Cyber Crime

The FBI is the lead federal agency for investigating cyber attacks by criminals, overseas adversaries, and terrorists. The threat is incredibly serious—and growing. Cyber intrusions are becoming more commonplace, more dangerous, and more sophisticated. Our nation's critical infrastructure, including both private and public sector networks, are targeted by adversaries. American companies are targeted for trade secrets and other sensitive corporate data, and universities for their cutting-edge research and development. Citizens are targeted by fraudsters and identity thieves, and children are targeted by online predators. Just as the FBI transformed itself to better address the terrorist threat after the 9/11 attacks, it is undertaking a similar transformation to address the pervasive and evolving cyber threat. This means enhancing the Cyber Division's investigative capacity to sharpen its focus on intrusions into government and private computer networks.

Read about the FBI's lead role in threat response for significant cyber activities (https://www.fbi.gov/news/stories/new-us-cyber-security-policy-codifies-agency-role), per Presidential Policy Directive-41.

For more information on the FBI's cyber security efforts, read our "Addressing Threats to the Nation's Cybersecurity" (https://www.fbi.gov/file-repository/addressing-threats-to-the-nations-cybersecurity-1.pdf/view) brochure.

Key Priorities

Computer and Network Intrusions

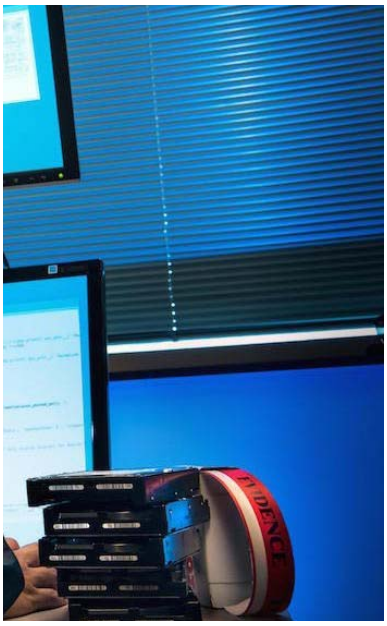
The collective impact is staggering. Billions of dollars are lost every year repairing systems hit by such attacks. Some take down vital systems, disrupting and sometimes disabling the work of hospitals, banks, and 9-1-1 services around the country.

Who is behind such attacks? It runs the gamut—from computer geeks looking for bragging rights…to businesses trying to gain an upper hand in the marketplace by hacking competitor websites, from rings of criminals wanting to steal your personal information and sell it on black markets…to spies and terrorists looking to rob our nation of vital information or launch cyber strikes.

Today, these computer intrusion cases—counterterrorism, counterintelligence, and criminal—are the paramount priorities of our cyber program because of their potential relationship to national security.

Combating the threat. In recent years, we've built a whole new set of technological and investigative capabilities and partnerships—so we're as comfortable chasing outlaws in cyberspace as we are down back alleys and across continents. That includes:

- A Cyber Division at FBI Headquarters "to address cyber crime in a coordinated and cohesive manner";
- Specially trained cyber squads at FBI headquarters and in each of our 56 field offices, staffed with "agents and analysts who protect against investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud";
- New Cyber Action Teams that "travel around the world on a moment's notice to assist in computer intrusion cases" and that "gather vital intelligence that helps us identify the cyber crimes that are most dangerous to our national security and to our economy;"
- Our 93 Computer Crimes Task Forces nationwide that "combine state-of-the-art technology and the resources of our federal, state, and local counterparts";
- A growing partnership with other federal agencies, including the Department of Defense, the Department of Homeland Security, and others—which share similar concerns and resolve in combating cyber crime.



Ransomware

Hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses—these are just some of the entities impacted by ransomware, an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them.

The inability to access the important data these kinds of organizations keep can be catastrophic in terms of the loss of sensitive or proprietary information, the disruption to regular operations, financial losses incurred to restore systems and files, and the potential harm to an organization's reputation. Home computers are just as susceptible to ransomware and the loss of access to personal and often irreplaceable items— including family photos, videos, and other data—can be devastating for individuals as well.

