Small Business Cyber Security Guide

University of Southern Maine

Maine Cyber Security Cluster (MCSC)

Cyber Security Organization (CSO)

Contents

Preface

Our goal is to give small business owners a reference on protecting their assets. We understand small business owners are extremely busy and will only read the sections of the guide that pertain to them. Therefore, if you do read the entire guide you will notice some information is repeated.

We recommend reading the *Secure Your Small Businesses Quick Start* section first because it gives great tips that are free to implement and apply to everyone.

Due to the vast number of topics covered we do not go into the technical details of implementing the suggestions given. Many of the suggestions should be easily implemented by your Systems Administrator or your family computer help person. For more assistance, try your internet service provider, local high school or university, or use an internet search on Google or Bing.

Acknowledgments

In the fall of 2012, Charles Largay adjunct professor for the University of Southern Maine's *Introduction to Cyber Security* class, assigned a final project to address some security topics faced by small business. All the students understood that today's small business are a target for criminals due to the lack of knowledge and resources to protect themselves from cyber attacks.

After the class David Lambert took on the project with some members of the University of Southern Maine student club *Cyber Security Organization*. For several months David Lambert, Maureen Largay, Charles Largay, and Brian Kurlychek continued working on the technical information for the guide.

During the summer of 2013 editors Nicole Kearns and Maxwell Chikuta continued with David Lambert to bring the guide to completion. Maxwell Chikuta and David Lambert are currently working on a 15 and 45 minute presentation.

We would like to thank the students in the University of Southern Maine's *Introduction to Cyber Security* (COS 470) class for building the foundation of the guide: Angela Doxsey, Scott Burns, David Briggs, Tristan McCann, Tessa Prince, Sam Wright, Brian Kurlychek, Nathaniel Butler, David Lambert, Brian Tellier, Edward Sihler, Vincent May, Joshua Smith, Maureen Largay, and Professor Charles Largay.

Special thanks to David Lambert for seeing the guide to completion and writing a major portion of the guide.

A big thank you to editors Nicole Kearns and Maxwell Chikuta, for helping out over the summer break.

Introduction

Few small businesses today can function without technology, and most of it involves the public internet. The internet is a great venue for business and offers many benefits; yet, it also presents challenges and dangers that are often difficult for many small business to understand and manage. This guide was created to provide an overview of cyber security best practices for small businesses and to be a starting point to plan how to follow these best practices.
Cyber security intrusions are very real and are increasing daily. The number of small businesses becoming victims of cyber crimes is growing rapidly. This victimization occurs either through scams, fraud, theft, or other malicious criminal activity.

In the first three months of this year alone, there were over one billion Internet based cyber attacks. 40% were against small business, and 77% thought they were prepared. To put that in perspective, there were more than 51 cyber attacks on small businesses every second.

Below are three examples where the damage to the small businesses was significant:

- In 2009, Patco Construction Company of Sanford, Maine lost nearly $600,000 to hackers that likely gained access to passwords and security questions via an implanted virus.
- In May 2012, within one over night heist, cyber thieves were able to rob $180,000 from a communications systems company called Primary Systems in St. Louis, Missouri.
- In July 2012, a family-owned business in southern New England called Consolidated Concrete was robbed of over $100,000 due to a cyber robbery.

The small businesses above were severely compromised and suffered significant losses. Small businesses make up 99.7% of all businesses in the United States according the the Department of Labor. The median number of employees is 4.9 and median income of less than $900,000.00 per year. Losses like those above can be devastating to any small business.

Small business owners tend to be so busy running their businesses that they lack time and access to understand good security practices. In many cases the mistakes they make are the small things that place their business at risk: using default or simple passwords, unsecure network settings, and or using business machines to access personal websites and social media sites.

The “bad actors” and criminals on the internet realize that small businesses often don’t take many of the basic steps, making them more vulnerable because there is less rigor associated with the protection, monitoring, and maintenance of their networks, servers and workstations. Small business owners and operators need to maintain a basic level of cyber defense for the safety of their businesses.

The odds are not in favor of small businesses. While not a certainty, the likelihood of being the target or victim of a cyber attack is real and growing. There is no such thing as being 100% secure, but taking basic steps to understand the risk to business operations and securing networks, servers, workstations, mobile devices, and critical information can decrease the possibilities of having the business breached. Beyond taking these defensive steps, a smart small business operator must develop a plan on how to recover from a cyber attack or when a breach occurs.

Secure Your Small Businesses Quick Start

First, start with taking an inventory of the technology your business uses and review the “12 Key Steps to Better Secure Your Company” below. Second, build a plan to secure your business and allow for a quick recovery from a breach or cyber attack.

It is a normal part of business operations to use locks on the doors to protect valuable products, files, records and other key business assets. The same principle applies to your computer and web-based information systems, because they need locks and protection as well. The biggest challenge in cyber security is realizing when you have been attacked and compromised. A physical break in or theft is often noticeable and action can be taken rapidly, while a cyber attack may be difficult and time consuming to detect.

12 Key Steps to Better Secure Your Company

Below are some basic steps you can take to better secure your existing systems. Most of these tips will be covered in detail throughout this document.

1. Machines that handle sensitive information like payroll or point of sales (POS) must be separate from machines that do routine services, like updating facebook and checking email.
2. Set your Domain Name Service (DNS) of your networked devices card(s) and your business router to one of the following pairs to avoids DNS attacks, and guard against ‘poisoned,’ spoof or fake sites:
    a. 208.67.220.220 and 208.67.222.222 (OpenDNS)
    b. 156.154.70.22 and 156.154.71.22 (Comodo DNS)
    c. 8.8.8.8 and 8.8.4.4 (Google DNS)
3. If possible, change any default username or passwords for a computer , printer, router smart phone, or any other device. - **ANYTHING** is better than the default.
    a. If you can change the **ADMIN** name on your router **DO IT**.
4. Use strong passwords.
    a. Don’t use the same password on different sites, or equipment. Use words not found in a dictionary.
    b. **Example:** Use the 1st two letters from each word in a memorable sentence. Using the sentence above the password would be “**Dousthsapaondisioreq**”.
    c. At the very least, use a favourite password (perhaps <BoS10ReDs0X!> (Boston Red Sox!) with a website's first 3 letters in front - google would be “goo<favouritepassword>”, facebook would be “fac<favoritepassword>”.
    d. Don’t let the browser remember your passwords if you must have the browser

remember passwords, set the master password.
    e. Consider using an online password manager such as http://www.lastpass.com
5. If you must use Windows (but Linux, Unix or OS X are better)
    a. Use antivirus software like http://www.avg.com.
    b. Keep all operating systems and software up to date.
6. Don't install any software you did not go looking for. Keep your software up to date. Remove or uninstall software you are no longer using.
7. Use any browser **EXCEPT Internet Explorer** (Chrome and Chromium are really good, Opera, Comodo Dragon is also good, as is Safari).
8. Use any email client **EXCEPT Outlook**, use BAT, Thunderbird, or Webmail.
9. **BEFORE clicking ANY link** in the e-mail, check the actual address by hovering over (bottom left in Chrome) – make sure it looks legit.
10. In any financial or secure transaction, make sure you see "https:" in the address bar, and a padlock (in front of "https:" – click padlock to check if it looks legit).
11. If you need remote access to your business network. Install a Virtual Private Network (VPN) on all your machines, and network them using the HAMACHI VPN (FREE) at https://secure.logmein.com/products/hamachi/default.aspx which will provide encrypted connections to your own network.
12. If you get a pop-up to do with anything like "you are infected, click here to clean, click here to ignore," **DON'T CLICK ON ANYTHING** Press and hold ALT-F4 on the keyboard to kill the browser window (if you click on "ignore it" or the "x" your machine may get infected).

Putting these changes in place can seem challenging or difficult, but you may get assistance from your own employees or reach out to your local higher educational institution (High School, University, College, Community College, or trusted technology services provider). There are guides to implement the tasks above in the manuals you have.

Additional information is included in this guide, including more detail on each of the above items. Government and Vendor sites also provide tutorials, and many are in video format to assist you in implementing a level security that will keep you protected from the average cyber attack.

Cyber security is more than a checklist, and it won't help you when your system has been compromised. It is important that you create a plan that is appropriate for you business.

Building Your Small Business Cyber Security Plan

A cyber security plan does not need to be overly complex, but it should have the necessary details to cover your situation. Since every business is different we will not go into the details of creating a guide. There are plenty of forms and questionnaires on the web to assist you. Below are a few.

Federal Communications Commission has an exellant online form
http://www.fcc.gov/cyberplanner

Contact your Internet Service Provider (ISP) and software vendors, find out what they have to offer. Below are more helpful links.

