



Albany,
Buffalo &
New York
Divisions



A CEO's Guide to Cyber Crime

This two-page guide contains the highlights of the Cyber Security Primer. While we strongly suggest reading the slightly longer full document, this briefing will provide an overview of the cyber crime threat.

CYBER CRIME:

Perhaps the most talked about cyber crime is **financialⁱ** and **automated clearinghouse (ACH) fraudⁱⁱ**, perpetrated through malware like Zeus. Zeus compromised hundreds of businesses in 2010, resulting in millions of dollars in loss. When malware like Zeus is installed on a computer, the software uses a **keystroke loggerⁱⁱⁱ** and submits every keystroke back to the criminal. This malware is particularly dangerous because most antivirus programs have trouble detecting it and it is a "**point-and-click^{iv}**" program. Consequently, criminals no longer need computer expertise to create malware that can defeat antivirus products.

High volumes of **spam^v** can overwhelm email servers and deleting it wastes valuable time. In addition, spam has become a preferred delivery method for **phishing^{vi}** emails and malware. Spam-delivered malware may contain viruses, Trojans, worms, or **botnets^{vii}**, and compromise the computer or the network. Phishers use spam to cast broad nets in identity theft scams. Spear phishers believe in quality over quantity, and do research before crafting an email specific to a small group.

The exploitation of trusted Internet resources has long been a cyber crime trend. "**Drive-by downloads^{viii}**" are one of the more insidious Internet-based malware attacks as they frequently exploit trusted websites and require no action by the user. **Malvertising^x** is one form of drive-by download. Malvertisers embed malicious code into advertisements on legitimate websites, turning popular websites into malware servers. This is both difficult to block and to detect because the user trusts the website and the advertisements rotate so only a few users to the website receive the malware.

The increasing use of social networking websites like Facebook and Twitter has spread to the criminal underground, too. These websites can be used to spread malware or disseminate links to malicious websites. Criminals can use the information gained on these websites to identify targets, craft spear phishing emails and to develop other more devious scams.

Rogue security software and fake antivirus programs are different names for the same type of **scareware^x**. These programs trick the user into downloading them through various ruses meant to frighten the user. Some fake antivirus programs provide realistic looking websites, live help desks, and 1-800 numbers to call. No matter what type of scareware is used, viruses, keystroke loggers, infections or identity theft are possible results.

Other online crimes include a rising use of webcams, blackmail, and smart phone vulnerabilities. Malware enables criminals to remotely turn on and monitor webcams, and numerous demonstrated vulnerabilities in smartphone “apps” are programmed to make expensive phone calls or steal documents. Companies have reported blackmail and extortion attempts resulting from a malware infection. Fake Wi-Fi access points at public locations use the same trust to convince victims to connect to the free access points. These access points may distribute malware or harvest personal information.

In July, **Stuxnet**^{xi} made a large splash in the and **Industrial Control System (ICS)/Supervisory Control and Data Acquisition (SCADA)**^{xii} world, proving that these simple systems are vulnerable to exploits; exploits that can crash trains, shut off the power or have other catastrophic effects.

While the above has focused on cyber criminal activity, cyber espionage is a real threat. The term “advanced persistent threat” is often used in cyber espionage discussions because of the long-term intelligence-gathering focus by foreign actors. Zeus operators have used its keystroke logger to learn login names and passwords, giving them access to company data. Spear phishing attempts frequently target business leaders, negotiators, lawyers and management to install malware for espionage purposes. Malicious actors use social networking sites to monitor company activity, which is easily accomplished by monitoring posts from several employees in a single company.

EMPLOYEE EDUCATION

Educating employees about cyber security can be one of the most difficult security tasks facing any business. Security warnings, even the best ones, inevitably produce glazed eyes and yawns, but security must become a habit because humans are the weakest link in any security network. Cyber security staples such as deleting suspicious emails unread, surfing only trusted sites and locking a computer when away from it, should be reflexive. Remind users to implement basic security steps through emails, a security banner or website pop-up box. Posters, calendars and toolkits that can be used to enhance employees’ awareness are available through the links at the bottom of this document.

October, National Cyber Security Awareness Month, is the perfect time to culminate efforts and join in the national campaigns to promote cyber security awareness. Many of these campaigns include special contests in which employees and their children may participate. There are also many opportunities to tailor or create contests for individual companies including creating a company calendar complete with special company dates, random funny facts and cyber security tips.

Building strong cyber security practices among employees requires significant work, but taken in small increments it can be managed. Add a new goal each week and explain why each goal is important and what can happen when it is not achieved. (A little Internet research can provide many examples of the risks and costs associated with security lapses.)