In a ransomware attack, victims—upon seeing an e-mail addressed to them—will open it and may click on an attachment that appears legitimate, like an invoice or an electronic fax, but which actually contains the malicious ransomware code. Or the e-mail might contain a legitimate-looking URL, but when a victim clicks on it, they are directed to a website that infects their computer with malicious software.

One the infection is present, the malware begins encrypting files and folders on local drives, any attached drives, backup drives, and potentially other computers on the same network that the victim computer is attached to. Users and organizations are generally not aware they have been infected until they can no longer access their data or until they begin to see computer messages advising them of the attack and demands for a ransom payment in exchange for a decryption key. These messages include instructions on how to pay the ransom, usually with bitcoins because of the anonymity this virtual currency provides.

Ransomware attacks are not only proliferating, they're becoming more sophisticated. Several years ago, ransomware was normally delivered through spam e-mails, but because e-mail systems got better at filtering out spam, cyber criminals turned to spear phishing e-mails targeting specific individuals. And in

newer instances of ransomware, some cyber criminals aren't using e-mails at all—they can bypass the need for an individual to click on a link by seeding legitimate websites with malicious code, taking advantage of unpatched software on end-user computers.

The FBI doesn't support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee an organization that it will get its data back—there have been cases where organizations never got a decryption key after having paid the ransom. Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals.

So what does the FBI recommend? As ransomware techniques and malware continue to evolve—and because it's difficult to detect a ransomware compromise before it's too late—organizations in particular should focus on two main areas:

- Prevention efforts—both in both in terms of awareness training for employees and robust technical prevention controls; and
- The creation of a solid business continuity plan in the event of a ransomware attack.

Here are some tips for dealing with ransomware (primarily aimed at organizations and their employees, but some are also applicable to individual users):

- Make sure employees are aware of ransomware and of their critical roles in protecting the organization's data.
- Patch operating system, software, and firmware on digital devices (which may be made easier through a centralized patch management system).
- Ensure antivirus and anti-malware solutions are set to automatically update and conduct regular scans.
- Manage the use of privileged accounts—no users should be assigned administrative access unless absolutely needed, and only use administrator accounts when necessary.
- Configure access controls, including file, directory, and network share permissions appropriately. If users only need read specific information, they don't need write-access to those files or directories.
- Disable macro scripts from office files transmitted over e-mail.
- Implement software restriction policies or other controls to prevent programs from executing from common ransomware locations (e.g., temporary folders supporting popular Internet browsers, compression/decompression programs).
- Back up data regularly and verify the integrity of those backups regularly.
- Secure your backups. Make sure they aren't connected to the computers and networks they are backing up.

Related Priorities

Going Dark

Law enforcement at all levels has the legal authority to intercept and access communications and information pursuant to court orders, but often lacks the technical ability to carry out those orders because of a fundamental shift in communications services and technologies. This scenario is often called “Going Dark” and can hinder access to valuable information that may help identity and save victims, reveal evidence to convict perpetrators, or exonerate the innocent.

Read more about the FBI’s response to the Going Dark problem. (https://www.fbi.gov/services/operational-technology/going-dark)

Identity Theft

Identity theft—increasingly being facilitated by the Internet—occurs when someone unlawfully obtains another’s personal information and uses it to commit theft or fraud. The FBI uses both its cyber and criminal resources—along with its intelligence capabilities—to identify and stop crime groups in their early stages and to root out the many types of perpetrators, which span the Bureau's investigative priorities.

More on the FBI's efforts to combat identity theft (https://www.fbi.gov/investigate/white-collar-crime/identity-theft).

Online Predators

The FBI's online predators and child sexual exploitation investigations are managed under our Violent Crimes Against Children Program, Criminal Investigative Division. These investigations involve all areas of the Internet and online services, including social networking venues, websites that post child pornography, Internet news groups, Internet Relay Chat channels, online groups and organizations, peer-to-peer file-sharing programs, bulletin board systems, and other online forums.

Read more about our Violent Crimes Against Children Program (https://www.fbi.gov/investigate/violent-crime/cac).