AllClear ID Incident Response Workbook
https://www.allclearid.com/data-breach/data-breach-response-plan

Federal Trade Commission (FTC): Bureau of Consumer Protection Business Center
http://business.ftc.gov/

Homeland Security U.S. Computer Emergency Readiness Team (US-CERT) Cyber Security Tips
http://www.us-cert.gov/cas/tips/

Microsoft Business Hub
http://www.microsoftbusinesshub.com/?fbid=7sVpa8DZY7y

On Guard Online: Small Business Resources
http://onguardonline.gov/features/feature-0007-featured-info-small-business

National Institute of Standards and Technology (NIST): Computer Security Resource Center
http://csrc.nist.gov/publications/PubsITLSB.html

National Institute of Standards and Technology (NIST): Small Business Corner
http://csrc.nist.gov/groups/SMA/sbc/index.html

U.S. Chamber of Commerce: Internet Security Essentials for Small Business
http://www.uschamber.com/issues/technology/internet-security-essentials-business

Passwords

There are some very fundamental steps you should take that are considered best practices, for individuals, small and large businesses. Some, but not all of these may not be applicable to your business.

Making a good password

Passwords are an important part of daily internet use, especially in a business setting. Almost every account and computer in a business is or probably should be password protected. So how do we make good passwords? Passwords are more than just a complex attempt at stringing numbers and letters together and require a bit of careful thought and care.

Before talking about what makes a good password, lets look at some tips on how to care for your passwords.

- Use different passwords for different accounts and email addresses.
- Change your passwords often. (Once per month is suggested)
- Say NO to letting a website “remember” your password.
- Don’t store your passwords on your computer.
- Don’t write your passwords on papers you store next to the computer.
- If you must write a password down, lock it away! (It’s valuable after all.)
- Don’t give out your passwords to anyone. Anyone who is authorized to be on the system would have their own login credentials.

Building a Password

As time goes on and technology advances, the suggestions for a good password will change. Techniques such as appending numbers after a word would have worked twenty years ago but are no longer sufficient. Consider criminals will adapt to current recommendations and choose a password accordingly. The following are good suggestions to start with.

- **Bigger is better,** at least 16 characters long when possible, otherwise use the max size.
- Include combinations of uppercase, lowercase, numbers, and special characters. (!@#$%...).
- Avoid real words! Passwords containing words from the dictionary are easier to crack.
- Don’t use personal tidbits just because they are easy to remember, such as birthdays or pin numbers.

- The more a password looks like a random mess, the better.

Now with all these rules, it may seem like your passwords will be impossible to remember. How can you build many good passwords but keep them all in your head?

- Passwords can be close. You might have some patterns of letters that don't change, but the more that changes from password to password it is less likely for a criminal to figure out all your passwords.
- Surround the constant parts of your passwords with different numbers or letters each time, such as the first 3 letters of the site you are logging into.
- Use words or sentences that are easy to remember, but don't use all of the letters. Maybe use every other letter.
- Hold the shift key down for parts of the password.

By following these steps, you can end up with a password that looks complex, but easy to remember because you know how you built it.

Antivirus

Antivirus will protect you from the majority of situations. Nothing is 100% secure so use an antivirus whenever possible. Remember to update your antivirus (and any) software on a regular basis. Some vendors will charge a fee for an update. If you can no longer afford the update, keep using the antivirus because it will protect you from all the known vulnerabilities since the last update. Even an old outdated virus protection program is better than nothing.

Antivirus Software Suite Comparison

All of the antivirus suites in the comparison table below have the following security features: antivirus, firewall, anti-spam, anti-spyware, anti-phishing, anti-adware, rootkit protection, keylogger detection, Trojan detection, browser hijacker detection, P2P file sharing protection, custom scanning modes, automatic updates, and ability to scan USBs and CD/DVDs. The following table indicates some key differences in the software packages, and an overall rating for a small business. (note – trial and free versions are available for some of those listed below):

	Rating	Cost	Sandboxing	Social Network Protection	Password Manager	Privacy & Identity Protection	Help Support Type
Bitdefender	1	$39.95	Yes	Yes	Yes	Yes	Email, Chat, Phone
Kaspersky	2	$79.95	Yes	Yes	Yes	Yes	Email, Chat, Phone
Avast	3	$49.99	Yes	Yes	Yes	Yes	Email, Phone
Norton	4	$79.95	Yes	Yes	Yes	Yes	Email, Phone
AVG	5	$54.99	No	Yes	Yes	Yes	Email, Chat, Phone
BullGuard	6	$59.95	Yes	Yes	No	Yes	Email, Phone
Panda	7	$59.99	Yes	No	Yes	Yes	Email
ESET	8	$59.99	No	Yes	Yes	Yes	Email, Phone
F-Secure	9	$59.99	No	No	Yes	Yes	Email, Phone
G Data	10	$34.95	No	Yes	No	No	Email

Avoiding Scams, Fraud, and Hoaxes

There are many internet scams today, ranging from phishing emails to internet hoaxes, so much that we can't list them all. Instead, we discuss key things that are common to most scams and fraud.

Spelling and Bad Grammar

When a company sends out a mass email usually the email is edited for spelling, grammar, and other mistakes. Bad guys tend not to edit their scams as well, especially when the bad guy's native language isn't English.

Threats

Any threat should be a red flag such as, "Click now or your account will be canceled !" or, "If you don't fill out the form your account will be suspended."

Beware of Links in Email

Check it before you click it, when you get a link in an email. Even if the email is from a trusted source, they could have been compromised and not be aware of it. Check the link by hovering over the link and a the actual URL will be in the lower left or your Chrome browser. Links could send you to an .exe file which is used to spread malware. Be extra careful of unexpected or unsolicited email that has links.

Spoofing Websites or Companies

It is easy for criminals to copy a popular website and make the copy install malware on your system. Sometimes you don't have to click anything on the bad site, just viewing the site could infect your machine.

One way to avoid faked or spoofed sites is to carefully check the URL for errors or inconsistencies with the actual site. For example, http://www.bank0famerica.com for Bank of America. Notice the "o" is actually a zero. Look for ones replacing lowercase "L" or vise-versa. Be aware of anything out of the ordinary.

Another way to avoid spoofed sites is to use Google instead of clicking links. Pick a few key words from the link and Google search it.

If its too good to be true, it probably is.

Is this legit?

Scams can be avoided by asking the simple question. “Is this legit?” Most scams involve a bad person trying to get you to do their bidding. A good way to check for legitimacy is to contact them in a way that the bad person didn’t give you. For example, say you're suspicious of a person calling you from Bank of America. Ask for their name and a supervisor's name, then inform them that you will call them back. If they refuse to give you any name, hang up immediately. Don’t call the phone number they gave you. Don’t go to a website they gave you. Google the business’s official website and use a number or contact that the suspicious person did NOT give you.

Hoaxes and scams are constantly changing and evolving, below are some sites to learn more.

Some of the past scams will resurface from time to time, the Nigerian scam is a good example
http://www.hoax-slayer.com/nigerian-scams.html#nigerian-scams

Snopes - Top Scams
http://www.snopes.com/

Hoax Slayer
http://www.hoax-slayer.com/

Microsoft Safety and Security Center - How to recognize phishing email messages, links, or phone calls
http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx

Apple Support - Identifying fraudulent "phishing" email
http://support.apple.com/kb/HT4933

IRS - Report Phishing
http://www.irs.gov/uac/Report-Phishing

Network Security Fundamentals

There are many types of network access controls that small businesses use. First we will go over some basic configurations that an average person can do.

Basic Network Recommendations

Connect to the ISP provided a router/cable modem. The Internet Service Provider (ISP) may provide a cable modem with routing and wireless capabilities as part of the consumer contract. To maximize administration control over the routing and wireless device, deploy a separate personally-owned routing device and follow these guidelines.

- Limit Administration to Internal Network

When given the option, external remote administration should be disabled for network devices. Disabling remote administration prevents an attacker from changing and possibly compromising the home network

- Implement an Alternate DNS Provider

The Domain Name Servers (DNS) provided by the ISP typically don't provide enhanced security services such as the blocking and blacklisting of dangerous and infected web sites. Consider using either open source or commercial DNS providers to enhance web browsing security. Alternate DNS Servers: 208.67.220.220 (OpenDNS), 156.154.70.22 (Comodo DNS), 8.8.8.8 (google DNS).

- Implement WPA2 on Wireless Network

When searching for suitable replacement devices, ensure that the device is WPA2-Personal certified. The wireless network should be protected using Wi-Fi Protected Access 2 (WPA2) instead of WEP (Wired Equivalent Privacy). Using current technology, WEP encryption can be broken in minutes (if not seconds) by an attacker, which afterwards allows the attacker to view all traffic passed on the wireless network. It is important to note that older client systems and access points may not support WPA2 and will require a software or hardware upgrade.

- Implement Strong Passwords on all Network Devices

In addition to a strong and complex password on the wireless access point, a strong password needs to be implemented on any network device that can be managed via a web interface. For instance, many network printers on the market today can be managed via a web interface to

configure services, determine job status, and enable features such as email alerts and logging.

- Turn off UPNP on all Network Devices

Universal Plug and Play (UPNP) is on by default on most wireless access points and is used to automate connection. Once the network is up and running turn off UPNP to limit others from accessing the wireless access points.

