Federal
Communications
Commission

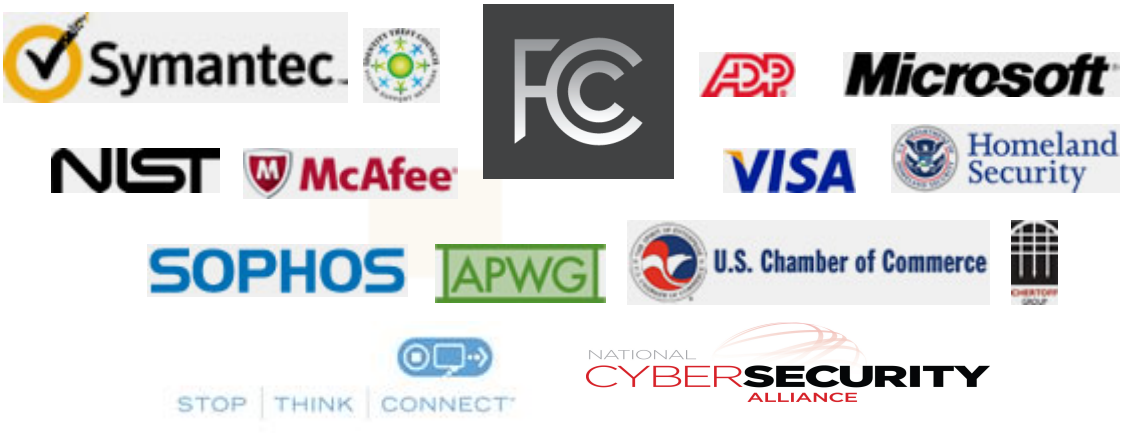

Table of Contents

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.

Privacy and Data Security

Data security is crucial for all small businesses. Customer and client information, payment information, personal files, bank account details - all of this information is often impossible replace if lost and dangerous in the hands of criminals. Data lost due to disasters such as a flood or fire is devastating, but losing it to hackers or a malware infection can have far greater consequences. How you handle and protect your data is central to the security of your business and the privacy expectations of customers, employees and partners.

Cyber Plan Action Items:

1. Conduct an inventory to help you answer the following questions:

- **What kind of data do you have in your business?**

A typical business will have all kinds of data, some of it more valuable and sensitive than others, but all data has value to someone. Your business data may include customer data such as account records, transaction accountability and financial information, contact and address information, purchasing history, buying habits and preferences, as well as employee information such as payroll files, direct payroll account bank information, Social Security numbers, home addresses and phone numbers, work and personal email addresses. It can also include proprietary and sensitive business information such as financial records, marketing plans, product designs, and state, local and federal tax information.

- **How is that data handled and protected?**

Security experts are fond of saying that data is most at risk when it's on the move. If all your business-related data resided on a single computer or server that is not connected to the Internet, and never left that computer, it would probably be very easy to protect.

But most businesses need data to be moved and used throughout the company. To be meaningful data must be accessed and used by employees, analyzed and researched for marketing purposes, used to contact customers, and even shared with key partners. Every time data moves, it can be exposed to different dangers.

As a small business owner, you should have a straightforward plan and policy – a set of guidelines, if you like – about how each type of data should be handled, validated and protected based on where it is traveling and who will be using it.

- **Who has access to that data and under what circumstances?**

Not every employee needs access to all of your information. Your marketing staff shouldn't need or be allowed to view employee payroll data and your administrative staff may not need access to all your customer information.

When you do an inventory of your data and you know exactly what data you have and where it's kept, it is important to then assign access rights to that data. Doing so simply means creating a list of the specific employees, partners or contractors who have access to specific data, under what circumstances, and how those access privileges will be managed and tracked.

Your business could have a variety of data, of varying value, including:

- Customer sales records
- Customer credit card transactions
- Customer mailing and email lists
- Customer support information

- Customer warranty information
- Patient health or medical records
- Employee payroll records
- Employee email lists
- Employee health and medical records
- Business and personal financial records
- Marketing plans
- Business leads and enquiries
- Product design and development plans
- Legal, tax and financial correspondence

2. Once you've identified your data, keep a record of its location and move it to more appropriate locations as needed.

3. Develop a privacy policy

Privacy is important for your business and your customers. Continued trust in your business practices, products and secure handling of your clients' unique information impacts your profitability. Your privacy policy is a pledge to your customers that you will use and protect their information in ways that they expect and that adhere to your legal obligations.