FURTHER RESOURCES:

Contributors to this paper have valuable cyber security information on their websites. In addition to those resources, the following sites may be useful:

Department of Homeland Security: www.dhs.gov
Stay Safe Online campaign: www.staysafeonline.org
On Guard, Online: www.onguardonline.gov
Looks too Good to be True: www.lookstoogoodtobetrue.com
Internet Crime Complaint Center (IC3): www.ic3.gov

Please send any comments or suggestions to CTICGfeedback@msisac.org.

Points of Contact	
<p>Multi-State Information Sharing and Analysis Center (MS-ISAC) 31 Tech Valley Drive East Greenbush, NY 12061 (518) 266-3485 7x24 Security Operations Center 1-866-787-4722 www.msisac.org</p>	<p>FBI Albany 200 McCarty Ave. Albany, NY 12209 518-465-7551 albany.fbi.gov</p>
<p>NY State Police Computer Crime Unit 1220 Washington Ave. Building 22 Albany, NY 12226 518-457-5712 www.troopers.state.ny.us</p>	<p>New York State Intelligence Center 630 Columbia Street Ext. Latham, NY 12110 (518)786-2100 www.troopers.state.ny.us</p>
<p>NY State Division of Homeland Security and Emergency Services Office of Homeland Security 1220 Washington Ave. Building 7A Suite 710 Albany, NY 12242 518-402-2227 www.security.state.ny.us</p>	<p>NY State Division of Homeland Security and Emergency Services Office of Cyber Security 30 S. Pearl Street P2 Albany, NY 12207 518-474-0865 www.cscic.state.ny.us</p>
<p>FBI Buffalo One FBI Plaza Buffalo, NY 14202 (716) 856-7800 buffalo.fbi.gov</p>	<p>FBI New York 26 Federal Plaza, 23rd Floor New York, NY 10278 (212) 384-1000 newyork.fbi.gov</p>
<p>United States Secret Service, Albany 39 N Pearl St # 2 Albany, NY 12207 (518) 436-9600 www.secretservice.gov</p>	

Endnotes

- ⁱ **Financial fraud** includes mortgage and Ponzi schemes, credit card theft and tax fraud. Identity theft frequently results in financial fraud.
- ⁱⁱ **ACH fraud** is fraudulent electronic funds transfer between banks through batch processing (a data handling method in which a large number of requests are processed in the same transaction).
- ⁱⁱⁱ **Keystroke loggers (keyloggers)** are software programs that record every key pressed. Newer versions include the ability to take a picture of the screen (screenshot) after each input, defeating voice recognition software and onscreen keyboards.
- ^{iv} **Point-and-click** software are programs that allow a user to easily accomplish tasks without having advanced computer knowledge. These easy to use programs generally offer self-explanatory menus or toolbars to aid the user.
- ^v **Spam** is unsolicited electronic mail, generally email, although it is possible to receive spam faxes. Spammers may send email to known email addresses or may try common emails ("jsmith@abc.com"). Spam costs so little that an extremely small number of positive responses will pay for millions of spam emails. Spam is frequently used to deliver malware and phishing attempts.
- ^{vi} **Phishing** is a variation of the word "fishing," because it is the electronic version of throwing a hook in the water and hoping for a bite. Other forms of phishing include "**spear phishing**" (a targeted phishing attack), "**SM Shishing**" (phishing through SMS and text messages) and "**vishing**" (phishing through phone calls). Spear phishing victims may receive an email that contains information about their company, "CEO Killed in Crash," or that appears to come from a friend "Vacation pictures").
- ^{vii} **Botnets** are large networks of computers around the world. Each bot consists of **zombie** computers, to which the **command and control** (C&C or C2) server can send commands. Most often, the owner of a zombie does not know they are part of the botnet. Botnets are used to send spam, spread malware and handle tasks that require lots of computing power or multiple geographic locations. Many botnet owners rent out their botnets to other criminals.
- ^{viii} **Drive-by downloads** are unintended downloads of programs from the Internet. These programs can be malicious in nature. A **drive-by installation** is the actual installation of a program without the user's knowledge.
- ^{ix} **Malvertising** is malicious advertising. Criminals may purchase an advertisement on a website like the New York Times home page and hide malicious code in the ad. All the users who visit that legitimate website and view that advertisement will be infected.
- ^x **Scareware** is any type of software that tricks the user into anxiety or panic. Rogue security software, like fake antivirus programs, offer the user a solution that will fix the problem that caused the panic. These solutions may require a credit card for purchase (identity theft/financial fraud) or trick the user into downloading malware.
- ^{xi} **Stuxnet** was the first widely publicized worm to attack PCS/SCADA systems. The worm reprogrammed infected computers and exfiltrated data possibly for espionage purposes.
- ^{xii} **ICS** and **SCADA** systems are very simple control computers for monitoring machinery, turning switches on and off, performing load balancing and other simple functions that can be easily automated.