Federal
Communications
Commission

Kinetik Networks, LLC
Paoli, IN
November 18, 2022

Table of Contents

Thank you for using the FCC's Small Biz Cyber Planner, a tool for small businesses to create customized cyber security planning guides. Businesses large and small need to do more to protect against growing cyber threats. As larger companies take steps to secure their systems, less secure small businesses are easier targets for cyber criminals.

This planning guide is designed to meet the specific needs of your company, using the FCC's customizable Small Biz Cyber Planner tool. The tool is designed for businesses that lack the resources to hire dedicated staff to protect their business, information and customers from cyber threats. Even a business with one computer or one credit card terminal can benefit from this important tool. We generally recommend that businesses using more sophisticated networks with dozens of computers consult a cyber security expert in addition to using the cyber planner. The FCC provides no warranties with respect to the guidance provided by this tool and is not responsible for any harm that might occur as a result of or in spite of its use.

The guidance was developed by the FCC with input from public and private sector partners, including the Department of Homeland Security, the National Cyber Security Alliance and The Chamber of Commerce.

Scams and Fraud

New telecommunication technologies may offer countless opportunities for small businesses, but they also offer cyber criminals many new ways to victimize your business, scam your customers and hurt your reputation. Businesses of all sizes should be aware of the most common scams perpetrated online.

To protect your business against online scams, be cautious when visiting web links or opening attachments from unknown senders, make sure to keep all software updated, and monitor credit cards for unauthorized activity.

Cyber Plan Action Items:

1. Train employees to recognize social engineering

Social engineering, also known as "pretexting," is used by many criminals, both online and off, to trick unsuspecting people into giving away their personal information and/or installing malicious software onto their computers, devices or networks. Social engineering is successful because the bad guys are doing their best to make their work look and sound legitimate, sometimes even helpful, which makes it easier to deceive users.

Most offline social engineering occurs over the telephone, but it frequently occurs online, as well. Information gathered from social networks or posted on websites can be enough to create a convincing ruse to trick your employees. For example, LinkedIn profiles, Facebook posts and Twitter messages can allow a criminal to assemble detailed dossiers on employees. Teaching people the risks involved in sharing personal or business details on the Internet can help you partner with your staff to prevent both personal and organizational losses.

Many criminals use social engineering tactics to get individuals to voluntarily install malicious computer software such as fake antivirus, thinking they are doing something that will help make them more secure. Fake antivirus is designed to steal information by mimicking legitimate security software. Users who are tricked into loading malicious programs on their computers may be providing remote control capabilities to an attacker, unwittingly installing software that can steal financial information or simply try to sell them fake security software. The malware can also make system modifications which make it difficult to terminate the program. The presence of pop-ups displaying unusual security warnings and asking for credit card or personal information is the most obvious method of identifying a fake antivirus infection.

2. Protect against online fraud

Online fraud takes on many guises that can impact everyone, including small businesses and their employees. It is helpful to maintain consistent and predictable online messaging when communicating with your customers to prevent others from impersonating your company.

Be sure to never request personal information or account details through email, social networking or other online messages. Let your customers know you will never request this kind of information through such channels and instruct them to contact you directly should they have any concerns.

3. Protect against phishing

Phishing is the technique used by online criminals to trick people into thinking they are dealing with a trusted website or other entity. Small businesses face this threat from two directions -- phishers may be impersonating them to take advantage of unsuspecting customers, and phishers may be trying to steal their employees' online credentials. Attackers often take advantage of current events and certain types of the year, such as:

- Natural disasters (Hurricane Katrina, Indonesian tsunami)

- Epidemics and health scares (H1N1)
- Economic concerns
- Major political elections
- Holidays

Businesses should ensure that their online communications never ask their customers to submit sensitive information via email, personal visits, or phone. Make a clear statement in your communications reinforcing that you will never ask for personal information via email so that if someone targets your customers, they may realize the request is a scam.

Employee awareness is your best defense against your users being tricked into handing over their usernames and passwords to cyber criminals. Explain to everyone that they should never respond to incoming messages requesting private information. If a stranger claims to be from a legitimate organization, verify his or her identity with his or her stated company before sharing any personal or classified information. Also, to avoid being led to a fake site, employees should know to never click on a link sent by email from an untrustworthy source. Employees needing to access a website link sent from a questionable source should open an Internet browser window and manually type in the site's web address to make sure the emailed link is not maliciously redirecting to a dangerous site.

This advice is especially critical for protecting online banking accounts belonging to your organization. Criminals are targeting small business banking accounts more than any other sector. If you believe you have revealed sensitive information about your organization, make sure to:

- Report it to appropriate people within your organization
- Contact your financial institution and close any accounts that may have been compromised (if you believe financial data is at risk)
- Change any passwords you may have revealed, and if you used the same password for multiple resources, make sure to change it for each account

4. Don't fall for fake antivirus offers

Fake antivirus, "scareware" and other rogue online security scams have been behind some of the most successful online frauds in recent times. Make sure your organization has a policy in place explaining what the procedure is if an employee's computer becomes infected by a virus.

Train your employees to recognize a legitimate warning message (using a test file from eicar.org, for example) and to properly notify your IT team if something bad or questionable has happened.
If possible, configure your computers to not allow regular users to have administrative access. This will minimize the risk of them installing malicious software and condition users that adding unauthorized software to work computers is against policy.

