

# Help stop cyber crime in its tracks with these resources.

If you suspect a cyber crime, the power to fight it is in your hands.

When it comes to stopping cyber criminals, public reporting is critical. By reporting suspicious activity, tech-savvy citizens like you can help law enforcement agencies, like the FBI, prevent future incidents.

## Help protect yourself and others by knowing how to spot these common cyber threats:

### Fraud

Regularly monitor your accounts and report any unknown activity.

### Identity theft

Be wary of anyone contacting you about unfamiliar debts and watch accounts and credit closely for unauthorized activity. (Subscribe to a credit monitoring service for extra protection.)

### Suspicious text messages

If you don't know the sender, they ask for personal, private information or request confirmation of a financial transaction, report it.

### Phishing

Be on the lookout for unusual emails that may appear to come from companies or people you know and trust.

### Online crime / cyber scams

Internet Crime Complaint Center (IC3):  
**IC3.gov**  
Cybersecurity & Infrastructure Security Agency:  
**cisa.gov/uscert/report**

### Suspicious text messages

Copy the message and forward it to **7726** (a centralized spam reporting service among all wireless carriers)

### Fraud

Federal Trade Commission (FTC):  
**ftc.gov/complaint**

### Identity theft

Federal Trade Commission (FTC):  
**IdentityTheft.gov**  
Social Security Administration:  
**1-800-269-0271**

### Phishing scams

National Cybersecurity Communications and Integration Center (NCCIC):  
**us-cert.gov/report**

## Suspected fraud on your ally accounts

Ally Customer Care:  
**ally.com/contact-us/** or  
**1-833-226-1520**

### Pro tip

Regularly change your login credentials (username and password) and anytime you believe your information has been stolen or compromised.

**ally** do it right.