Your policy starts with a simple and clear statement describing the information you collect about your customers (physical addresses, email addresses, browsing history, etc), and what you do with it. Customers, your employees and even the business owners increasingly expect you to make their privacy a priority. There are also a growing number of regulations protecting customer and employee privacy and often costly penalties for privacy breaches. You will be held accountable for what you claim and offer in your policy.

That's why it's important to create your privacy policy with care and post it clearly on your website. It's also important to share your privacy policies, rules and expectations with all employees and partners who may come into contact with that information. Your employees need to be familiar with your legally required privacy policy and what it means for their daily work routines.

Your privacy policy will should address the following types of data:

- **Personally Identifiable Information:** Often referred to as PII, this information includes such things as first and last names, home or business addresses, email addresses, credit card and bank account numbers, taxpayer identification numbers, patient numbers and Social Security numbers. It can also include gender, age and date of birth, city of birth or residence, driver's license number, home and cell phone numbers.

- **Personal Health Information**: Whether you're a healthcare provider with lots of sensitive patient information or you simply manage health or medical information for a small number of employees, it's vital that you protect that information. A number of studies have found most consumers are very concerned about the privacy and protection of their medical records. They do not want their health information falling into the hands of hackers or identity thieves who might abuse it for financial gain. But they also may not want employees or co-workers prying into their personal health details. And they often don't want future employers or insurers finding out about any medical conditions or history.

- **Customer information**: This includes payment information such as credit or debit card numbers and verification codes, billing and shipping addresses, email addresses, phone numbers, purchasing history, buying preferences and shopping behavior.

The Better Business Bureau has a copy of a privacy policy that you are free to download and use. It is available here: http://www.bbbonline.org/reliability/privacy/.

4. Protect data collected on the Internet

Your website can be a great place to collect information – from transactions and payments to purchasing and browsing history, and even newsletter signups, online enquiries and customer requests.

This data must be protected, whether you host your own website and therefore manage your own servers or your website and databases are hosted by a third party such as a web hosting company.

If you collect data through a website hosted by a third party, be sure that third party protects that data fully. Apart from applying all the other precautions that have been described, such as classifying data and controlling access, you need to make sure any data collected through your website and stored by the third party is sufficiently secure. That means protection from hackers and outsiders as well as employees of that hosting company.

5. Create layers of security

Protecting data, like any other security challenge, is about creating layers of protection. The idea of layering security is simple: You cannot and should not rely on just one security mechanism – such as a password – to protect something sensitive. If that security mechanism fails, you have nothing left to protect you.

When it comes to data security, there are a number of key procedural and technical layers you should consider:

Inventory your data

We mentioned before the need to conduct a data inventory so you have a complete picture of all the data your business possesses or controls. It's essential to get a complete inventory, so you don't overlook some sensitive data that could be exposed.

Identify and protect your sensitive and valuable data

Data classification is one of the most important steps in data security. Not all data is created equal, and few businesses have the time or resources to provide maximum protection to all their data. That's why it's important to classify your data based on how sensitive or valuable it is – so that you know what your most sensitive data is, where it is and how well it's protected.

Common data classifications include:

> HIGHLY CONFIDENTIAL: This classification applies to the most sensitive business information that is intended strictly for use within your company. Its unauthorized disclosure could seriously and adversely impact your company, business partners, vendors and/or customers in the short and long term. It could include credit-card transaction data, customer names and addresses, card magnetic stripe contents, passwords and PINs, employee payroll files, Social Security numbers, patient information (if you're a healthcare business) and similar data.
>
> SENSITIVE: This classification applies to sensitive business information that is intended for use within your company, and information that you would consider to be private should be included in this classification. Examples include employee performance evaluations, internal audit reports, various financial reports, product designs, partnership agreements, marketing plans and email marketing lists.
>
> INTERNAL USE ONLY: This classification applies to sensitive information that is generally accessible by a wide audience and is intended for use only within your company. While its unauthorized disclosure to

outsiders should be against policy and may be harmful, the unlawful disclosure of the information is not expected to impact your company, employees, business partners, vendors and the like.

Control access to your data

No matter what kind of data you have, you must control access to it. The more sensitive the data, the more restrictive the access. As a general rule, access to data should be on a need-to-know basis. Only individuals who have a specific need to access certain data should be allowed to do so.

Once you've classified your data, begin the process of assigning access privileges and rights – that means creating a list of who can access what data, under what circumstances, what they are and are not allowed to do with it and how they are required to protect it. As part of this process, a business should consider developing a straightforward plan and policy – a set of guidelines – about how each type of data should be handled and protected based on who needs access to it and the level of classification.