5. Protect against malware

Businesses can experience a compromise through the introduction of malicious software, or malware. Malware can make its way onto machines from the Internet, downloads, attachments, email, social media, and other platforms. One specific malware to be aware of is key logging, which is malware that tracks a user's keyboard strokes.

Many businesses are falling victim to key-logging malware being installed on computer systems in their environment. Once installed, the malware can record keystrokes made on a computer, allowing bad guys to see passwords, credit card numbers and other confidential data. Keeping security software up to date and patching your computers regularly will make it more difficult for this type of malware to infiltrate your network.

6. Develop a layered approach to guard against malicious software

Despite progress in creating more awareness of security threats on the Internet, malware authors are not giving up. The malware research firm SophosLabs reports seeing more than 100,000 unique malicious software samples every single day.

Effective protection against viruses, Trojans and other malicious software requires a layered approach to your defenses. Antivirus software is a must, but should not be a company's only line of defense. Instead, deploy a combination of many techniques to keep your environment safe.

Also, be careful with the use of thumb drives and other removable media. These media could have malicious software pre-installed that can infect your computer, so make sure you trust the source of the removable media devices before you use them.

Combining the use of web filtering, antivirus signature protection, proactive malware protection, firewalls, strong security policies and employee training significantly lowers the risk of infection. Keeping protection software up to date along with your operating system and applications increases the safety of your systems.

7. Be aware of spyware and adware

Spyware and adware, when installed will send pop-up ads, redirect to certain websites, and monitor websites that you visit. Extreme versions can track what keys are typed. Spyware can cause your computer to become slow and also leaves you susceptible to privacy theft. If you are subject to endless pop-up windows or are regularly redirected to websites other than what you type in your browser, your computer is likely infected with spyware.

To remove spyware run an immediate full scan of your computer with anti-virus software and if necessary run a legitimate product specifically designed to remove spyware. To avoid being infected with spyware, limit cookies on your browser preferences, never click on links within pop-up windows, and be wary of free downloadable software from unreputable sources.

8. Verify the identity of telephone information seekers

Most offline social engineering occurs over the telephone. Information gathered through social networks and information posted on websites can be enough to create a convincing ruse to trick your employees.
Ensure that you train employees to never disclose customer information, usernames, passwords or other sensitive details to incoming callers. When someone requests information, always contact the person back using a known phone number or email account to verify the identity and validity of the individual and their request.

Helpful links

- Use the Department of Homeland Security's Stop.Think.Connect.™ Campaign's resources created especially for businesses to train their employees: www.dhs.gov/stopthinkconnect
- Find the most updated patches for your computer and software applications: http://www.softwarepatch.com/
- Free computer security scan tools for your PC or network: http://www.staysafeonline.org/tools-resources/free-security-check-ups
- Stay on top of the latest scams, frauds and security threats as they happen: http://nakedsecurity.sophos.com/
- Additional tops to prevent against phishing: http://www.fraud.org/scams/internet-fraud/phishing
- Learn how to resist phishing techniques with this interactive game: http://cups.cs.cmu.edu/antiphishing_phil/

Network Security

Securing your company's network consists of: (1) identifying all devices and connections on the network; (2) setting boundaries between your company's systems and others; and (3) enforcing controls to ensure that unauthorized access, misuse, or denial-of-service events can be thwarted or rapidly contained and recovered from if they do occur.

Cyber Plan Action Items:

1. Secure internal network and cloud services

Your company's network should be separated from the public Internet by strong user authentication mechanisms and policy enforcement systems such as firewalls and web filtering proxies. Additional monitoring and security solutions, such as anti-virus software and intrusion detection systems, should also be employed to identify and stop malicious code or unauthorized access attempts.

Internal network

After identifying the boundary points on your company's network, each boundary should be evaluated to determine what types of security controls are necessary and how they can be best deployed. Border routers should be configured to only route traffic to and from your company's public IP addresses, firewalls should be deployed to restrict traffic only to and from the minimum set of necessary services, and intrusion prevention systems should be configured to monitor for suspicious activity crossing your network perimeter. In order to prevent bottlenecks, all security systems you deploy to your company's network perimeter should be capable of handling the bandwidth that your carrier provides.

Cloud based services

Carefully consult your terms of service with all cloud service providers to ensure that your company's information and activities are protected with the same degree of security you would intend to provide on your own. Request security and auditing from your cloud service providers as applicable to your company's needs and concerns. Review and understand service level agreements, or SLAs, for system restoration and reconstitution time.

You should also inquire about additional services a cloud service can provide. These services may include backup-and-restore services and encryption services, which may be very attractive to small businesses.

2. Develop strong password policies

Generally speaking, two-factor authentication methods, which require two types of evidence that you are who you claim to be, are safer than using just static passwords for authentication. One common example is a personal security token that displays changing passcodes to be used in conjunction with an established password. However, two-factor systems may not always be possible or practical for your company.

Password policies should encourage your employees to employ the strongest passwords possible without creating the need or temptation to reuse passwords or write them down. That means passwords that are random, complex and long (at least 10 characters), that are changed regularly, and that are closely guarded by those who know them.

3. Secure and encrypt your company's Wi-Fi

Wireless access control

Your company may choose to operate a Wireless Local Area Network (WLAN) for the use of customers, guests and visitors. If so, it is important that such a WLAN be kept separate from the main company network so that traffic from the public network cannot traverse the company's internal systems at any point.

