Cybercrimes

NATIONAL
CRIME
PREVENTION
COUNCIL

What is Cybercrime?

A crime committed or facilitated via the Internet is a cybercrime. Cybercrime is any criminal activity involving computers and networks. It can range from fraud to unsolicited emails (spam). It can include the distant theft of government or corporate secrets through criminal trespass into remote systems around the globe. Cybercrime incorporates anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-money offenses, such as creating viruses on other computers or posting confidential business information on the Internet.

Most cybercrimes cannot be placed into a single crime category, which makes statistical recording of this activity limited at best. The Internet Crime Complaint Center (IC3) compiles and releases annual reports on the statistics and cybercrime facts. Using statistics and facts, analysts prepare reports on cybercrime trends and growth. Knowing the facts, trends, and growth is critical to crime prevention efforts on protecting personal data in public and private sectors. This also helps in the creation of tools and strategies to combat cyber criminals.

Internet connected activities are as vulnerable to crime and can lead to victimization as effectively as common physical crimes. The types of crimes that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to commit cybercrimes, criminals are now more anonymous and provided with a virtual market of available victims. The responsibility falls on individuals to protect themselves and their families through safe online practices.

> "In 2011, the annual cost of identity theft alone was $37 billion dollars….Identity Theft made up only 9.8 of all cybercrime in 2010." (*Gordon M. Snow, Assistant Director, Cyber Division, Federal Bureau of Investigation, Statement before the Senate Judiciary Committee,*

Subcommittee on Crime and Terrorism, Washington, D.C., April 12, 2011.)

In 2010, the top ten reported cybercrimes to the IC3 were

1. **Non-delivery payment/ merchandise**—14.4 percent of the sellers/purchasers did not receive payment/merchandise.
2. **FBI-related scams**—13.2 percent of criminals pose as the FBI to defraud victims.
3. **Identity Theft**—9.8 percent were unauthorized use of personal identifying information to commit crimes.
4. **Computer crimes**—9.1 percent were crimes that target a computer or were facilitated by a computer.
5. **Miscellaneous fraud**—8.6 percent of scams and fraud included sweepstakes and work-from-home scams.
6. **Advance fee fraud**—7.6 percent were the Nigerian letter scam.
7. **Spam**—6.9 percent of users received unsolicited, mass produced bulk messages.
8. **Auction fraud**—5.9 percent was fraudulent or misleading information in the context of an online auction site.
9. **Credit card fraud**—5.3 percent was fraudulent charging of goods and/or services to a victim's account.
10. **Overpayment fraud**—5.3 percent of victims deposited bad checks for payment and sent the excess funds to sender.

(*Source: 2010 Internet Crime Report)*

Other types of cybercrimes include the following:

- Threats or threatening a person with fear for his or her safety or the safety of others through use of a computer network
- Child pornography, which includes the creation, distribution, or accessing of materials that sexually exploit underage children
- Contraband to include transferring illegal items via the Internet
- Copyright or trademark infringement
- Money laundering, which is transferring proceeds from criminal activity with the intent of hiding the source and destination of the funds
- Cyberbullying, which includes stalking, sending threatening messages, altering images then distributing them with the intent to harass or intimidate
- Cyber terrorism, which is violence, commonly politically motivated, committed against a civilian population through the use of or facilitated by computer technology
- Human trafficking when it is either soliciting or advertising Internet facilitated prostitution
- Online gambling, which is currently illegal in the United States
- Hacking, which is the illegal access of computer or network resources without authorization
- Criminal mischief, which includes damaging or destroying data or information contained on a network with the intent of depriving the owners and users of the information. This can include installing malicious codes such as viruses, Trojans, and worms.

Cybercrime Prevention Strategies

Cyber criminals are no different than traditional criminals in that they want to make their money as quickly and easily as possible. Cybercrime prevention can be achieved fairly quickly and in a cost-effective manner. When armed with a little technical advice and common sense, many cybercrime attacks can be avoided. Similar to target hardening for a residence or a business (e.g., lights, locks, and alarms), the more difficult it is for a cyber criminal to successfully attack a target, the more likely he or she is to leave it alone and move on to an easier target.

The following ten tips are basic ways that cybercrime can be prevented.

- **Keep the computer system up to date**—Cyber criminals will use software flaws to attack computer systems frequently and anonymously. Most Windows-based systems can be configured to download software patches and updates automatically. By doing

this, cyber criminals who exploit flaws in software packages may be thwarted. This will also deter a number of automated and simple attacks criminals use to break into your system.