Secure your data

In addition to administrative safeguards that determine who has access to what data, technical safeguards are essential. The two primary safeguards for data are passwords and encryption.

Passwords implemented to protect your most sensitive data should be the strongest they can reasonably be. 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. Employee training on the basics of secure passwords and their importance is a must.

Passwords alone may not be sufficient to protect sensitive data. Businesses may want to consider two-factor authentication, which often combines a password with another verification method, such as a dynamic personal identification number, or PIN.

Some popular methods of two-factor identification include:

- Something the requestor individually knows as a secret, such as a password or a PIN.
- Something the requestor uniquely possesses, such as a passport, physical token or ID card.
- Something the requestor can uniquely provide as biometric data, such as a fingerprint or face geometry.

Another essential data protection technology is encryption. Encryption has been used to protect sensitive data and communications for decades, and today's encryption is very affordable, easy-to-use and highly effective in protecting data from prying eyes.

Encryption encodes or scrambles information to such an advanced degree that it is unreadable and unusable by anyone who does not have the proper key to unlock the data. The key is like a password, so it's very important that the key is properly protected at all times.

Encryption is affordable for even the smallest business, and some encryption software is free. You can use encryption to encrypt or protect an entire hard drive, a specific folder on a drive or just a single document. You can also use encryption to protect data on a USB or thumb drive and on any other removable media.

Because not all levels of encryption are created equal, businesses should consider using a data encryption method that is FIPS-certified (Federal Information Processing Standard), which means it has been certified for compliance with federal government security protocols.

Back up your data

Just as critical as protecting your data is backing it up. In the event that your data is stolen by thieves or hackers, or even erased accidentally by an employee, you will at least have a copy to fall back on.

Put a policy in place that specifies what data is backed up and how; how often it's backed up; who is responsible for creating backups; where and how the backups are stored; and who has access to those backups.

Small businesses have lots of affordable backup options, whether it's backing up to an external drive in your office, or backing up automatically and online so that all your data is stored at a remote and secure data center.

Remember, physical media such as a disc or drive used to store a data backup is vulnerable no matter where it is, so make sure you guard any backups stored in your office or off site and also make sure that your backup data storage systems are encrypted.

6. Plan for data loss or theft

Every business has to plan for the unexpected, and that includes the loss or theft of data from your business. Not only can the loss or theft of data hurt your business, brand and customer confidence, it can also expose you to the often-costly state and federal regulations that cover data protection and privacy. Data loss can also expose businesses to significant litigation risk.

That's why it's critical to understand exactly what data or security breach regulations affect your business and how prepared you are to respond to them. That should be the foundation of a data breach response plan that will make it easier to launch a rapid and coordinated response to any loss or theft of data.

At the very least, all employees and contractors should understand that they must immediately report any loss or theft of information to the appropriate company officer. And because data privacy and breach laws can be very broad and strict, no loss should be ignored. So even if you have sensitive data that just can't be accounted for, such as an employee who doesn't remember where he left a backup tape, it may still constitute a data breach and you should act accordingly.

And just in case you don't think a data breach could happen at your small business, think about this. In 2010, the U.S. Secret Service and Verizon Communications Inc.'s forensic analysis unit responded to a combined 761 data breaches. Of those, 482, or 63 percent, were at companies with 100 employees or fewer. And in 2011 Visa estimated that about 95 percent of the credit-card data breaches it discovers are on its smallest business customers.

The Online Trust Alliance has a comprehensive guide to understand and preparing for data breaches, available at https://otalliance.org/resources/2011DataBreachGuide.pdf.

The Federal Trade Commission has materials to help small businesses secure data in their care and protect their customers' privacy, including an interactive video tutorial, at http://business.ftc.gov/privacy-and-security.

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 HTTPS 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://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Cyber Security Links

Cyber Security and Privacy Protection

- Center for Internet Security (CIS):
  www.cisecurity.org
- Free online security check ups:
  http://www.staysafeonline.org/stay-safe-online/free-security-check-ups
- National Cyber Security Alliance for Small Business Home Users:
  http://www.staysafeonline.org
- 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

- Cyber Safety Links for High School Students
  http://blackboard.aacps.org/portal/lor/obj/mods/4students/HSCybrSfty/addlinks.pdf
- 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/
- Free DOD user training: http://iase.disa.mil/eta/Pages/online-catalog.aspx
- 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: http://www.dhs.gov/national-strategy-secure-cyberspace
- 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/smb-presentation.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://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.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

- 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://download.microsoft.com/download/3/a/2/3a208c3c-f355-43ce-bab4-890db267899b/Security_Guide_for_Small_Business.pdf

- 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