents people from using it
- Anyone can freeze and unfreeze their credit **for free** and at their leisure
- *If you think you may be a victim of identity theft, freeze your credit immediately*

Source: Consumer Federation of America

What to Do If Your Identity Was Stolen

- **Contact your bank or card company immediately.** If it involves fraudulent use of your credit card or check card, contact the bank or credit card company immediately to inform them and file a report.
- **Create an initial fraud alert and request your credit reports.**
  - Contact one of the three credit report agencies and ask for a fraud alert to be put on your account, as well as a copy of your credit report. Fraud alerts are free and last for 90 days. Carefully review your credit report upon receiving it – check that all information is correct. Dispute any errors with the three national credit bureaus and any businesses involved in your ID theft.
- **File a police report immediately.**
- **Create an Identity Theft Report.**
  - First, create an Identity Theft Affidavit with the Federal Trade Commission: 1-877-438-4338 or www.ftc.gov/complaint. Then, file a police report. Bring a copy of your FTC Identity Theft Affidavit, a government-issued photo ID, proof of address, and additional proof of theft.

Source: The University of Texas at Austin

What to Do If Your Identity Was Stolen (cont'd)

- **Replace any missing documents.**
  - Contact your state DMV, the U.S. Department of State, the Social Security Administration, and your bank and credit card companies to replace missing driver's licenses, passports, SSNs or cards, and debit/credit cards or checks (respectively).
- Consider a credit freeze and an extended fraud alert (lasts for 7 years instead of 90 days).
- Clear compromised tax records by contacting the IRS.
- *Keep all documents related to the theft and your report.*

- For more help, **contact the Identity Theft Resource Center (ITRC).**
  - Contact the ITRC at 888-400-5530.
  - Visit www.idtheftcenter.org for resources and information about identity theft.

ITRC | IDENTITY THEFT RESOURCE CENTER 888.400.5530

Source: The University of Texas at Austin

GEORGIA WATCH PROTECTING CONSUMERS SINCE 2002

Reporting Suspicious Activity

- If you were targeted by a scam or received any suspicious communications, report it immediately
  - If identity theft may be involved,
    - File a police report
    - Contact the FTC
      - 1-877-FTC-HELP
      - www.ftccomplaintassistant.gov
- As appropriate, you may also consider contacting:
  - Consumer Financial Protection Bureau
  - Georgia Attorney General Consumer Protection Division
  - Banks/credit unions
  - Creditors
  - Involved retailers or companies
  - Better Business Bureau

Tax Fraud Prevention

- **Everyone** should file a tax return
- The IRS will only contact you and request payment via mail
- Keep personal documents locked away and shred old documents
- GA residents can obtain a PIN number to use as an extra layer of protection
- Choose a reliable tax preparer
  - AARP Tax-Aide Program
    - All ages, all incomes
    - 1-888-227-7669
    - https://taxaideqa.aarp.org/hc/en-us
  - IRS Volunteer Income Tax Assistance (VITA)
    - People making $55,000 or less, persons with disabilities, limited English-speaking taxpayers
    - 1-800=906-9887
    - https://irs.treasury.gov/freetaxprep/
  - If you have a higher income, find a CPA with experience
    - Visit Georgia Society of CPAs at www.gscpa.org.

GEORGIA WATCH™ PROTECTING CONSUMERS SINCE 2002

Report Tax Fraud

File complaints with…

IRS: **1-800-829-0433**

Georgia Department of Revenue: **1-877-423-6711**

FTC: **1-877-382-4357**

GEORGIA WATCH™
PROTECTING CONSUMERS SINCE 2002

Local Help and Resources

- **Georgia Legal Services Program**
  - Visit www.glsp.org to find the office nearest you
  - Must be income-qualified
- **Atlanta Legal Aid**
  - Visit atlantalegalaid.org to find the office nearest you
  - Must be income-qualified
  - If you are a senior, contact the Senior Legal Hotline at 404-657-9915 (or toll free 1-888-257-9519)
- **Georgia Watch's Consumer Hotline**
  - 1-866-33-WATCH (92824)