Internal, non-public WLAN access should be restricted to specific devices and specific users to the greatest extent possible while meeting your company's business needs. Where the internal WLAN has less stringent access controls than your company's wired network, dual connections -- where a device is able to connect to both the wireless and wired networks simultaneously -- should be prohibited by technical controls on each such capable device (e.g., BIOS-level LAN/WLAN switch settings). All users should be given unique credentials with preset expiration dates to use when accessing the internal WLAN.

Wireless encryption

Due to demonstrable security flaws known to exist in older forms of wireless encryption, your company's internal WLAN should only employ Wi-Fi Protected Access 2 (WPA2) encryption.

4. Encrypt sensitive company data

Encryption should be employed to protect any data that your company considers sensitive, in addition to meeting applicable regulatory requirements on information safeguarding. Different encryption schemes are appropriate under different circumstances. However, applications that comply with the OpenPGP standard, such as PGP and GnuPG, provide a wide range of options for securing data on disk as well as in transit. If you choose to offer secure transactions via your company's website, consult with your service provider about available options for an SSL certificate for your site.

5. Regularly update all applications

All systems and software, including networking equipment, should be updated in a timely fashion as patches and firmware upgrades become available. Use automatic updating services whenever possible, especially for security systems such as anti-malware applications, web filtering tools and intrusion prevention systems.

6. Set safe web browsing rules

Your company's internal network should only be able to access those services and resources on the Internet that are essential to the business and the needs of your employees. Use the safe browsing features included with modern web browsing software and a web proxy to ensure that malicious or unauthorized sites cannot be accessed from your internal network.

7. If remote access is enabled, make sure it is secure

If your company needs to provide remote access to your company's internal network over the Internet, one popular and secure option is to employ a secure Virtual Private Network (VPN) system accompanied by strong two-factor authentication, using either hardware or software tokens.

8. Create Safe-Use Flash Drive **Policy**

Ensure employees never put any unknown flash drive or USBs into their computer. As the U.S. Chamber's *Internet Security Essentials for Business 2.0* states, small businesses should set a policy so that employees know they should

never open a file from a flash drive they are not familiar with and should hold down the Shift key when inserting the flash drive to block malware.

Helpful links

- Microsoft Password Strength Checker: https://www.microsoft.com/security/pc-security/password-checker.aspx
- Philip Zimmerman, Where to Get PGP: http://philzimmermann.com/EN/findpgp/
- US-CERT Security Publications: http://www.us-cert.gov/reading_room/
- NIST Special Publication 800-153, Draft Guidelines for Securing Wireless Local Area Networks (WLANs): http://csrc.nist.gov/publications/nistpubs/800-153/sp800-153.pdf
- U.S. Chamber of Commerce: Internet Security Essentials for Business 2.0 https://www.uschamber.com/sites/default/files/issues/technology/files/ISEB-2.0-CyberSecurityGuide.pdf

Email

Email has become a critical part of our everyday business, from internal management to direct customer support. The benefits associated with email as a primary business tool far outweigh the negatives. However, businesses must be mindful that a successful email platform starts with basic principles of email security to ensure the privacy and protection of customer and business information.

Cyber Plan Action Items:

1. Set up a spam email filter

It has been well documented that spam, phishing attempts and otherwise unsolicited and unwelcome email often accounts for more than 60 percent of all email that an individual or business receives. Email is the primary method for spreading viruses and malware and it is one of the easiest to defend against. Consider using email-filtering services that your email service, hosting provider or other cloud providers offer. A local email filter application is also an important component of a solid antivirus strategy. Ensure that automatic updates are enabled on your email application, email filter and anti-virus programs. Ensure that filters are reviewed regularly so that important email and/or domains are not blocked in error.

2. Train your employees in responsible email usage

The last line of defense for all of your cyber risk efforts lies with the employees who use tools such as email and their responsible and appropriate use and management of the information under their control. Technology alone cannot make a business secure. Employees must be trained to identify risks associated with email use, how and when to use email appropriate to their work, and when to seek assistance of professionals. Employee awareness training is available in many forms, including printed media, videos and online training.

Consider requiring security awareness training for all new employees and refresher courses every year. Simple efforts such as monthly newsletters, urgent bulletins when new viruses are detected, and even posters in common areas to remind your employees of key security and privacy to-do's create a work environment that is educated in protecting your business.

3. Protect sensitive information sent via email

With its proliferation as a primary tool to communicate internally and externally, business email often includes sensitive information. Whether it is company information that could harm your business or regulated data such as personal health information (PHI) or personally identifiable information (PII), it is important to ensure that such information is only sent and accessed by those who are entitled to see it.

Since email in its native form is not designed to be secure, incidents of misaddressing or other common accidental forwarding can lead to data leakage. Businesses that handle this type of information should consider whether such information should be sent via email, or at least consider using email encryption. Encryption is the process of converting data into unreadable format to prevent disclosure to unauthorized personnel. Only individuals or organizations with access to the encryption key can read the information. Other cloud services offer "Secure Web Enabled Drop Boxes" that enable secure data transfer for sensitive information, which is often a better approach to transmitting between companies or customers.

4. Set a sensible email retention policy

Another important consideration is the management of email that resides on company messaging systems and your users' computers. From the cost of storage and backup to legal and regulatory requirements, companies should

document how they will handle email retention and implement basic controls to help them attain those standards. Many industries have specific rules that dictate how long emails can or should be retained, but the basic rule of thumb is only as long as it supports your business efforts. Many companies implement a 60-90 day retention standard if not compelled by law to another retention period.