- Separate High Value Devices to Dedicated Sub-Network

Devices handling sensitive information should be on a separate dedicated sub-network. Consider a business that has five computers and one computer to handle accounting transactions and only accounting transactions. One router or wireless access point will connect to the ISP, five computers, and another router creating a sub-network. The router on the sub-network will connect only to the accounting transactions computer.

Advanced Network Recommendations

The following recommendations require a higher level of administrative skills to implement and maintain on home networks than the previous recommendations. These recommendations provide additional layers of security but may impact your web browsing experience or require some iteration to adjust settings to the appropriate thresholds.

Enhanced Wireless Router Configuration Settings

Additional protections can be applied to the wireless network to limit access. The following security mechanisms do not protect against the experienced attacker, but are very effective against a less experienced attacker.

- Filter MAC address

MAC address or hardware address filtering enables the wireless access point to only allow authorized systems to associate with the wireless network. The hardware address for all authorized hosts must be configured on the wireless access point.

- Reduce wireless range

Limiting the transmit power of the wireless access point will reduce the area of operation (signal strength) of the wireless network. This capability curtails the home wireless network from extending beyond the borders of a home (e.g., parking lot or adjacent building).

- Turn off SSID broadcast

SSID cloaking is a means to hide the ssm, the name of a wireless network, from the wireless medium. This technique is often used to prevent the detection of wireless networks by war drivers. It is important to note that enabling this capability prevents client systems from finding the wireless network. Instead, the wireless settings must be manually configured on all client systems.

- Limit number of local IPs

Reducing the dynamic IP address pool or configuring static IP addresses is another mechanism to limit access to the wireless network. This provides an additional layer of protection to MAC address filtering and prevents rogue systems from connecting to the wireless network.

- Disable Scripting Within the Web Browser

If using third party web browsers such as Firefox or Chrome, use NoScript (Firefox) or NotScript (Chrome) to prevent the execution of scripts from untrusted domains. Disabling scripting can cause usability issues, but is an effective technique to reduce web borne attacks. Therefore you will need to tell NoScript or NotScript to allow trusted sites.

- Enable Data Execution Prevention (DEP) for all Programs

By default, DEP is only enabled for essential Windows programs and services. Some third party or legacy applications may not be compatible with DEP, and could possibly crash when run with DEP enabled. Any program that requires DEP to execute can be manually added to the DEP exception list, but this requires some technical expertise.

Secure Browsing Fundamentals

Many attacks are based on the internet browser you may be using. Some malicious sites will infect your machine just by visiting the site. Sometimes you don't need to click anything. Picking the right browser is the first step.

- Avoid Microsoft Internet Explorer

Internet Explorer is not necessarily more or less secure than any other browser but the fact remains it is a major target. The bad guys write malicious code for Internet Explorer because everyone uses it. More than 50% of all users on the internet use Internet Explore. If a person wants to write malicious code that will affect the most people, they will write it for Internet Explorer. We can't expect any company, even as big as Microsoft, to keep up with all the exploits.

Sometimes it is necessary to use Internet Explorer for things like updating Microsoft Windows and thats ok. Use Internet Explorer for website you know to be safe. If your are going to a site you have never heard of or been before, use Google Chrome with NotScript, or Firefox with NoScript.

- Google Chrome is currently the best choice

The Pwn2Own compatition http://en.wikipedia.org/wiki/Pwn2Own has tested the vulnerabliites of web browsers like Chrome, Firefox, and Internet Explorer. It is only a matter of time for the contestants to break all the browsers. Chrome is a better choice because of their rapid response to fix the exploits found, and Chrome is rarely the first to be exploited. Chrome sandboxes each tab that is open, therefore increasing the difficulty for exploitation. In other words, every time you open a tab a new instance of Chrome is created.

- Safari and Firefox are the middle choices

Safari is better than Firefox. Firefox uses the same dll (Data Linked Libraries) files as Internet Explorer, which theoretically means some exploits could apply to both Firefox and Internet Explorer.

Now that you have chosen the best browser, below are some best practices for secure browsing.

- Login in as a Limited User

Microsoft Windows has two major user groups Administrator and Limited. Never go surfing on the web while logged in as an Administrator.

- Use NoScript or NotScripts

Scripts are blocks of code that run when you view a website. Some websites will require scripts to run to to give the user a better experience, some may not. Malicious scripts are used to exploit your system while you visit a malicious website.

NoScript http://noscript.net/ is a Firefox extension that will prevent scripts from running as you surf the web. NoScript will block them all by default and it is up to you to teach NoScript when to allow sites to run scripts. Therefore, when you run NoScript for the first time the web will appear to be broken. Just right click on the website and choose weather you want to allow the entire site or selected scripts.

NotScripts is a similar extension for Google Chrome and can be found in the Chrome Web Store.

- Know what link you are clicking

Check the URL (Universal Resource Locator) or link you are clicking. Ask yourself, “Is this legit?” or, “Does this link go where it says it goes?” Hover your cursor over the link and check to see if it matches the link in the lower left corner of Chrome or Firefox. A malicious link may have incorrect spelling compared to the real site. For example is *http://bannk0famerica.com* or *http://g00gle.com*. Sometimes it’s a zero replacing “o” or a one replacing a lowercase “L.”
Be extra careful of tiny URLs or QR codes because they hide their true destination. Use a google search to find the content you want or where the tiny URL is sending you to.

A good explanation of Tiny URLs
http://en.wikipedia.org/wiki/TinyURL

A good explanation of Bitly, another URL shortener.
http://en.wikipedia.org/wiki/Bitly

A good explanation of QR Codes
http://en.wikipedia.org/wiki/QRcode

When in total doubt try a third party site to check the link. There are websites that will check databases of known malicious sites, below are a few to try.

Comodo is simple and easy to check a URL or website.
http://siteinspector.comodo.com/

McAfee Threat Center has more features like malware searching.
http://www.mcafee.com/us/mcafee-labs/threat-intelligence.aspx

Norton Safe Web is good but lacks advice when no data is found.
https://safeweb.norton.com/

E-Mail Security Fundamentals

E-Mail is a fundamental part of nearly all small businesses. Currently email phishing is common tactic to compromise a business.

- Avoid sending or accepting sensitive information via email

Most email is sent via plain text, which means that anyone who intercepts it can read it.

Unencrypted email stored on a remote server has the potential to be compromised.

- Avoid phishing attempts

Phishing is a technique used by criminals to acquire sensitive user information. Email phishing usually involves a malicious link inside an email that attempts to trick the user to click on it. Once clicked, the user can be taken to a fake site containing malware, which can then be downloaded onto the compromised machine.

In 2008, Akron Children's hospital was compromised when an employee clicked on a malicious link sent by her ex-boyfriend. The spyware sent over 1000 screen shots in less than 10 days before it was discovered. (http://www.pcworld.com/article/172185/article.html)

According to the FCC, 60% of all emails a company receives contains spam, phishing attempts, or otherwise unsolicited email. A properly set up spam filter will help reduce the chances of a breach. Depending on how good the filter is, most spam will be redirected so that no one will be tempted to click on it.

For more information regarding email security, see the FCC's *How to Protect Yourself Online* http://www.fcc.gov/guides/how-protect-yourself-online. Below are some tips from the guide and more.

- Look for an email provider with strong anti-spam filtering capability.

You don't have to use the email service provided by your Internet Service Provider (ISP), the company from which you purchase your access to the Internet, because there are independent email services available. One way email providers compete for your business is to provide better filtering capability. You can also talk to your provider if you think their spam filtering could be improved.

- Use filters

Some email spam filters have settings that can be changed to make them stronger. Check your filter to be sure it's set where you want it to be. If you have questions about changing settings, contact your email provider.

- Identify unwanted spam with the "spam" button.

Many email services allow you to select spam email, and then push a "spam" button to identify it as unwanted email. Use this button if you have it, because it lets your email provider know what emails you don't want.

- Consider viewing email in plain text.

Email settings also allow you to prevent images such as logos and pictures from automatically displaying when you open an incoming email. Open images can contain malware and spyware and let spammers know their emails have been opened, and thus that the emails have been sent to a valid address.

- Turn off auto replies

Set your email so that it doesn't automatically accept incoming appointments or automatically download attachments, again so that you don't let spammers know the email has been sent to a valid address.

- Never respond to spam and avoid chain mail

Try to limit sending or displaying your email address to people or groups you know. Check the privacy policy before sending your address to a Web site or directory, and, if you can, "opt out" of allowing your address to be shared. Protect your friends' addresses by putting them on the "bcc" line when sending emails to a group of people who don't know each other.

- Use separate emails for work and home

In order to limit exposure both at work and home, consider using different usernames for home and work email addresses. Unique usernames make it more difficult for someone targeting your work account to also target you via your personal accounts.

