**[FBI - WHAT WE INVESTIGATE](https://www.fbi.gov/investigate)**

* [Terrorism](https://www.fbi.gov/investigate/terrorism)
* [Counterintelligence](https://www.fbi.gov/investigate/counterintelligence)
* [Cyber Crime](https://www.fbi.gov/investigate/cyber)
* [Public Corruption](https://www.fbi.gov/investigate/public-corruption)
* [Civil Rights](https://www.fbi.gov/investigate/civil-rights)
* [Organized Crime](https://www.fbi.gov/investigate/organized-crime)
* [White-Collar Crime](https://www.fbi.gov/investigate/white-collar-crime)
* [Violent Crime](https://www.fbi.gov/investigate/violent-crime)
* [More](https://www.fbi.gov/investigate/cyber)
* [News](https://www.fbi.gov/investigate/cyber/news)
* [Most Wanted](https://www.fbi.gov/investigate/cyber/most-wanted)
* [Business And Industry Partners](https://www.fbi.gov/investigate/cyber/partnerships)

**The Cyber Threat**

Malicious cyber activity threatens the public’s safety and our national and economic security. The FBI’s [cyber strategy](https://www.fbi.gov/news/stories/wray-announces-fbi-cyber-strategy-at-cisa-summit-091620) is to impose risk and consequences on cyber adversaries. Our goal is to change the behavior of criminals and nation-states who believe they can compromise U.S. networks, steal financial and intellectual property, and put critical infrastructure at risk without facing risk themselves. To do this, we use our unique mix of authorities, capabilities, and partnerships to impose consequences against our cyber adversaries.

The FBI is the lead federal agency for investigating cyber attacks and intrusions. We collect and share intelligence and engage with victims while working to unmask those committing malicious cyber activities, wherever they are.

Learn more about what you can do to [protect yourself](https://www.fbi.gov/investigate/cyber#What-You%20Should%20Know) from cyber criminals, how you can [report cyber crime](https://www.fbi.gov/investigate/cyber#Respond-and%20Report), and the Bureau's efforts in [combating the evolving cyber threat](https://www.fbi.gov/investigate/cyber#Combating-the%20Threat).﻿



[**﻿Private Sector Partners**](https://www.fbi.gov/investigate/cyber/partnerships)

Learn how businesses and organizations can work with the FBI to get ahead of the threat and make an impact on our cyber adversaries.

**A Complex, Global Concern**

Our adversaries look to exploit gaps in our intelligence and information security networks. The FBI is committed to working with our federal counterparts, our foreign partners, and the [private sector](https://www.fbi.gov/investigate/cyber/partnerships) to close those gaps.

These partnerships allow us to defend networks, attribute malicious activity, sanction bad behavior, and take the fight to our adversaries overseas. The FBI fosters this team approach through unique hubs where government, industry, and academia form long-term trusted relationships to combine efforts against cyber threats.

Within government, that hub is the [National Cyber Investigative Joint Task Force (NCIJTF)](https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force). The FBI leads this task force of more than 30 co-located agencies from the Intelligence Community and law enforcement. The NCIJTF is organized around mission centers based on key cyber threat areas and led by senior executives from partner agencies. Through these mission centers, operations and intelligence are integrated for maximum impact against U.S. adversaries.

Only together can we achieve safety, security, and confidence in a digitally connected world.

**How We Work**

Whether through developing innovative investigative techniques, using cutting-edge analytic tools, or forging new partnerships in our communities, the FBI continues to adapt to meet the challenges posed by the evolving cyber threat.