To ensure compliance, companies should consider mandatory archiving at a chosen retention cycle end date and automatic permanent email removal after another set point, such as180-360 days in archives. In addition, organizations should discourage the use of personal folders on employee computers (most often configurable from the e-mail system level), as this will make it more difficult to manage company standards.

5. Develop an email usage policy

Policies are important for setting expectations with your employees or users, and for developing standards to ensure adherence to your published polices.

Your policies should be easy to read, understand, define and enforce. Key areas to address include what the company email system should and should not be used for, and what data are allowed to be transmitted. Other policy areas should address retention, privacy and acceptable use.

Depending on your business and jurisdiction, you may have a need for email monitoring. The rights of the business and the user should be documented in the policy as well. The policy should be part of your general end user-awareness training and reviewed for updates on a yearly basis.

For a sample email usage policy, see: http://www.sans.org/security-resources/policies/Email_Policy.pdf

Employees

Businesses must establish formal recruitment and employment processes to control and preserve the quality of their employees. Many employers have learned the hard way that hiring someone with a criminal record, falsified credentials or undesirable background can create a legal and financial nightmare.

Without exercising due diligence in hiring, employers run the risk of making unwise hiring choices that can lead to workplace violence, theft, embezzlement, lawsuits for negligent hiring and numerous other workplace problems.

Cyber Plan Action Items:

1. Develop a hiring process that properly vets candidates

The hiring process should be a collaborative effort among different groups of your organization, including recruitment, human resources, security, legal and management teams. It is important to have a solid application, resume, interview and reference-checking process to identify potential gaps and issues that may appear in a background check.

An online employment screening resource called the "Online Safe Hiring Certification Course" can help you set the groundwork for a safe recruitment process. The course will teach your teams what to look for in the different stages of the hiring process, how to interview and how to set up a safe hiring program to avoid hiring an employee that may be problematic. The course is available here: http://www.esrcheck.com/ESRonlineSafeHiringCourse.php.

2. Perform background checks and credentialing

Background checks are essential and must be consistent. Using a background screening company is highly recommended. The standard background screening should include the following checks:

- Employment verification
- Education verification
- Criminal records
- Drug testing
- The U.S. Treasury Office of Foreign Affairs and Control
- Sex offender registries
- Social Security traces and validation

Depending on the type of your business, other screening criteria may consist of credit check, civil checks and federal criminal checks. Conducting post-hire checks for all employees every two to three years, depending on your industry, is also recommended.

If you do conduct background checks, you as an employer have obligations under the Fair Credit Reporting Act. For more information about employer obligations under the FCRA, visit http://business.ftc.gov/documents/bus08-using-consumer-reports-what-employers-need-know.

3. Take care in dealing with third parties

Employers should properly vet partner companies through which your organization hires third-party consultants. To ensure consistent screening criteria are enforced for third-party consultants, you need to explicitly set the credentialing requirements in your service agreement. State in the agreement that the company's credentialing requirements must be followed.

4. Set appropriate access controls for employees

Both client data and internal company data are considered confidential and need particular care when viewed, stored, used, transmitted or disposed. It is important to analyze the role of each employee and set data access control based upon the role. If a role does not require the employee to ever use sensitive data, the employee's access to the data should be strictly prohibited. However, if the role requires the employee to work with sensitive data, the level of access must be analyzed thoroughly and be assigned in a controlled and tiered manner following "least-privilege" principles, which allow the employee to only access data that is necessary to perform his or her job.

If the organization does not have a system in place to control data access, the following precautions are strongly recommended. Every employee should:

- Never access or view client data without a valid business reason. Access should be on a need-to-know basis.
- Never provide confidential data to anyone – client representatives, business partners or even other employees – unless you are sure of the identity and authority of that person.
- Never use client data for development, testing, training presentations or any purpose other than providing production service, client-specific testing or production diagnostics. Only properly sanitized data that cannot be traced to a client, client employee, customer or your organization's employee should be used for such purposes.
- Always use secure transmission methods such as secure email, secure file transfer (from application to application) and encrypted electronic media (e.g., CDs, USB drives or tapes).
- Always keep confidential data (hard copy and electronic) only as long as it is needed.
- Follow a "clean desk" policy, keeping workspaces uncluttered and securing sensitive documents so that confidential information does not get into the wrong hands.
- Always use only approved document disposal services or shred all hardcopy documents containing confidential information when finished using them. Similarly, use only approved methods that fully remove all data when disposing of, sending out for repair or preparing to reuse electronic media.

5. Provide security training for employees

Security awareness training teaches employees to understand system vulnerabilities and threats to business operations that are present when using a computer on a business network.

A strong IT security program must include training IT users on security policy, procedures and techniques, as well as the various management, operational and technical controls necessary and available to keep IT resources secure. In addition, IT infrastructure managers must have the skills necessary to carry out their assigned duties effectively. Failure to give attention to the area of security training puts an enterprise at great risk because security of business resources is as much a human issue as it is a technology issue.

Technology users are the largest audience in any organization and are the single most important group of people who can help to reduce unintentional errors and IT vulnerabilities. Users may include employees, contractors, foreign or domestic guest researchers, other personnel, visitors, guests and other collaborators or associates requiring access. Users must:

- Understand and comply with security policies and procedures.
- Be appropriately trained in the rules of behavior for the systems and applications to which they have access.
- Work with management to meet training needs.
- Keep software and applications updated with security patches.
- Be aware of actions they can take to better protect company information. These actions include: proper password usage, data backup, proper antivirus protection, reporting any suspected incidents or violations of

security policy, and following rules established to avoid social engineering attacks and deter the spread of spam or viruses and worms.