Initiatives and Partnerships

The Internet Crime Complaint Center

The mission of the Internet Crime Complaint Center (IC3) is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated fraud schemes and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness.

Visit the IC3's website (https://www.ic3.gov) for more information, including IC3 annual reports (https://www.ic3.gov/media/annualreports.aspx).

Cyber Action Team

It can be a company’s worst nightmare—the discovery that hackers have infiltrated their computer networks and made off with trade secrets, customers’ personal information, and other critical data. Today’s hackers have become so sophisticated that they can overcome even the best network security measures. When such intrusions happen—and unfortunately, they occur frequently—the FBI can respond with a range of investigative assets, including the little-known Cyber Action Team (CAT). This rapid deployment group of cyber experts can be on the scene just about anywhere in the world within 48

hours, providing investigative support and helping to answer critical questions that can quickly move a case forward.

Established by the FBI's Cyber Division in 2006 to provide rapid incident response on major computer intrusions and cyber-related emergencies, the team has approximately 50 members located in field offices around the country. They are either special agents or computer scientists, and all possess advanced training in computer languages, forensic investigations, and malware analysis. And since the team's inception, the Bureau has investigated hundreds of cyber crimes, and a number of those cases were deemed of such significance that the rapid response and specialized skills of the Cyber Action Team were required. Some of those cases affected U.S. interests abroad, and the team deployed overseas, working through our legal attaché offices and with our international partners.

Members of the team make an initial assessment, and then call in additional experts as needed. Using cutting-edge tools, the team look's for a hacker's signature. In the cyber world, such signatures are called TTPs—tools, techniques, and procedures. The TTPs usually point to a specific group or person. The hackers may represent a criminal enterprise looking for financial gain or state-sponsored entities seeking a strategic advantage over the U.S.

National Cyber Forensics & Training Alliance

Long before cyber crime was acknowledged to be a significant criminal and national security threat, the FBI supported the establishment of a forward-looking organization to proactively address the issue. Called the National Cyber-Forensics & Training Alliance (NCFTA), this organization—created in 1997 and based in Pittsburgh—has become an international model for bringing together law enforcement, private industry, and academia to build and share resources, strategic information, and threat intelligence to identify and stop emerging cyber threats and mitigate existing ones.

Since its establishment, the NCFTA has evolved to keep up with the ever-changing cyber crime landscape. Today, the organization deals with threats from transnational criminal groups including spam, botnets, stock manipulation schemes, intellectual property theft, pharmaceutical fraud, telecommunications scams, and other financial fraud schemes that result in billions of dollars in losses to companies and consumers.

The FBI Cyber Division's Cyber Initiative and Resource Fusion Unit (CIRFU) works with the NCFTA, which draws its intelligence from the hundreds of private sector NCFTA members, NCFTA intelligence analysts, Carnegie Mellon University's Computer Emergency Response Team (CERT), and the FBI's Internet Crime Complaint Center. This extensive knowledge base has helped CIRFU play a key strategic role in some of the FBI's most significant cyber cases in the past several years.

(https://www.fbi.gov/investigate/violent-crime/cac)

Violent Crimes Against Children/Online Predators (https://www.fbi.gov/investigate/violent-crime/cac)

Even with its post-9/11 national security responsibilities, the FBI continues to play a key role in combating violent crime in big cities and local communities across the United States…

Because of the global reach of cyber crime, no single organization, agency, or country can defend against it. Vital partnerships like the NCFTA are key to protecting cyberspace and ensuring a safer cyber future for our citizens and countries around the world.