- Configure email software securely

Always use secure email protocols if possible when accessing email, particularly if using a wireless network. Secure email protocols include Secure IMAP and Secure POP3. These protocols, or "always use SSL" for web-based email, can be configured in the options for most email clients. Secure email prevents others from reading email while in transit between your computer and the mail server.

- Be aware of hoaxes and scams

Unsolicited emails containing attachments or links should be considered suspicious. If the identity of the sender can't be verified, consider deleting the email without opening. For those emails with embedded links, open your browser and navigate to the web site either by its well-known web address or search for the site using a common search engine. Be wary of an email requesting personal information such as a password or social security number. Any web service that you currently conduct business with should already have this information.

Securing Servers & Workstations (Windows, Mac and Linux/Unix)

Servers and workstations are a core part of most small businesses' basic operations These devices keep financial records, customer records, business transactions, inventory details as well as the storage and transmittal of other confidential information. It is very important to properly secure these devices. Below are several suggestions for improved server and workstation security.

Windows Host OS

- Migrate to a Modern OS and 64 bit Hardware Platform

Windows 8, 7, and Vista provide substantial security enhancements over earlier Windows workstation operating systems, such as XP. Many of these security features are enabled by default and help prevent many of the common ways that cyber attacks can occur. Upgrading hardware to a 64 bit platform will prevent 32 bit and 16 bit malware from running. Data Execution Protection (DEP) is enabled for all processes on a 64 bit platform, this blocks malware from being able to run in certain areas of your computer system.

- Update Automatically

For any Windows-based OS, verify that Windows Update is configured to provide updates automatically.

- Install a Comprehensive Host-Based Security Suite

A comprehensive host-based security suite provides support for anti-virus, anti-phishing, safe browsing, Host-based Intrusion Prevention System (HIPS), and firewall capabilities. These services work collaboratively to provide a layered defense against the most common security threats. Several security suites today provide access to a cloud-based reputation service for leveraging corporate knowledge and history of malware and domains. Remember to enable any automated update service within the suite to keep signatures up-to-date. Examples of security suites include Microsoft Security Essentials, Bitdefender, Kaspersky, Panda, AVG, Norton, F-Secure, Avast, ESET, G Data Furthermore, and BullGuard.

- Limit Use of the Administrator Account

The first account that is typically created when configuring a Windows host for the first time is the local administrator account. A limited "user" account should be created and used for the bulk of activities conducted on the host to include web browsing, email access, and document

creation/editing. The privileged administrator account should only be used to install updates or software, and configure the host as needed. Browsing the web or reading email as an administrator provides an effective means for an adversary to gain persistence on your host. Within Vista or Windows 7, administrative credentials can be easily accessed by right clicking on any application, selecting the “Run as Administrator” option, then providing the appropriate administrator password. All passwords associated with accounts on the host should be at least 16 characters long and be complex (include upper case, lower case, numbers, special characters).

- Use a Web Browser with Sandboxing

Capabilities Several currently available third party web browsers now provide a sandboxing capability that can contain malware during execution thereby insulating the host operating system from exploitation. Most of these web browsers also provide a feature to auto-update or at least notify you when updates are available for download. Also, promising approaches that move the web browser into a virtual machine (VM) are starting to appear on the market but are not yet ready for mass consumer use. The most secure web-browser is Google Chrome. Do not use Internet Explorer.

- Update to a PDF Reader with Sandboxing Capabilities

A sandbox provides protection from malicious code that may be contained in a PDF file. PDF files have become a popular technique for delivering malicious executables. Several commercial and open source PDF readers now provide sandboxing capabilities as well as block execution of embedded URLs (website links) by default.

- Migrate to Microsoft Office 2007 or Later

If using Microsoft Office products for email, word processing, spreadsheets, presentations, or database applications, upgrade to Office 2007 or later and its XML format for storing documents. By default, the XML file formats do not execute embedded code when opened within Office 2007 or later products thereby protecting the user from malicious code delivered via Office documents. The Office 2010 suite also provides “Protected View” mode which opens documents in read-only mode thereby potentially minimizing the impact of a malicious file.

- Keep Application Software Up-to-Date

Most home users do not have the time or patience to verify that all applications installed on their workstation are fully patched and up-to-date. Since many applications do not have an automated update feature, attackers frequently target these applications as a means to exploit host. Several products exist in the market which will quickly survey the software installed on your workstation and indicate which applications have reached end-of-life, require a patch, or need updating. For some products, a link is conveniently provided in the report to download the latest update or

patch.

- Implement Full Disk Encryption (FDE)

Windows 7 Ultimate as well as Vista Enterprise and Ultimate provide support for Bitlocker Full Disk Encryption (FDE) natively. For other versions of Windows, third party FDE products such as http://www.truecrypt.org are available that will help prevent data disclosure in the event that a laptop is lost or stolen.

- Turn Off Autorun or Autoplay

Windows Autorun is a common avenue to execute malicious software on a system. Be sure to turn off Autorun and Autoplay for any medium such as network drive, Flash drive, CD, and DVD. Some mediums, such as a network drive, are more difficult to disable. Please refer to http://support.microsoft.com/kb/967715 to properly disable Autorun.

- Disable Services and Uninstall Programs Not Used

Limit the running services and installed programs to only what is needed. As the number of services and programs increase the number of avenues for an attack also increases. Turn off print and folder sharing as they are often used to compromise a system.

Apple Host OS

- Maintain an Up-to-Date OS

Configure any Mac OS X system to automatically check for updates. When notified of an available update, provide privileged credentials in order to install the update.

Apple iPad note: this guideline includes the Apple iPad. The iPad requires a physical connection (e.g., USB) to a host running iTunes in order to receive its updates. A good practice is to connect the iPad to an iTunes host at least once a month or just prior to any travel where the iPad will be used.

- Keep Third Party Applications Software Up-to-Date

Periodically check key applications for updates. Several of these third party applications may have options to automatically check for updates. Legacy applications may require some research to determine their status.

- Limit Use of the Privileged (Administrator Account)

The first account that is typically created when configuring a Mac host for the first time is the local administrator account. A non-privileged “user” account should be created and used for the bulk of activities conducted on the host to include web browsing, email access, and document creation/editing. The privileged administrator account should only be used to install updates or software, and configure the host as needed. Browsing the web or reading email as an administrator provides an effective means for an adversary to gain persistence on your host.

- Enable Data Protection on the iPad

The data protection feature on the iPad enhances hardware encryption by protecting the hardware encryption keys with a pass code. The pass code can be enabled by selecting “Settings,” then “General”, and finally “Pass code.” After the pass code is set, the “Data protection is enabled” icon should be visible at the bottom of the screen. For iPads that have been upgraded from iOS 3, follow the instructions at: http://support.apple.com/kb/HT4175.

- Implement FileVault on Mac OS Laptops

In the event that a Mac laptop is lost or stolen, FileVault (available in Mac as x, v10.3 and later) can be used to encrypt the contents of a user’s home directory to prevent data loss.

- Find iPhone

The ‘Find iPhone’ app is a good tool for locating a lost or stolen Apple laptop, iPad, or iPhone. The app uses your device’s location services to broadcast its location to Apple servers, which can then be tracked from any iPhone, iPad, or web browser.

Linux/Unix OS

- Maintain an Up-to-Date OS

Linux, Unix (BSD, Free BSD) and other similar operating systems on servers, workstations and other devices, provide updates occasionally. These updates provide new features, content, and sometimes fix security issues. These updates are provided OTA (over the air) in cell phones as well as over a WI-FI connection for tablets as well as phones. Most devices must be told to update manually, but the operating system automatically checks for the availability of updates, it is the responsibility of the user to apply them and keep their device current.

- Disable Bluetooth and Wireless when not in use

In addition to increasing battery life, there are security concerns with having the wireless radio and Bluetooth enabled when they aren’t in use. Many devices have a default PIN for access to Bluetooth. Those with malicious intent and knowledge of this PIN are able to pair with the device

and potentially read personal information stored therein. Wireless should also be disabled when not in use. Though not generally set up in peer to peer mode, in such a case it would be easy to compromise the device if that were the case.

- Only download Apps from trusted sources

Apps available both from the Google Play store and other sources are potentially malicious. Being based on Linux, the Android OS has a certain amount of security built in, however, given the proper access and permissions, an App can perform malicious actions and or destroy the device. When downloading Apps from the Play store (formerly the Android Market) check reviews, ensure there are a substantial number and check for any credible sources deeming the App to be malicious (a quick internet search usually does it). Also, check the developer to ensure that the App is from who it says it is. An example would be the Angry Birds FREE scam. A third party with malicious intent put up an app called 'Angry Birds FREE' (in contrast to the actual 'Angry Birds'). The App's page in the store looked almost identical to the actual one, but it had roughly 10 reviews, versus the 900,000+ of the actual app. It also had a different developer. Upon installing the software, the App asked to disable security features of the device. With security built into the system, this is never a good sign, ie: red flag.

- Install Antivirus for Android

Though not required for safety and security of the Android device, the installation of an Antivirus program for Android devices is another added layer of security. There are free ones available such as: AVG, McAfee, and Norton, as well as many paid ones such as: AVG Pro, Kaspersky, and Trend Micro.