A clear categorization of what is considered sensitive data versus non-sensitive data is also needed. Typically, the following data are considered sensitive information that should be handled with precaution:

- Government issued identification numbers (e.g., Social Security numbers, driver's license numbers)
- Financial account information (bank account numbers, credit card numbers)
- Medical records
- Health insurance information
- Salary information
- Passwords

The training should cover security policies for all means of access and transmission methods, including secure databases, email, file transfer, encrypted electronic media and hard copies.

Employers should constantly emphasize the critical nature of data security. Regularly scheduled refresher training courses should be established in order to instill the data security culture of your organization. Additionally, distribute data privacy and security related news articles in your training, and send organization-wide communication on notable data privacy related news as reminders to your employees.

6. Implement Employee Departure Checklist

Create a security checkout checklist for employees that are no longer with your company, regardless of their reason for leaving (voluntary or involuntary). It's recommended by the U.S. Chamber of Commerce and others that all small businesses ensure terminated employee accounts are erased on all network devices and drives immediately. This is especially true for any devices that may have been taken offsite such as laptops and smartphones.

Helpful links

- Stop.Think.Connect. Internal Employee Rollout Materials
  http://www.dhs.gov/stopthinkconnect
- Internet Safety at Work PowerPoint Presentation
  http://go.microsoft.com/?linkid=9745638
- Tip Cards: Top Tips for Internet Safety at Work
- http://go.microsoft.com/?linkid=9745642
- Video: "Stay Sharp on Internet Safety at Work"
  http://go.microsoft.com/?linkid=9745640
- U.S. Chamber of Commerce: Internet Security Essentials for Business 2.0
  https://www.uschamber.com/sites/default/files/issues/technology/files/ISEB-2.0-CyberSecurityGuide.pdf

Cyber Security Glossary

Adware

Any software application that displays advertising banners while the program is running. Adware often includes code that tracks a user's personal information and passes it on to third parties without the user's authorization or knowledge. And if you gather enough of it, adware slows down your computer significantly. Over time, performance can be so degraded that you may have trouble working productively. See also **Spyware** and **Malware**.

Anti-Virus Software

Software designed to detect and potentially eliminate viruses before they have had a chance to wreak havoc within the system. Anti-virus software can also repair or quarantine files that have already been infected by virus activity. See also **Virus** and **Electronic Infections**.

Application

Software that performs automated functions for a user, such as word processing, spreadsheets, graphics, presentations and databases—as opposed to operating system (OS) software.

Attachment

A file that has been added to an email—often an image or document. It could be something useful to you or something harmful to your computer. See also **Virus**.

Authentication

Confirming the correctness of the claimed identity of an individual user, machine, software component or any other entity.

Authorization

The approval, permission or empowerment for someone or something to do something.

Backdoor

Hidden software or hardware mechanism used to circumvent security controls.

Backup

File copies that are saved as protection against loss, damage or unavailability of the primary data. Saving methods include high-capacity tape, separate disk sub-systems or on the Internet. Off-site backup storage is ideal, sufficiently far away to reduce the risk of environmental damage such as flood, which might destroy both the primary and the backup if kept nearby.

Badware

See **Malware**, **Adware** and **Spyware**.

Bandwidth

The capacity of a communication channel to pass data such as text, images, video or sound through the channel in a given amount of time. Usually expressed in bits per second.

Blacklisting Software

A form of filtering that blocks only websites specified as harmful. Parents and employers sometimes use such software to prevent children and employees from visiting certain websites. You can add and remove sites from the "not permitted" list. This method of filtering allows for more full use of the Internet, but is less efficient at preventing access to any harmful material that is not on the list. See also **Whitelisting Software**.

Blended Threat

A computer network attack that seeks to maximize the severity of damage and speed of contagion by combining methods—for example, using characteristics of both viruses and worms. See also **Electronic Infection**.

Blog

Short for "Web log," a blog is usually defined as an online diary or journal. It is usually updated frequently and offered in a dated log format with the most recent entry at the top of the page. It often contains links to other websites along with commentary about those sites or specific subjects, such as politics, news, pop culture or computers.

Broadband

General term used to refer to high-speed network connections such as cable modem and Digital Subscriber Line (DSL). These types of "always on" Internet connections are actually more susceptible to some security threats than computers that access the Web via dial-up service.

Browser

A client software program that can retrieve and display information from servers on the World Wide Web. Often known as a "Web browser" or "Internet browser," Examples include Microsoft's Internet Explorer, Google's Chrome, Apple's Safari, and Mozilla's Firefox.

Brute Force Attack

An exhaustive password-cracking procedure that tries all possibilities, one by one. See also **Dictionary Attack** and **Hybrid Attack**.

Clear Desk Policy

A policy that directs all personnel to clear their desks at the end of each working day, and file everything appropriately. Desks should be cleared of all documents and papers, including the contents of the "in" and "out" trays —not simply for cleanliness, but also to ensure that sensitive papers and documents are not exposed to unauthorized persons outside of working hours.

Clear Screen Policy

A policy that directs all computer users to ensure that the contents of the screen are protected from prying eyes and opportunistic breaches of confidentially. Typically, the easiest means of compliance is to use a screen saver that engages either on request or after a specified short period of time. See also **Shoulder Surfing**.

