On the Internet

Learn tips for protecting your computer, the risk of peer-to-peer systems, the latest e-scams and warnings, Internet fraud schemes, and more.

New E-Scams & Warnings

To report potential e-scams, please go the **Internet Crime Complaint Center and file a report (https://www.ic3.gov/complaint/default.aspx)**. Note: The FBI does not send mass e-mails to private citizens about cyber scams, so if you received an e-mail that claims to be from the FBI Director or other top official, it is most likely a scam.

If you receive unsolicited e-mail offers or spam, you can forward the messages to the Federal Trade Commission at spam@uce.gov (mailto:spam@uce.gov).

For the the latest e-scams and warnings, visit the FBI's Internet Crime Complaint Center (https://www.ic3.gov/media/default.aspx).

Internet Fraud (https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud)

Protect yourself and your family from various forms of Internet fraud.

How to Protect Your Computer

The same advice parents might deliver to young drivers on their first solo journey applies to everyone who wants to navigate safely online. A special agent in our Cyber Division offered the following:

- "Don't drive in bad neighborhoods."
- "If you don't lock your car, it's vulnerable; if you don't secure your computer, it's vulnerable."
- "Reduce your vulnerability, and you reduce the threat."

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.

Risk of Peer-to-Peer Systems

The FBI is educating and warning citizens about certain risks and dangers associated with the use of Peer-to-Peer systems on the Internet. While the FBI supports and encourages the development of new technologies, we also recognize that technology can be misused for illicit and, in some cases, criminal purposes.

Peer-to-Peer networks allow users connected to the Internet to link their computers with other computers around the world. These networks are established for the purpose of sharing files. Typically, users of Peer-to-Peer networks install free software on their computers which allows them (1) to find and download files located on another Peer-to-Peer user's hard drive, and (2) to share with those other users files located on their own computer. Unfortunately sometimes these information-sharing systems have been used to engage in illegal activity. Some of the most common crimes associated with Peer-to-Peer networks are the following:

Copyright Infringement: It is a violation of federal law to distribute copyrighted music, movies, software, games, and other works without authorization. There are important national economic consequences associated with such theft. The FBI has asked industry associations and companies that are particularly concerned with intellectual property theft to report to the FBI—for possible criminal investigation and prosecution—anyone that they have reason to believe is violating federal copyright law.

Child Exploitation and Obscenity: The receipt or distribution of child pornography and unlawful obscenity over the Internet also is a serious federal crime. The FBI cautions parents and guardians that, because there is no age restriction for the use of Peer-to-Peer services, pornography of all types is easily accessible by the many young children whose parents mistakenly believe they are only accessing music or movies. In fact, children may be exposed to pornography—and subsequently lured by sexual predators—even though they were not searching for pornography, as some network users deliberately mislabel the names of files for this purpose.

Computer Hacking: Peer-to-Peer networks also have been abused by hackers. Because these systems potentially expose your computer and files to millions of other users on the network, they also expose your computer to worms and viruses. In fact, some worms have been specifically written to spread by popular Peer-to-Peer networks. Also, if Peer-to-Peer software is not properly configured, you may be unknowingly opening up the contents of your entire hard drive for others to see and download your private information.

The FBI urges you to learn about the risks and dangers of Peer-to-Peer networks, as well as the legal consequences of copyright infringement, illegal pornography, and computer hacking. For more information about the law, visit www.usdoj.gov/criminal (https://www.justice.gov/criminal). The FBI takes seriously its mission to enforce the laws against those who use the Internet to commit crime. To report cyber crime, please contact your local FBI Field Office (https://www.fbi.gov/contact-us/field-offices), or file a complaint through the Internet Crime Complaint Center at www.IC3.gov (https://www.ic3.gov/default.aspx).