- Encrypt the data

Under the Location and Security section of an Android device's settings menu, there will be the option to set up a screen lock, and an option for data encryption. The screen lock should be set up to prevent easy access to the device itself. This alone does not provide the optimal level of data security however. The data encryption should also be turned on. The device will provide the option to encrypt personal data, this should be checked to prevent personal data from being obtained. The device will also prevent the option to encrypt the memory card that is inserted (if it supports this) and that should also be turned on to ensure that data is as secure as possible. Third party programs, such as APG (the Android version of GPG) are also available for strong single file encryption.

- Utilize email encryption

A program such as APG, or something similar, should be used to send secure emails and keep sensitive information private. The program is very similar to the PC and MAC versions, and is also compatible with them.

- Utilize a trusted external source or remote storage solution if necessary

Measures should be taken to avoid storing sensitive information on the device itself whenever possible. The device itself, if not secured properly, is an easy target for either social engineering or theft and during such events, the compromise of personal or sensitive data is highly likely. To prevent this, the use of a trusted remote storage solution should be used to prevent the theft or loss of the device itself from posing a risk.

Securing Mobile Devices

The security of mobile devices is an equally important part of many small businesses.

Traveling with Personal Mobile Devices

Many establishments (e.g., coffee shops, hotels, airports, etc.) offer wireless hotspots or kiosks for customers to access the Internet. Since the underlying infrastructure is unknown and security is often lax, these hotspots and kiosks are susceptible to adversarial activity. The following options are recommended for those with a need to access the Internet while traveling:

- Avoid free and open hotspots

Mobile devices (e.g., laptops, smartphones) should utilize the cellular network (e.g., mobile Wi-Fi, 3G or 4G services) to connect to the Internet instead of wireless hotspots. This option often requires a service plan with a cellular provider.

- Use Virtual Private Networks (VPN)

Regardless of the underlying network, users can set up tunnels to a trusted VPN service provider. This option can protect all traffic between the mobile device and the VPN gateway from most malicious activities such as monitoring.

- Restrict usage in free and open hotspots

If using a hotspot is the only option for accessing the Internet, then limit activities to web browsing. Avoid accessing services that require user credentials or entering personal information. Whenever possible, maintain physical control over mobile devices while traveling. All portable devices are subject to physical attack given access and sufficient time.

- Use full disk encryption

If a laptop must be left behind in a hotel room, the laptop should be powered down and have Full Disk Encryption enabled as discussed above (see Host-Based Recommendations- Windows Host OS).

Android OS

- Maintain an Up-to-Date OS

Android devices, like many other, provide updates occasionally. These updates provide new features, content, and sometimes fix security issues. These updates are provided OTA (over the air) in cell phones as well as over a WI-FI connection for tablets as well as phones. Most devices must be told to update manually, but the operating system automatically checks for the availability of updates, it is the user's responsibility to apply them and keep their device current.

- Disable Bluetooth and Wireless when not in use

In addition to increasing battery life, there are security concerns with having the wireless radio and Bluetooth enabled when they aren't in use. Many devices have a default PIN for access to Bluetooth. Those with malicious intent and knowledge of this PIN are able to pair with the device and potentially read personal information stored therein. Wireless should also be disabled when not in use. Though not generally set up in peer to peer mode, in such a case it would be easy to compromise the device.

- Only download Apps from trusted sources

Apps available both from the Google Play store and other sources are potentially malicious. Being based on Linux, the Android OS has a certain amount of security built in, however, given the proper access and permissions, an App can perform malicious actions and or destroy the device. When downloading Apps from the Play store (formerly the Android Market) check reviews, ensure there are a substantial number and check for any credible sources deeming the App to be malicious (a quick internet search usually does it). Also, check the developer to ensure that the App is from who it says it is. An example would be the Angry Birds FREE scam. A third party with malicious intent put up an app called 'Angry Birds FREE' (in contrast to the actual 'Angry Birds'). The said App's page in the store looked almost identical to the actual one, but it had roughly 10 reviews, versus the 900,000+ of the actual app. It also had a different developer. Upon installing the software, the App asked to disable security features of the device. With security built into the system, this is never a good sign, ie: red flag.

- Install Antivirus for Android

Though not required for safety and security of the Android device, the installation of an Antivirus program for Android devices is another added layer of security. There are free ones available such as: AVG, McAfee, and Norton, as well as many paid ones such as: AVG Pro, Kaspersky, and Trend Micro.

- Encrypt the data

Under the Location and Security section of an Android device's settings menu, there will be the option to set up a screen lock, and an option for data encryption. The screen lock should be set up to prevent easy access to the device itself. This alone does not provide the optimal level of data security however. The data encryption should also be turned on. The device will provide the option to encrypt personal data, this should be checked to prevent personal data from being obtained. The device will also prevent the option to encrypt the memory card that is inserted (if it supports this) and that should also be turned on to ensure that data is as secure as possible. Third party programs, such as APG (the Android version of GPG) are also available for strong single file encryption.

- Utilize email encryption

A program such as APG, or something similar, should be used to send secure emails and keep sensitive information private. The program is very similar to the PC and MAC versions, and is also compatible with them.

- Utilize a trusted external source or remote storage solution if necessary

Measures should be taken to avoid storing sensitive information on the device itself whenever possible. The device itself, if not secured properly, is an easy target for either social engineering or theft and during such events, the compromise of personal or sensitive data is highly likely. To prevent this, the use of a trusted remote storage solution should be used to prevent the theft or loss of the device itself from posing a risk.

Social Networking

Social media has become an integral part of modern society, and it appeals to many small businesses as a cheap and easy way to advertise and spread the word about their goods and services. However, society is also full of stories illustrating the security risks and hazards of putting information on the web. Here we offer some tips on how to responsibly represent your business on the web.

A better question to start with however is not how to advertise with social media, but IF you

should be advertising with social media. Before jumping on the Facebook or Twitter bandwagon, here is some food for thought:

People talk anyway. If nothing else, social media has shown us that folks love to discuss things. Posts, likes, blogs: Criticism and gossip are all over the web and chances are your business has been mentioned. Despite what your business says about itself on a social networking site, people will always say more. Providing strong customer service and a desirable product, rather than a fancy fan page, may carry farther through the collective word of mouth.

You may have a website. Let's face it: when you want to make a purchase on Amazon or a similar shopping site, you don't visit their fan page on Facebook. A business website is an excellent way of maintaining your company's identity, while providing a wealth of products and information from your company to the world at large. Also, your content isn't located on a social networking site next to relationship statuses and party posts; your website is just yours.

But everyone's doing it! (except Apple) It may seem like a small point, but Apple has landed the number 2 spot on Interbrand's top 100 brands list (Wasserman, 2012) without representing themselves through the social network. Apple has always built its business around simply providing better, more user-friendly products. From mp3 players to computers, Apple became a household name by delivering a strong product, not by having thousands of likes.

Up to this point, it may seem like we are telling you to stay away from social networking sites. However, the fact still remains that pages on social networking sites are easy and low-cost, making them particularly attractive to small business owners with tight budgets. Risks come from multiple sources when moving your company onto a social networking site, so below are some tips on how to avoid these risks and the sources that these risks might come from:

Your Social Media Page

- Avoid links to other pages

Hackers do a lot of damage by simply getting users to click on something. Don't click on links posted on your business's page, and avoid including links to other pages on your page unless you trust the source, or better yet you own it.

- Use a different email

Email scams are one of the most popular forms of hacking and gathering personal information. It would be a shame if the scam that compromised your personal account gave up your business's Facebook page too. It's a good idea to have a separate work email that you manage your business's pages with.

- Don’t post personal information

This tip applies to everyone who has a social networking account, but for businesses it means not posting the personal details of employees or clients. Hackers can use this information to compromise your employees’ computers and accounts, and in turn damage your company.

- Keep your computer up-to-date

If you have a work computer that you regularly manage your social networking pages on, keep that computer’s operating system and antivirus software updated. By regularly installing updates, you can avoid potential security hazards and loop-holes that used to exist, but were fixed in an update.

Your Employees

Employees shouldn’t get personal on your page. Damaging information can come from anywhere, even a well-minded employee who posts something he shouldn’t on your business’s page. Educate employees about the dangers of posting personal opinions and sensitive information.

- Employees need to know what not to post

Damaging information doesn’t only have to appear on your business’s page. Sensitive information placed anywhere on the web can always end up in the wrong hands. Employees should be aware of which information is public and which is private, and should be reminded not to post any information about the company on the web that is not meant to be seen by everyone.

- Limit social networking in the workplace

Social networking sites are great for connecting people, but they can also expose users to threats and vulnerabilities. The best way to keep these threats from your computers at work is to block social networking sites if accessing them is not needed in workplace. The easiest way to avoid the threats of social networking is to avoid the sites themselves. If your business doesn’t really need the extra exposure of a social networking page, it might be better to stick to a business website and avoid social networking altogether. In this day and age, however, that isn’t likely, but following the tips above and getting other employees to follow these tips is a strong start to socially networking safely.