- **Secure configuration of the system**—It is important that computers are configured to the security level that is appropriate and comfortable for the user. Too much security can have the adverse effect of frustrating the user and possibly preventing them from accessing certain web content. Using the *"help"* feature of the operating system can often address many of the questions in this area.
- **Choose a strong password and protect it**—Usernames, passwords, and personal identification numbers (PIN) are used for almost every online transaction today. A strong password should be at least eight characters in length with a mixture of letters and numbers. Using the same password for various sites or systems increases the risk of discovery and possible exploitation. It is never a good practice to write a password down and leave it near the system it is intended to be used on. Changing a password every 90 days is a good practice to limit the amount of time it can be used to access sensitive information.
- **Keep your firewall turned on**—A firewall helps to protect your computer from hackers who might try to gain access to crash it, delete information, or steal passwords and 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. (www.fbi.gov/scams-safety/, How to Protect Your Computer, www.fbi.gov/scams-safety/computer_protect)
- **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 the users' knowledge. Most types of antivirus software can be set up to update automatically (www.fbi.gov/scams-safety/, How to Protect Your Computer, www.fbi.gov/scams-safety/computer_protect.) Nearly 100 percent of the computers sold in the United States today come with some form of antivirus software. Failure to keep this software current is where a majority of the issues arise. The firewall monitors all data flowing in and out of the computer to the Internet, often blocking attacks from reaching the system. Antivirus software is the next line of defense, monitoring all online activity with the intent to protect the system from viruses, other malicious programs, and can be upgraded to protect against spyware and adware. To be safe on the Internet, the antivirus software should be configured to update itself every time the system connects to the Internet.
- **Protect your personal information**—Using many of the online services today involves sharing basic personal information to include name, home address, phone number, and email address. Using common sense is the best way to protect against and prevent cybercrime. Do not respond to email messages that contain misspellings, poor grammar, odd phrases, or web sites with strange extensions. When in doubt about responding to an email, consider a telephone call to the organization to verify authenticity. Type the address for the website in the browser instead of clicking on a link. Any financial transaction website should have an "s" after the letters "http" (e.g., https://www.mystore.com not http://www.mystore.com). The "s" stands for secure and should appear when you are in an area requesting you to login or provide other sensitive data. Another sign that you have a secure connection is the small lock icon in the bottom of your web browser (usually the right-hand corner.)

- **Read the fine print on website privacy policies**—On many social networking and photo sharing sites, there is wording on the privacy policies that allow the website to keep information and photos posted to the site, sometimes indefinitely, even after the original has been deleted by the user. While this may not discourage one from posting images or messages, awareness that this can be later retrieved and disseminated may be a consideration as to what information or photos are posted. What today may seem to be a harmless prank can have a devastating effect on one's reputation several years later when applying for a job or other opportunity.
- **Review financial statements regularly**—Reviewing credit card and bank statements regularly will often reduce the impact of identity theft and credit fraud by discovering the problem shortly after the data has been stolen or when the first use of the information is attempted. Credit card protection services can often alert a person when there is unusual activity occurring on his or her account, for example, purchases in a geographically distant location or a high volume of purchases. These alerts should not be taken lightly and could be the first indicator that a victim receives that something is wrong.
- **If it seems too good to be true, it is**—No one is going to receive a large sum of money from a dead Nigerian politician, win a huge lottery from being "randomly selected from a database of email addresses," or make big money from "passive residual income a few hours each day working out of your home." Many of these crimes go unreported because the victim is too embarrassed to admit to law enforcement that they were duped.
- **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. (FBI Website -Scams and Safety, How to Protect Your Computer: www.fbi.gov/scams-safety/computer_protect)

The bottom line is for every preventative measure that you take, you limit your chances for becoming a victim of cybercrime.

Resources

- Federal Bureau of Investigation (FBI) for cybercrime information www.fbi.gov/about-us/investigate/cyber/cyber
- Federal Bureau of Investigation (FBI) for tips to avoid Internet fraud www.fbi.gov/scams-safety/fraud/Internet_fraud
- Internet Crime Complaint Center www.ic3.gov
- Department of Justice- Computer Crime and Intellectual Property Section www.cybercrime.gov
- Federal Trade Commission Consumer Information www.ftc.gov/bcp
- National Crime Prevention Council www.ncpc.org

Also, contact your local police department for information on local cybercrime issues and prevention suggestions.

Bibliography

2010 Internet Crime Report, Internet Crime Complaint Center, 2011 www.ic3.gov/media/annualreport/2010_IC3Report.pdf

Cyber Investigations, Federal Bureau of Investigation, 2010 www.fbi.gov/cyberinvest/cyberhome.htm

Gordon M. Snow, Assistant Director, Cyber Division, Federal Bureau of Investigation Statement before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, Washington, DC, April 12, 2011 www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism

This project was supported by Grant No. 2009-GP-BX-K052 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the SMART Office, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice.

Printed in the United States of America
September 2012

2001 Jefferson Davis Highway
Suite 901
Arlington, VA 22202
202-466-6272
www.ncpc.org