Cookie

A small file that is downloaded by some websites to store a packet of information on your browser. Companies and organizations use cookies to remember your login or registration identification, site preferences, pages viewed and online "shopping-cart" so that the next time you visit a site, your stored information can automatically be pulled up for you. A cookie is obviously convenient but also presents potential security issues. You can configure your browser to alert you whenever a cookie is being sent. You can refuse to accept all cookies or erase all cookies saved on your browser.

Credit Card

A card indicating the holder has been granted a line of credit. Often sought after by criminals looking for an easy way to purchase things without having to pay for them. For this reason and others, a credit card preferable to a debit card for online shopping since it provides a buffer between buyer and seller, affording more protections to the buyer in case there is a problem with the order or the card number is compromised. See also **Debit Card**.

Cyberbullying

Sending or posting harmful, cruel, rude or threatening messages, or slanderous information, text or images using the Internet or other digital communication devices.

Debit Card

A card linked directly to the holder's bank account, withdrawing money from the account. Not as safe as credit cards for online shopping since if problems arise, the buyer's money has already been spent and is harder to get back. See also **Credit Card**.

Denial of Service Attack

The prevention of authorized access to a system resource or the delaying of system operations and functions. Often this involves a cyber criminal generating a large volume of data requests. See also **Flooding**.

Dictionary Attack

A password-cracking attack that tries all of the phrases or words in a dictionary. See also **Brute Force Attack** and **Hybrid Attack**.

Digital Certificate

The electronic equivalent of an ID card that establishes your credentials when doing business or other transactions on the Web. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

Domain Hijacking

An attack in which an attacker takes over a domain by first blocking access to the domain's DNS server and then putting his own server up in its place.

Domain Name System (DNS)

The DNS is the way that Internet domain names are located. A website's domain name is easier to remember than its IP (Internet Protocol) address.

Dumpster Diving

Recovering files, letters, memos, photographs, IDs, passwords, checks, account statements, credit card offers and more from garbage cans and recycling bins. This information can then be used to commit identity theft.

Electronic Infections

Often called "viruses," these malicious programs and codes harm your computer and compromise your privacy. In addition to the traditional viruses, other common types include worms and Trojan horses. They sometimes work in tandem to do maximum damage. See also Blended Threat.

Encryption

A data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that it appears as a meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key.

End User License Agreement (EULA)

A contract between you and your software's vendor or developer. Many times, the EULA is presented as a dialog box that appears the first time you open the software and forces you to check "I accept" before you can proceed. Before accepting, though, read through it and make sure you understand and are comfortable with the terms of the agreement. If the software's EULA is hard to understand or you can't find it, beware!

Evil Twins

A fake wireless Internet hot spot that looks like a legitimate service. When victims connect to the wireless network, a hacker can launch a spying attack on their transactions on the Internet, or just ask for credit card information in the standard pay-for-access deal. See also **Man-in-the-Middle Attacks**.

File-Sharing Programs

Sometimes called peer-to-peer (P2P) programs, these allow many different users to access the same file at the same time. These programs are often used to illegally upload and download music and other software. Examples include Napster, Grokster, Kazaa, iMesh, Ares and Limewire.

Firewall

A hardware or software link in a network that inspects all data packets coming and going from a computer, permitting only those that are authorized to reach the other side.

Flooding

An attack that attempts to cause a failure in the security of a computer by providing more input, such as a large volume of data requests, than it can properly process. See also **Denial of Service Attack**.

Grooming

Using the Internet to manipulate and gain trust of a minor as a first step towards the future sexual abuse, production or exposure of that minor. Sometimes involves developing the child's sexual awareness and may take days, weeks, months or in some cases years to manipulate the minor.

Hacker

An individual who attempts to break into a computer without authorization.

HTTPS

When used in the first part of a URL (e.g., http://), this term specifies the use of hypertext transfer protocol (HTTP) enhanced by a security mechanism such as Secure Socket Layer (SSL). Always look for the HTTP*S* on the checkout or order form page when shopping online or when logging into a site and providing your username and password.

Hybrid Attack

Builds on other password-cracking attacks by adding numerals and symbols to dictionary words. See also **Dictionary Attack** and **Brute Force Attack**.

Instant Messaging (IM)

A service that allows people to send and get messages almost instantly. To send messages using instant messaging you need to download an instant messaging program and know the instant messaging address of another person who uses the same IM program. See also **Spim**.

IP (Internet Protocol) Address

A computer's inter-network address, written as a series of four 8-bit numbers separated by periods, such as 123.45.678.990. Every website has an IP Address, although finding a website is considerably easier to do when using its domain name instead. See also **Domain Name System (DNS)**.

Internet Service Provider (ISP)
A company that provides internet access to customers.

Keystroke Logger
A specific type of electronic infection that records victims' keystrokes and sends them to an attacker. This can be done with either hardware or software. See also **Trojan Horse**.

Malware
A generic term for a number of different types of malicious code. See also **Adware** and **Spyware**.

Man-In-the-Middle Attack
Posing as an online bank or merchant, a cyber criminal allows a victim to sign in over a Secure Sockets Layer (SSL) connection. The attacker then logs onto the real server using the client's information and steals credit card numbers.

Monitoring Software
Software products that allow parents to monitor or track the websites or email messages that a child visits or reads. See also **Blacklisting Software** and **Whitelisting Software**.

Network
Two or more computer systems that are grouped together to share information, software and hardware.