Social media security tips for small business
http://www.securityforsmallbusiness.com/blog/social-media-security-tips-for-small-business.aspx

6 tips to avoid social networking security disasters
http://www.smallbizdaily.com/9318/6-tips-to-avoid-social-networking-security-disasters

Hey, small-business owner: maybe social media isn't for you
https://www.openforum.com/articles/hey-small-business-owner-maybe-social-media-isnt-for-you

Facebook Security Tips
http://www.facebook.com/help/379220725465972/

Employees and Service Providers

It is very important that you consider who you're working with. This includes your employees and your service providers and any other people who might be coming in contact with your systems.

- Ask for references and follow up on them

The best source to find out if the company or person you are dealing with is honest and legit is to check their references. Get in contact with their reference and ask how they came to know the person or vendor? How was their experience with them? Would they recommend them to their mother or sister? The more questions you ask the better chance you will filter out the liars.

For vendors, go to their customers and inquire about them. For example, say you are looking for a painter to paint your building. Get references from the painter and visit the customers of painter's work. People tend to be more truthful in person and you can inspect the work while you are there.

The Small Business Administration is an excellent source to help you hire an employee, contractor or vendor.
http://www.sba.gov/

Consumer Action is a great source to assist unhappy customers properly complain to a company.
http://www.consumer-action.org/

Knowing who to complain to will give you a source to check. For example, if you want to check on a local contractor you would ask the Better Business Bureau if they have received complaints on that contractor.

Check the Better Business Bureau
http://www.bbb.org/

Do a background check, the Small Business Administration is a great source on background checks.
http://www.sba.gov/content/performing-pre-employment-background-checks

The best advice is to do your homework when hiring an employee, contractor or vendor. Follow up on references and ask many questions. Try to get examples of their work and trust your gut.

Facility and Physical Security

It is important to pay attention to the security of your information services assets, especially at your place of business. Know what physical places in your business are the most at risk. A good example is the cash register, it is a place of risk therefore the area needs to be visible and video recording is advised. Below are some suggestions to consider.

- Understand what is sensitive information

Sensitive information is usually associated with personal information which can be connected to an individual person. For example, a Social Security, or driver's licence number is sensitive information while a person's age is not. Some more examples of sensitive information are listed below:

1. Social Security numbers (SSNs)
2. Credit card or other financial account numbers
3. Drivers license numbers
4. Personally identifiable information pertaining to individuals (employees, applicants, parental/familial relatives)
5. Employee schedules and vacation times.
6. Medical and health data
7. Proprietary and/or copyrighted data, such as research data and publications
8. Confidential legal or financial data
9. Vendor and subcontractor agreements and schedules

Some information may not seem sensitive but can still be a liability to you or your company. Your company's vendors or subcontractors could be compromised in order to access your company. When in doubt, keep information confidential.

- Secure the environment

Monitors for computers that handle sensitive information like customer account information, should not face any public spaces. A computer used to check in customers should have the

monitor facing away from windows and the waiting room.

- Lock it

Teach your employees not to leave laptops, cellphones, or any device having sensitive data, unattended or unsecured. Lock the screen and require a password to get back in when an employee leaves the area. Consider cable locks for laptops, to prevent theft.

- Be prepared if equipment is stolen

If a laptop has sensitive data consider using LoJack http://www.lojack.com/Laptops to assit law enforcment to recover the laptop if it is stolen. TrueCrypt http://www.truecrypt.org/ can also be used to prevent thieves from reading the contents of the laptop.

- Your employees are your best defence

Small business are usually small enough that everyone knows everyone therefore, an employee badge system may not be needed. Teach your employees to be alert and question suspicious people in the work environment. Your employees should be alert if random people arrive unexpectedly. For example, if a person dressed as a UPS carrier arrives during a time when a package is not expected, your employees should be asking for confirmation to ensure the individual really is a UPS employee. Don't use the number given by the individual and instead call the local UPS directly. Teaching your employees to be suspicious and ask questions is the best line of defence. Encourage people to question whether a person should be here and wonder if this really the boss on the phone.

- Secure printed materials

Minimize printed sensitive information and destroy or shred the paper when no longer needed. Teach employees not to leave sensitive information lying on a desk or out in the open. Keep sensitive paper files locked in a cabinet. Consider locking sensitive account information in a safe.

- Dispose of trash securely

Any paper documents containing sensitive information should be shredded.

Computer equipment should be destroyed properly. A hard drive no longer in use should be taken apart to break the disk inside. Drilling holes throughout the drive will also break the disk inside.

Small Business Operational Security

Having consistent and thorough guidelines for data management is key to protecting your confidential business and customer data.

- Exchanging Home and Work Content

Government-maintained hosts like the ones used in many work environments are generally configured more securely than those in your home environment. These government-maintained hosts also have an enterprise infrastructure in place (email filtering, web content filtering, IDS, etc.) for preventing and detecting malicious content. Since many users do not exercise the same level of security on their home systems (e.g., limiting the use of administrative credentials), home systems are generally easier to compromise. The forwarding of content (e.g., emails or documents) from home systems to work systems either via email or removable media may put work systems at an increased risk of compromise. For those interactions that are solicited and expected, have the contact send any work-related correspondence to your work email account.

- Storage of Personal Information on the Internet

Personal information which has traditionally been stored on a local computing device is steadily moving to the Internet cloud. Examples of information typically stored in the cloud include webmail, financial information, and personal information posted to social networking sites. Information in the cloud is difficult to remove and governed by the privacy policies and security of the hosting site. Individuals who post information to these web-based services should ask themselves, “Who will have access to the information I am posting?” and “What controls do I have over how this information is stored and displayed?” before proceeding. Internet users should also be aware of personal information already published online by periodically searching for their personal information using popular Internet search engines.

- Use of Social Networking Sites

Social networking sites provide an incredibly convenient and efficient way to share personal information with family and friends. This convenience introduces some new factors that need to be taken into consideration to mitigate risk. While this does provide a convenient way to share information, *anybody* can potentially access the information. It is therefore critical to periodically review the website's privacy policy and the privacy settings made available to you.

It is essential to think twice concerning the information one is making available. Users should think twice about posting information such as address, phone number, place of employment, and other personal information that can be used to target or harass you. If available, consider limiting access to posted personal data to “friends only” and attempt to verify any new sharing requests either by phone or in person.

Use caution when receiving content (such as third-party applications) from friends and new acquaintances. There are some applications that can bypass your security settings and expose your information. This content may appear benign and provide new features, but in actuality it may have a malicious component that is not apparent to the typical user.

Several social networking sites now provide a feature to opt-out of exposing your personal information to Internet search engines. A good recommendation is to periodically review the security policies and settings available from your social network provider to determine if new features are available to protect your personal information.

- Enable the Use of SSL/TLS Encryption Application encryption (https in your browser)

This protects the confidentiality of sensitive information while in transit. SSL also prevents people who can see your traffic (for example at a public WiFi hotspot) from being able to impersonate you when logging into web based applications (webmail, social networking sites, etc.). Whenever possible, web-based applications such as browsers should be set to force the use of SSL. Financial institutions rely heavily on the use of SSL to protect financial transactions while in transit. Many popular applications such as Facebook and Gmail have options to force all communication to use SSL by default. Most web browsers provide some indication that SSL is enabled, typically a lock symbol either next to the URL for the web page or within the status bar along the bottom of the browser.

Email Best Practices

E-Mail is a fundamental part of nearly all small businesses. Currently email phishing is common tactic to compromise a business.

- Avoid sending or accepting sensitive information via email

Most email is sent via plain text, which means that anyone who intercepts it can read it. Unencrypted email stored on a remote server has the potential to be compromised.

- Avoid phishing attempts

Phishing is a technique used by criminals to acquire sensitive user information. Email phishing usually involves a malicious link inside an email that attempts to trick the user to click on it. Once clicked, the user can be taken to a fake site containing malware, which can then be downloaded onto the compromised machine.

For more information regarding email security, see the FCC's *How to Protect Yourself Online* http://www.fcc.gov/guides/how-protect-yourself-online. Below are some tips from the guide and

more.

- Look for an email provider with strong anti-spam filtering capability.

You don't have to use the email service provided by your Internet Service Provider (ISP), the company from which you purchase your access to the Internet, but can chose an independent email service. One way email providers compete for your business is to provide better filtering capability. You can also talk to your provider if you think spam filtering could be improved.

- Use filters

Some email spam filters have settings that can be changed to make them stronger. Check your filter to be sure it's set where you want it to be. If you have questions about changing settings, contact your email provider.

- Identify unwanted spam with the "spam" button.

Many email services allow you to select spam email, and then push a "spam" button to identify it as unwanted email. Use this button if you have it, because it lets your email provider know what email you don't want.

- Consider viewing email in plain text.

