The Cyber Threat

Malicious cyber activity threatens the public's safety and our national and economic security. The FBI's cyber strategy 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 from cyber criminals, how you can report cyber crime, and the Bureau's efforts in combating the evolving cyber threat.

Private Sector Partners

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 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). 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 55 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) 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.

Asset Forfeiture

Asset forfeiture is a powerful tool used by law enforcement agencies, including the FBI, against criminals and criminal organizations to deprive them of their property used illegally and their ill-gotten gains through seizure of these assets. It is also used to compensate victims of crime. Learn more about the FBI's asset forfeiture program and to see forfeiture in action.

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.

Understand Common Crimes and Risks Online

- Business email compromise (BEC) 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 happens when someone steals your personal information, like your Social Security number, and uses it to commit theft or fraud.
- 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 are schemes aimed at tricking you into providing sensitive information to scammers.
- Online predators are a growing threat to young people.
- More common crimes and scams

Respond and Report

File a Report with the Internet Crime Complaint Center (IC3)

If you are the victim of a cyber-enabled crime or fraud, 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 for more information, including tips and information about current crime trends.

Contact Your Local FBI Field Office

If you need to report an ongoing crime, threat to life, or national security threat, file a report at tips.fbi.gov or by contacting your local field office.

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.
- 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

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.

Cyber News

10.02.2024 Former University of Delaware Student Who Stalked Women and Defrauded the Government Out of $1.5 Million Sentenced to Over Seven Years in Federal Prison

10.01.2024 Indiana Man Pleads Guilty to Conspiracies Involving Cyber Intrusion and $37 Million Cryptocurrency Theft

10.01.2024 Russian National Indicted for Series of Ransomware Attacks

10.01.2024 Sex Trafficker Sentenced to 27 Years in Federal Prison

10.01.2024 Previously Extradited Nigerian National Sent to Prison for Role in Multimillion-Dollar Business Email Compromise Scheme

10.01.2024 FBI Philadelphia Highlights Cyber Safety during National Cybersecurity Awareness Month

09.26.2024 Virginia Man Sentenced to Three Years in Prison for Sextortion Scheme Targeting More Than 100 Young Female Victims Across the Country

09.26.2024 Two Nigerian Nationals Charged in Connection with Business E-Mail Compromise Scheme

09.26.2024 Plymouth Man Indicted for His Role in International Conspiracy to Traffic Counterfeit Computer Network Devices

09.26.2024 United States Seizes More Than $6 Million in Alleged Proceeds of a Crypto-Confidence Scheme

More News

Featured Story