Operating System (OS)
Programs that manage all the basic functions and programs on a computer, such as allocating system resources, providing access and security controls, maintaining file systems and managing communications between end users and hardware devices. Examples include Microsoft's Windows, Apple's Macintosh and Red Hat's Linux.

Password
A secret sequence of characters that is used as a means of authentication to confirm your identity in a computer program or online.

Password Cracking
Password cracking is the process of attempting to guess passwords, given the password file information. See also **Brute Force Attacks**, **Dictionary Attacks** and **Hybrid Attacks**.

Password Sniffing
Passive wiretapping, usually on a local area network, to gain knowledge of passwords.

Patch

A patch is a small security update released by a software manufacturer to fix bugs in existing programs. Your computer's software programs and/or operating system may be configured to check automatically for patches, or you may need to periodically visit the manufacturers' websites to see if there have been any updates.

Peer-to-Peer (P2P) Programs

See **File-Sharing Programs**.

Phishing

Soliciting private information from customers or members of a business, bank or other organization in an attempt to fool them into divulging confidential personal and financial information. People are lured into sharing user names, passwords, account information or credit card numbers, usually by an official-looking message in an email or a pop-up advertisement that urges them to act immediately, usually by clicking on a link provided. See also **Vishing**.

Pharming

Redirecting visitors from a real website to a bogus one. A user enters what is believed to be a valid Web address and is unknowingly redirected to an illegitimate site that steals the user's personal information. On the spoofed site, criminals may mimic real transactions and harvest private information unknowingly shared by users. With this, the attacker can then access the real website and conduct transactions using the credentials of a valid user.

Router

A hardware device that connects two or more networks and routes incoming data packets to the appropriate network. Many Internet Service Providers (ISPs) provide these devices to their customers, and they often contain firewall protections.

Script

A file containing active content -- for example, commands or instructions to be executed by the computer.

Shoulder Surfing

Looking over a person's shoulder to get confidential information. It is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine or type a password. Can also be done long-distance with the aid of binoculars or other vision-enhancing devices. To combat it, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. Also, be sure you password-protect your computer screen when you must leave it unattended, and clear your desk at the end of the day. See also **Clear Desk Policy** and **Clear Screen Policy**.

Skimming

A high-tech method by which thieves capture your personal or account information from your credit card, driver's license or even passport using an electronic device called a "skimmer." Such devices can be purchased online for under $50. Your card is swiped through the skimmer and the information contained in the magnetic strip on the card is then read into and stored on the device or an attached computer. Skimming is predominantly a tactic used to perpetuate credit card fraud, but is also gaining in popularity amongst identity thieves.

Social Engineering

A euphemism for non-technical or low-technology means—such as lies, impersonation, tricks, bribes, blackmail and threats—used to attack information systems. Sometimes telemarketers or unethical employees employ such tactics.

Social Networking Websites

Sites specifically focused on the building and verifying of social networks for whatever purpose. Many social networking services are also blog hosting services. There are more than 300 known social networking websites, including Facebook, MySpace, Friendster, Xanga and Blogspot. Such sites enable users to create online profiles and post pictures and share personal data such as their contact information, hobbies, activities and interests. The sites facilitate connecting with other users with similar interests, activities and locations. Sites vary in who may view a user's profile—some have settings which may be changed so that profiles can be viewed only by "friends." See also **Blogs**.

Spam

Unwanted, unsolicited email from someone you don't know. Often sent in an attempt to sell you something or get you to reveal personal information.

Spim

Unwanted, unsolicited instant messages from someone you don't know. Often sent in an attempt to sell you something or get you to reveal personal information.

Spoofing

Masquerading so that a trusted IP address is used instead of the true IP address. A technique used by hackers as a means of gaining access to a computer system.

Spyware

Software that uses your Internet connection to send personally identifiable information about you to a collecting device on the Internet. It is often packaged with software that you download voluntarily, so that even if you remove the downloaded program later, the spyware may remain. See also **Adware** and **Malware**.

SSL (Secure Socket Layer)

An encryption system that protects the privacy of data exchanged by a website and the individual user. Used by websites whose URLs begin with https instead of http.

Trojan Horse

A computer program that appears to be beneficial or innocuous, but also has a hidden and potentially malicious function that evades security mechanisms. A "keystroke logger," which records victims' keystrokes and sends them to an attacker, or remote-controlled "zombie computers" are examples of the damage that can be done by Trojan horses. See also **Electronic Infection**.

URL

Abbreviation for "Uniform (or Universal) Resource Locator." A way of specifying the location of publicly available information on the Internet. Also known as a Web address.

URL Obfuscation

Taking advantage of human error, some scammers use phishing emails to guide recipients to fraudulent sites with names very similar to established sites. They use a slight misspelling or other subtle difference in the URL, such as "monneybank.com" instead of "moneybank.com" to redirect users to share their personal information unknowingly.

Virus

A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting—i.e., inserting a copy of itself into and becoming part of -- another program. A virus cannot run by itself; it requires that its host program be run to make the virus active. Often sent through email attachments. Also see **Electronic Infection** and **Blended Threat**.

Vishing

Soliciting private information from customers or members of a business, bank or other organization in an attempt to fool them into divulging confidential personal and financial information. People are lured into sharing user names, passwords, account information or credit card numbers, usually by an official-looking message in an email or a pop-up advertisement that urges them to act immediately—but in a vishing scam, they are urged to call the phone number provided rather than clicking on a link. See also **Phishing**.

Vulnerability

A flaw that allows someone to operate a computer system with authorization levels in excess of that which the system owner specifically granted.