Email settings also allow you to prevent images such as logos and pictures from automatically displaying when you open an incoming email. Open images can contain malware and spyware and let spammers know their emails have been opened, and thus that the emails have been sent to a valid address.

- Turn off auto replies

Set your email so that it doesn't automatically accept incoming appointments or automatically download attachments, again so that you don't let spammers know the email has been sent to a valid address.

- Never respond to spam and avoid chain mail

Try to limit sending or displaying your email address to people or groups you know. Check the privacy policy before sending your address to a Web site or directory, and, if you can, "opt out" of allowing your address to be shared. Protect your friends' addresses by putting them on the "bcc" line when sending emails to a group of people who don't know each other.

- Use separate emails for work and home

In order to limit exposure both at work and home, consider using different usernames for home and work email addresses. Unique usernames make it more difficult for someone targeting your work account to also target you via your personal accounts.

- Configure email software securely

Always use secure email protocols if possible when accessing email, particularly if using a wireless network. Secure email protocols include Secure IMAP and Secure POP3. These protocols, or “always use SSL” for web-based email, can be configured in the options for most email clients. Secure email prevents others from reading email while in transit between your computer and the mail server.

- Be aware of hoaxes and scams

Unsolicited emails containing attachments or links should be considered suspicious. If the identity of the sender can’t be verified, consider deleting the email without opening. For those emails with embedded links, open your browser and navigate to the web site either by its well-known web address or search for the site using a common search engine. Be wary of an email requesting personal information such as a password or social security number. Any web service that you currently conduct business with should already have this information.

Password Management

Ensure that passwords and challenge responses are properly protected since they provide access to large amounts of personal and financial information. Passwords should be unique for each account. They should also be strong and difficult to guess. A strong password should be at least 16 characters long and contain multiple character types (lowercase, uppercase, numbers, and special characters). A unique password should be used for each account to prevent an attacker from gaining access to multiple accounts if anyone password is compromised. Disable the feature that allows programs to remember passwords and automatically enter them when required.

Additionally, many online sites make use of password recovery or challenge questions. The answers to these questions should be something that no one else would know or find from Internet searches or public records. To prevent an attacker from leveraging personal information about yourself to answer challenge questions, consider providing a false answer to a fact-based question, assuming the response is unique and memorable.

Photo/GPS Integration

Many phones and some new point and shoot cameras embed the GPS coordinates for a particular location within a photo when taken. Care should be taken to limit exposure of these photos on the Internet, ensure these photos can only be seen by a trusted audience, or use a third party tool to remove the coordinates before uploading to the Internet.

These coordinates can be used to profile the habits and places frequented for a particular individual, as well as provide near real time notifications of an individual's location when uploaded directly from a smartphone. Some services such as Facebook automatically strip out the GPS coordinates in order to protect the privacy of their users.

Software

Know what software is crucial to the functionality of your business and keep a log of all the software your company uses. Having a log of all the software or applications will help you identify what is crucial to the business and what can be taken away. Below are some tips regarding software.

- Never install something you initially did not go looking for

When exploring new places on the web or going to a link that has been shared, be wary of requests to install new software, drivers or anything else. Some websites will require a Java or Flash plugin, then provide a convenient link to install the plugin. Do not click on the convenient link provided, use a popular search engine to find the required plugin and install from the provider's website.

- Keep your software up to date

Updating the operating system is not enough, you must update the software installed to keep vulnerabilities to a minimum.

- Remove software not used or unnecessary

The security of any system is directly related to how many features are offered. The more software installed on a computer, the more opportunities a criminal has to infiltrate or compromise your system. Plus, having less software means less updates to do and easier management.

Payment Cards and Point of Service Systems

The security of point of service payment systems is a very important part of many small businesses. If you business accepts credit or debit card payments you must take steps to secure your customer's information. The FCC Cyber Plan at http://www.fcc.gov/cyberplanner has an excellant section titled Payment Cards, below are some good pointers from that section with additional advise.

- Understand and catalog customer and card information you keep

Make a list of the type of customer and card information you collect and keep such as, names, addresses, identification information, payment card numbers, magnetic stripe data, bank account details and Social Security numbers. It's not only card numbers criminals want; they're looking for all types of personal information, especially if it helps them commit identity fraud.

- Understand where you keep such information and how it is protected
- Determine who has access to this data and if they need to have access
- Evaluate whether you need to keep all the data you store

Once you know what information you collect and store, evaluate whether you really need to keep it. Often businesses may not realize they're logging or otherwise keeping unnecessary data until they conduct an audit.

It is best to store as little as possible when it comes to credit and debit card information such as payment card numbers and magnetic stripe data. Not keeping sensitive data in storage makes it harder for criminals to steal it. If you've been using card numbers for purposes other than payment transactions, such as a customer loyalty program, ask your merchant processor if you can use alternative data instead. Tokenization for example, is technology that masks card numbers and replaces it with an alternate number that can't be used for fraud.

- Use secure tools and services

The payments industry maintains lists of hardware, software and service providers who have been validated against industry security requirements. Small businesses that use integrated payment systems, in which the card terminal is connected to a larger computer system, should check the list of validated payment applications to make sure any software they employ has been tested. Have a conversation about security with your provider if the products or services you are currently using are not on the lists.

- Control access to payment systems

Whether you use a more complicated payment system or a simple standalone terminal, make

sure you carefully control access. Isolate payment systems from other, less secure programs, especially those connected to the Internet. For example, don't use the same computer to process payments and surf the Internet or check email.

- Control or limit access to payment systems to only employees who need access

Make sure you use a secure system for remote access or eliminate remote access if you don't need it so that criminals cannot infiltrate your system from the Internet. Keep your POS system separate from any other public or business network.

- Use security tools and resources

Work with your bank or processor and ask about the anti-fraud measures, tools and services you can use to ensure criminals cannot use stolen card information at your business.

For e-commerce retailers

The CVV2 code is the three-digit number on the signature panel that can help verify that the customer has physical possession of the card and not just the account number. Retailers can also use Address Verification Service to ensure the cardholder has provided the correct billing address associated with the account. Services such as Verified by Visa prompt the cardholder to enter a personal password confirming their identity and providing an extra layer of protection.

For brick and mortar retailers

- Swipe the card and get an electronic authorization for the transaction.
- Check that the signature matches the card.
- Ensure your payment terminal is secure and safe from tampering.
- Remember the security basics
- Use strong, unique passwords and change them frequently.
- Use up-to-date firewall and anti-virus technologies.
- Do not click on suspicious links you may receive by email or encounter online.

Helpful links

You don't have to tackle security on your own. Work with your bank or processor to make sure you're getting the support and expertise you need.

Visa offers a data security guide for small business as part of its Cardholder Information Security Program

http://usa.visa.com/merchants/risk_management/data_security_demo/popup.html

Information about industry security standards is available from the PCI Security Standards Council
https://www.pcisecuritystandards.org

The Paysimple.com blog offers a helpful post on credit card security
http://paysimple.com/blog/2011/09/01/5-tips-for-proper-handling-of-customer-credit-card-account-information/

American Express provides data security advice for merchants
https://www260.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=US

MasterCard offers resources for on safeguarding customer information
http://www.mastercard.us/small-business/resources/index.html

Incident Response and Reporting

Depending on your type of business and the type of cyber attack or event you may encounter, there are varying responsibilities for notification.

What is an incident?

The following is an excerpt from the Data Breach Response Checklist
http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf

A data breach is any instance in which there is an unauthorized release or access of Personally Identifiable Information (PII) or other information not suitable for public release. This definition applies regardless of whether an organization stores and manages its data directly or through a contractor, such as a cloud service provider. Data breaches can take many forms including

1. Hackers gaining access to data through a malicious attack
2. Lost, stolen, or temporarily misplaced equipment (e.g., laptops, mobile phones, portable thumb drives, etc.)
3. Employee negligence (e.g., leaving a password list in a publicly accessible location, technical staff misconfiguring a security service or device, etc.)
4. Policy and/or system failure (e.g., a policy that doesn't require multiple overlapping security measures—if backup security measures are absent, failure of a single protective system can leave data vulnerable)

In some cases, an organization may discover that control over PII, medical information, or other sensitive information has been lost for an unspecified period of time, but there is no evidence that data have been compromised. In such an instance, unless applicable federal, state, or local data breach notification laws would define this as constituting a breach, it would be up to the organization to determine whether to treat the incident as a full-scale breach or as inadequate security practice requiring immediate correction.

Unauthorized access to PII are especially serious, as the leaked information can be used by criminals to make fraudulent purchases, obtain loans or establish lines of credit, and even obtain false identification documents. Childrens' data are of particular interest to criminals. Criminals are often interested collecting the child's social security numbers (SSNs), permanent resident card (green card) serial numbers, naturalization document control numbers, and other PII to obtain credit or apply for benefits fraudulently. , Parents and the affect youth themselves may not be monitoring their credit histories until the children get older, which is why criminals are so interested in collecting their data.