* The FBI has specially trained cyber squads in each of our 56 field offices, working hand-in-hand with interagency task force partners.
* The rapid-response Cyber Action Team can deploy across the country within hours to respond to major incidents.
* With cyber assistant legal attachés in embassies across the globe, the FBI works closely with our international counterparts to seek justice for victims of malicious cyber activity.
* The [Internet Crime Complaint Center (IC3)](https://www.ic3.gov/default.aspx) collects reports of Internet crime from the public. Using such complaints, the IC3’s Recovery Asset Team has assisted in freezing hundreds of thousands of dollars for victims of cyber crime.
* CyWatch is the FBI’s 24/7 operations center and watch floor, providing around-the-clock support to track incidents and communicate with field offices across the country.

**What You Should Know**

**Protect Yourself**

* Taking the right security measures and being alert and aware when connected are key ways to prevent cyber intrusions and online crimes. [**Learn how to protect your computer, network, and personal information**](https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/on-the-internet).

**Understand Common Crimes and Risks Online**

* [**Business email compromise (BEC)**](https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise) scams exploit the fact that so many of us rely on email to conduct business—both personal and professional—and it’s one of the most financially damaging online crimes.
* [**Identity theft**](https://consumer.ftc.gov/features/identity-theft) happens when someone steals your personal information, like your Social Security number, and uses it to commit theft or fraud.
* [**Ransomware**](https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware) is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return.
* [**Spoofing and phishing**](https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing) are schemes aimed at tricking you into providing sensitive information to scammers.
* [**Online predators**](https://www.fbi.gov/how-we-can-help-you/parents-and-caregivers-protecting-your-kids) are a growing threat to young people.
* [**More common crimes and scams**](https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety)

**Respond and Report**

[](https://www.ic3.gov/default.aspx)

**File a Report with the Internet Crime Complaint Center**

If you are the victim of online or internet-enabled crime, file a report with the Internet Crime Complaint Center (IC3) as soon as possible. Crime reports are used for investigative and intelligence purposes. Rapid reporting can also help support the recovery of lost funds. Visit [**ic3.gov**](https://www.ic3.gov/default.aspx) for more information, including tips and information about current crime trends.

**Contact Your Local FBI Field Office**

If you or your organization is the victim of a network intrusion, data breach, or ransomware attack, contact your [**nearest FBI field office**](https://www.fbi.gov/contact-us/field-offices) or report it at [**tips.fbi.gov**](https://tips.fbi.gov/).

**Cyber Safety Tips**

Internet-enabled crimes and cyber intrusions are becoming increasingly sophisticated and preventing them requires each user of a connected device to be aware and on guard.

* Keep systems and software up to date and install a strong, reputable anti-virus program.
* Be careful when connecting to a public Wi-Fi network and do not conduct any sensitive transactions, including purchases, when on a public network.
* Create a strong and unique passphrase for each online account and change those passphrases regularly.
* Set up multi-factor authentication on all accounts that allow it.
* Examine the email address in all correspondence and scrutinize website URLs before responding to a message or visiting a site
* Don’t click on anything in unsolicited emails or text messages.
* Be cautious about the information you share in online profiles and social media accounts. Sharing things like pet names, schools, and family members can give scammers the hints they need to guess your passwords or the answers to your account security questions.
* Don't send payments to unknown people or organizations that are seeking monetary support and urge immediate action.

**Additional Resources and Related Priorities**

[[](https://www.fbi.gov/investigate/counterintelligence/the-iran-threat)](https://www.fbi.gov/investigate/counterintelligence/the-iran-threat)

**[The Iran Threat](https://www.fbi.gov/investigate/counterintelligence/the-iran-threat)**

[Threats from the Iranian regime and its terrorist partners are far reaching. The FBI is committed to identifying and disrupting all Iranian intelligence and military operations that threaten American citizens or our nation's security and critical infrastructure.](https://www.fbi.gov/investigate/counterintelligence/the-iran-threat)

[**﻿Lawful Access**](https://www.fbi.gov/about/mission/lawful-access)

Law enforcement agencies all over the country are bumping up against “warrant-proof” encryption. This means that even with a warrant, law enforcement cannot obtain the electronic evidence needed to investigate and prosecute crimes or security threats.