Whitelisting Software

A form of filtering that only allows connections to a pre-approved list of sites that are considered useful and appropriate for children. Parents sometimes use such software to prevent children from visiting all but certain websites. You can add and remove sites from the "permitted" list. This method is extremely safe, but allows for only extremely limited use of the Internet.

Worm

Originally an acronym for "Write once, read many times," a type of electronic infection that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively. Once this malicious software is on a computer, it scans the network for another machine with a specific security vulnerability. When it finds one, it exploits the weakness to copy itself to the new machine, and then the worm starts replicating from there, as well. See also **Electronic Infection** and **Blended Threat**.

Zombie Computer

A remote-access Trojan horse installs hidden code that allows your computer to be controlled remotely. Digital thieves then use robot networks of thousands of zombie computers to carry out attacks on other people and cover up their tracks. Authorities have a harder time tracing criminals when they go through zombie computers.

Sources:

National Institute of Standards and Technology:
http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf

Whoiswatchingcharlottesville.org:
http://www.whoswatchingcharlottesville.org/glossary.html

Cyber Security Links

Cyber Security and Privacy Protection

- Carnegie Mellon Software Engineering Institute's CERT Coordination Center:
  www.cert.org/other_sources
- Center for Internet Security (CIS):
  www.cisecurity.org
- Free online security check ups:
  http://www.staysafeonline.org/tools-resources/free-security-check-ups
- National Cyber Security Alliance for Small Business Home Users:
  http://www.staysafeonline.info/
- OnGuard Online:
  www.OnGuardOnline.gov
- SANS (SysAdmin, Audit, Network, Security) Institute's Most Critical Internet Security Vulnerabilities:
  www.sans.org/top20
- Security Tips from Securing our eCity:
  http://securingourecity.org/
- Small Business Solutions form StopBadware:
  http://stopbadware.org/
- The Open Web Application Security Project:
  www.owasp.org

Cyber Security Threat Centers

- McAfee Cybersafety Resource Portal
  http://www.mcafee.com/cru
- McAfee Security Solutions for Small Business:
  http://shop.mcafee.com/Default.aspx?site=us&pid=HOME&CID=MFE-MHP001
- Symantec Security Solutions for Small Business:
  http://store.symantec.com/?om_sem_cid=hho_sem_nam_us_Google_SMB_Store_Home&inid=hho_sem_sy:us:ggl:en:e%7Ckw0000006084%7CSMB

Training and Exercises

- Free training materials, security configuration guides from Internet Security Alliance: http://www.isalliance.org/
- NIH Free Online User Training: http://iase.disa.mil/eta/issv4/index.htm
- NIH Free Online User Training (non DOD version): http://irtsectraining.nih.gov/publicUser.aspx

Government Resources

- Department of Homeland Security (DHS)'s National Strategy to Secure Cyberspace: www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf
- DHS testimony before the House on Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies: http://www.dhs.gov/ynews/testimony/testimony_1300283858976.shtm
- FCC Cyber Security Encyclopedia Page http://www.fcc.gov/cyberforsmallbiz
- FCC Public Safety and Homeland Secuirity Bureau Clearinghouse: http://publicsafety.fcc.gov/pshs/clearinghouse/index.htm
- FCC Public Safety and Homeland Security Bureau Guidelines for Emergency Planning: http://transition.fcc.gov/pshs/emergency-information/guidelines/
- FCC Ten Cybersecurity Tips for Small Businesses http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-306595A1.pdf
- Federal Trade Commission Guide for Business http://www.ftc.gov/bcp/edu/microsites/infosecurity/
- Federal Trade Commission – Identity Theft Information: http://www.onguardonline.gov/topics/computer-security.aspx
- Federal Trade Commission's Interactive Tutorial: www.ftc.gov/infosecurity
- National Institute of Standards and Technology (NIST)'s Computer Security Resource Center: www.csrc.nist.gov
- NIST briefing on Cybersecurity for Small Businesses: http://csrc.nist.gov/groups/SMA/sbc/documents/sbc_workshop_presentation_2015_ver1.pdf

Government Resources (cont'd)

- NIST Guide to Selecting Information Technology Security Products: http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf
- NIST's Risk Management Guide for Information Technology Systems: www.csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- NIST Small Business Corner - A link to the NIST-SBA-FBI Small Business Information Security outreach pages : http://csrc.nist.gov/groups/SMA/sbc/index.html
- NIST Small Business Information Security: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
- SBA, NIST and FBI partnership on Cybersecurity for small businesses: http://csrc.nist.gov/groups/SMA/sbc/overview.html
- United States Computer Emergency Readiness Team (US-CERT): www.us-cert.gov
- U.S. Department of Homeland Security Cyber Security Resources: http://www.dhs.gov/cyber

Publications

- 2011 Awards for best computer security tools, SC Magazine: http://www.scmagazineus.com/2011-sc-awards-us-finalists/section/1908/
- Cloud Security Alliance https://cloudsecurityalliance.org/csaguide.pdf
- Computer Security Resource Center, National Instiitute of Standards and Technology: http://csrc.nist.gov/groups/SMA/sbc/library.html
- Microsoft Small Business Guide: http://www.microsoft.com/smallbusiness/support/security-toolkit-pdf.mspx
- Protecting Your Small Business, Entrepreneur Magazine: http://www.entrepreneur.com/magazine/entrepreneur/2010/june/206656.html
- Small business Information Security: The Fundamentals, National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf