REPORTING CYBERCRIME

From identity theft to phishing scams and cyberbullying, the spectrum of cybercrimes is vast and most of us will, unfortunately, encounter it in our digital life. In honor of Cybersecurity Awareness Month, we wanted to help you understand how to navigate these challenges and protect yourself.

General

You can report various forms of cybercrime to the following agencies:
CISA: cisa.gov/report **FBI:** ic3.gov

Hacked Account

Report your hacked account to the respective platform's support team. Find direct links to popular platforms here: staysafeonline.org/online-safety-privacy-basics/hacked-accounts/

Ransomware

Contact local law enforcement, including:

- **CISA:** cisa.gov/forms/report
- **FBI:** fbi.gov/contact-us/field-offices
- **U.S. Secret Service:** secretservice.gov/contact/field-offices

Identity Theft

Report identity theft to:
FTC: identitytheft.gov

You can also report to:
ID Theft Resource Center:
idtheftcenter.org or call 888.400.5530

Tax-Related Cybercrime

Report tax-related phishing messages or calls to the IRS via email: phishing@irs.gov

More about tax fraud:
irs.gov/individuals/how-do-you-report-suspected-tax-fraud-activity

Credit Card Fraud

Report credit card fraud to your credit card company or use the FTC's fraud, scam and bad business reporting tool: reportfraud.ftc.gov

Elder Fraud

If you or someone you know has been the victim of elder fraud, contact the U.S. Department of Justice's National Elder Fraud Hotline 833.372.8311

Social Security Fraud

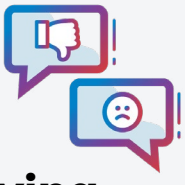
Notify the Social Security Administration if you suspect any fraudulent activities related to your social security number: ssa.gov/fraud or call: 800.269.0271

Business Email Compromise

Report spoofed business-related emails or scams to your organization's IT department and the FBI at: ic3.gov

Online Stalking

If you believe you are being stalked or are a victim of stalkerware, call, chat or text the National Domestic Violence Hotline:
Call: 800.799.7233
Chat: thehotline.org
Text: "Start" to 88788



Cyberbullying

Report cyberbullying to the platform where the bullying occurred or to your child's school.

Report to local law enforcement if there have been threats of violence, stalking or hate crimes at: stopbullying.gov/cyberbullying/how-to-report

Phishing

Report suspicious emails to your email platform and then delete it. Or you can also report to:

- **FTC:** reportfraud.ftc.gov
- **Anti-Phishing Working Group:** reportphishing@apwg.org
- **AARP Fraud Watch Network:** 877.908.3360

Remember: Collect and Keep Evidence

You may be asked to provide evidence when you report certain types of cybercrime. This material can help law enforcement stop and prosecute hackers. All of the following documentation might be considered evidence, but you should keep anything you think could be related to the incident:

- Canceled checks
- Certified or other mail receipts
- Chatroom or newsgroup text
- Credit card receipts
- Envelopes (if you received items via FedEx, UPS or U.S. Mail)
- Log files, if available, with date, time and time zone
- Social media messages
- Money order receipts
- Pamphlets or brochures
- Phone bills
- Copies of emails, preferably electronic copies. If you print the email, include full email header information.
- Copies of web pages, preferably electronic
- Wire receipts

Taking these steps helps **Secure Our World.**

We can all help one another

stay safer online, so share these tips with a family member or friend!

cisa.gov/SecureOurWorld

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY — CISA