For more information visit the National Cyber-Forensics & Training Alliance website. (http://www.ncfta.net/)

(https://www.fbi.gov/resources/law-enforcement/iguardian)

iGuardian (https://www.fbi.gov/resources/law-enforcement/iguardian)

With cyber threats continuing to emerge at the forefront of the FBI's criminal and national security challenges, engaging public-private partners in information exchange alongside law enforcement and intelligence communities…

(https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force)

National Cyber Investigative Joint Task Force (https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force)

As a unique multi-agency cyber center, the National Cyber Investigative Joint Task Force (NCIJTF) has the primary responsibility…

(https://www.fbi.gov/file-repository/cyber-task-forces-fact-sheet.pdf/view)

Cyber Task Forces: Building Alliances to Improve the Nation's Cybersecurity (https://www.fbi.gov/file-repository/cyber-task-forces-fact-sheet.pdf/view)

Each Cyber Task Force synchronizes domestic cyber threat investigations in the local community through information sharing, incident response…

(https://www.fbi.gov/resources/law-enforcement/eguardian)

eGuardian (https://www.fbi.gov/resources/law-enforcement/eguardian)

In 2007, eGuardian was developed to help meet the challenges of collecting and sharing terrorism-related activities amongst law enforcement agencies across various jurisdictions. The eGuardian system is a sensitive but…

Protections

How to Protect Your Computer

Below are some key steps to protecting your computer from intrusion:

Keep Your Firewall Turned On: A firewall helps protect your computer from hackers who might try to gain access to crash it, delete information, or even steal passwords or other sensitive information. Software firewalls are widely recommended for single computers. The software is prepackaged on some operating systems or can be purchased for individual computers. For multiple networked computers, hardware routers typically provide firewall protection.

Install or Update Your Antivirus Software: Antivirus software is designed to prevent malicious software programs from embedding on your computer. If it detects malicious code, like a virus or a worm, it works to disarm or remove it. Viruses can infect computers without users' knowledge. Most types of antivirus software can be set up to update automatically.

Install or Update Your Antispyware Technology: Spyware is just what it sounds like—software that is surreptitiously installed on your computer to let others peer into your activities on the computer. Some spyware collects information about you without your consent or produces unwanted pop-up ads on your web browser. Some operating systems offer free spyware protection, and inexpensive software is readily available for download on the Internet or at your local computer store. Be wary of ads on the Internet offering downloadable antispyware—in some cases these products may be fake and may actually contain spyware or other malicious code. It's like buying groceries—shop where you trust.

Keep Your Operating System Up to Date: Computer operating systems are periodically updated to stay in tune with technology requirements and to fix security holes. Be sure to install the updates to ensure your computer has the latest protection.

Be Careful What You Download: Carelessly downloading e-mail attachments can circumvent even the most vigilant anti-virus software. Never open an e-mail attachment from someone you don't know, and be wary of forwarded attachments from people you do know. They may have unwittingly advanced malicious code.

Turn Off Your Computer: With the growth of high-speed Internet connections, many opt to leave their computers on and ready for action. The downside is that being "always on" renders computers more susceptible. Beyond firewall protection, which is designed to fend off unwanted attacks, turning the computer off effectively severs an attacker's connection—be it spyware or a botnet that employs your computer's resources to reach out to other unwitting users.

Safe Online Surfing

The FBI Safe Online Surfing (FBI-SOS) program is a nationwide initiative designed to educate children in grades 3 to 8 about the dangers they face on the Internet and to help prevent crimes against children.

It promotes cyber citizenship among students by engaging them in a fun, age-appropriate, competitive online program where they learn how to safely and responsibly use the Internet.

The program emphasizes the importance of cyber safety topics such as password security, smart surfing habits, and the safeguarding of personal information.

For more information, visit the Safe Online Surfing website. (http://sos.fbi.gov)

External Links & Resources

- InfraGard: Protecting Infrastructure (https://www.infragard.org/)
- National Cyber Awareness System (https://www.us-cert.gov/mailing-lists-and-feeds)
- National Cyber-Forensics & Training Alliance (http://www.ncfta.net/)
- Law Enforcement Cyber Incident Reporting (https://www.fbi.gov/file-repository/law-enforcement-cyber-incident-reporting.pdf/view)
- DOJ Computer Crime & Intellectual Property Section (https://www.justice.gov/criminal-ccips)

- Secret Service Electronic Crimes Task Forces (http://www.secretservice.gov/investigation/#field)
- Stop.Think.Connect Campaign (https://www.dhs.gov/stopthinkconnect)