Although electronic attacks by hackers and other cyber-criminals are a common cause of data breaches, other types of breaches occur regularly as well. "Insider threats," or threats coming from inside the organization, are also common and often involve employees accidentally, unknowingly, or maliciously mishandling, exposing, or losing sensitive data. All breaches are equally dangerous regardless of the cause, as they leave PII and other sensitive data vulnerable to exploitation. Every company or institution should, therefore, be prepared to detect and respond to the eventuality of a breach.

What to Do

Once you have discovered the breach or noticed that sensitive data might have been leaked, do the following.

- Stop the bleeding

If you think a machine has been compromised then disconnect it from the network and any other device attached to it like printers or card machines.

- Leave the infected machine running

If you shut off the machine you could destroy valuable evidence the Secret Service can use. Keep the machine running until authorities arrive.

- Call the Secret Service or FBI

Usually breaches will fall under Secret Service jurisdiction.

Secret Service field office list.
http://www.secretservice.gov/field_offices.shtml

FBI field office list
http://www.fbi.gov/contact-us/field

- Check Reporting Requirements.

Each state has different reporting requirements depending on the situation. The National Conference of State Legislature has links to the state security breach notification laws to explain the requirements.

State Security Breach Notification Laws
http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

- Hire an Attorney

We live in an “I sue you,” society. Find an attorney that has experience in Privacy and Data Security law.

- Inform affected parties

Informing all affected parties early and often may be the difference in keeping customers happy about how you handled the breach. It may also be a legal requirement to notify all affected parties.

- Fix it.

After the authorities are finished with the investigation you will need to remove the infection from the machine. Virus, trojans, and other malware have become quite advanced and difficult to remove. It is usually best to reformat the harddrive and do a fresh install. Be aware it is possible, but rare for malware to survive a reformat of the hard drive. It is also possible that several machines could be infected, so consider hiring a professional to do an analysis of your network and clean up the infection.

- Revisit Security Practices.

Make sure you have a plan to respond to a breach or incident. Keep your systems up to date. Use strong passwords and teach employees to avoid security risks. Below are some links.

What to Do If Your Business Gets Hacked
http://businessonmain.msn.com/browseresources/articles/onlinebusiness.aspx?cp-documentid=31726409

How Small Businesses Can Protect and Secure Customer Information
http://www.sba.gov/community/blogs/community-blogs/business-law-advisor/how-small-businesses-can-protect-and-secure-cus

What if my Business Get Hacked
http://www.securityforsmallbusiness.com/blog/what-if-my-business-gets-hacked.aspx

Data Breach Response Checklist
http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf

Above all communication is key to incident response and reporting. The cyber security community frowns upon those who hide a breach or attempt to deny their wrong doings. Being honest and asking for help when you need it can make the difference in whether your breach will remain a media headline or just a quick problem that was corrected.

Helpful links

Computer Security Incident Handling Guide
http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

---

Recovering from a Cyber Attack, Event, or Disaster

While taking preventative measures is important, it is also important to have a recovery plan in case a cyber attack or cyber event. Having an up to date security plan and following the recommendations will make recovering from an attack easier.

Unfortunately, if you have been attacked or compromised by criminal action, your equipment, servers, workstations, and even network gear may be needed by law enforcement personnel to track down the perpetrators. Statistically small businesses that close their doors for a disaster longer than a weeks time, rarely survive and recover. This is why it is important to plan ahead, and be aware of what to expect.

Key Disaster Recovery Principles

Small businesses should not wait until after a disaster to think about what should have been done to protect their data.

- Don’t wait until it’s too late

Not only is downtime costly from a financial perspective, but it could mean the complete demise of the business. Small businesses should map out disaster preparedness plans ahead of time, including the identification of key systems, data and other resources that are critical to running the business.

- Protect information completely

To reduce the risk of losing critical business information, small businesses must implement the appropriate security and backup solutions to archive important files, such as customer records and financial information for the long term. Natural disasters, theft and cyber attacks can all result in data and financial loss, so small businesses need to make sure important files are saved not only on an external hard drive and/or company network, but in a safe, off-site location.

- Get employees involved

Employees play a key role in helping to prevent downtime. They should be educated on computer security best practices and what to do if information is accidentally deleted or cannot easily be found in their files. Since small businesses often have limited resources, all employees should know how to retrieve the businesses’ information in times of disaster.

- Test frequently

Regular disaster recovery testing is invaluable. After a disaster hits is the worst time to learn that critical files were not backed up as planned. Test your plan anytime anything changes in your environment.

- Review your plan

If frequent testing is not feasible due to resources and bandwidth, small businesses should at least review their disaster preparedness plan on a quarterly basis.

- Be prepared

It is always better and less costly to invest in adequate security up-front rather than going through a costly incident response which could result in rebuilding your entire network infrastructure. Organizations should:

1. Identify all functions, then determine which must be continued under all circumstances
2. Prioritize these essential functions
3. Establish staffing and resource requirements
4. Integrate supporting activities
5. Develop a plan to perform additional functions as the situation permits.
6. Consider alternate locations

Alternate facilities should provide:

1. Sufficient space and equipment
2. Capability to perform essential functions within 12 hours, up to 30 days
3. Reliable logistical support, services, and infrastructure systems
4. Consideration for health, safety, and emotional well-being of personnel
5. Interoperable communications
6. Computer equipment and software

Business Continuity and Recovery Plan

The following was taken from:
http://smallbusiness.chron.com/examples-continuity-operations-plans-13528.html

When you own a business, it's not sufficient to simply run the company well and build a customer base. You must also plan for the possibility of a business disruption due to an unforeseen event such as a natural disaster. Many businesses make the mistake of failing to develop a Continuity of Operations Plan (COOP). For the prepared business owner, a COOP can be the single best investment in your future.

Continuity of Operations

All businesses have requirements that are critical to their function. You may have a printer contracted to create tickets, or specialized equipment that you can't do business without. If you lose your equipment or your supplier in a disaster, how will you replace them? If your supplier is out of town, is his phone number recorded only at work? Can you operate if your customer records are lost in a flood, or if they're only stored on your recently-fried computer hard drive? A COOP forces you to think analytically about your business, identify its critical resources, personnel and weaknesses, then construct contingencies and put them into a plan.

Business Impact Analysis

The first task in developing a COOP is doing a Business Impact Analysis (BIA). The BIA reduces your business to its core functions and helps you identify the most basic structure you'd need to continue operating. You look at your business function by function to determine which functions are the most critical and must continue for your business to survive the disaster. Take into

account the financial and operational impact such as order and distribution processing, for example. Identify the personnel, resources, equipment and systems needed to survive with only essential services, and determine when the absent services will adversely affect you.

Risks

Identify the potential risks to your organization to determine the best contingency plan for the affected assets. If you determine that the minimum number of office personnel you need is 50, for example, find an alternative location that fits 50 workers and ensure it'll be available. If you have specialized equipment in an open yard that's prone to tornadoes, determine the minimum number of machines you must have to avoid disruption, and find an alternate location to store that equipment during tornado season. Don't think you're going overboard in your worst case scenarios. However, if your area only receives blizzards than it most likely isn't necessary to plan for tornados.

Resiliency

When you look at your business this closely, you'll identify easily correctable flaws that will make recovery more likely. For example, if you have a critical function that only one person can perform, cross train someone else in the event the experienced person is unavailable during a disaster. If you perform all of your critical tasks in one location, consider decentralizing it, so all critical functions aren't so concentrated. Be sure you backup your critical data each night, ensuring the items you identified as critical are included, and move a copy to a separate location.

Download the plan and follow the template.
http://www.ready.gov/sites/default/files/documents/files/sampleplan.pdf

Helpful Links

DHS Disasters
http://www.dhs.gov/topic/disasters

NIST Contingency Planning Guide for Federal Information Systems
http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

FEMA Preparedness Planning for Your Business
http://www.ready.gov/business

A webinar from 2010 that includes some templates
http://www.sacog.org/coop/

SBA Disaster Recovery Plan
http://www.sba.gov/sites/default/files/Disaster%20Recovery%20Plan%202012.pdf

Links

Below is a list of all links included in this guide plus some additional guides and organizations that can provide more detailed information.

Contractors / Employees

BBB: Better Business Bureau
http://www.bbb.org/

Consumer Action: Welcome to Consumer Action
http://www.consumer-action.org/

SBA: Small Business Administration
http://www.sba.gov/

SBA: Pre-Employment Background Checks
http://www.sba.gov/content/performing-pre-employment-background-checks

Credit Cards

American Express: Data Security for Merchants
https://www260.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=US

MasterCard: EDUCATIONAL WEBINAR SERIES
http://www.mastercard.us/small-business/resources/index.html

PaySimple: 5 Tips for Proper Handling of Customer Credit Card Account Information
http://paysimple.com/blog/2011/09/01/5-tips-for-proper-handling-of-customer-credit-card-account-information/

Disasters / Events / Breaches

Chron: Examples of Continuity Operations Plans
http://smallbusiness.chron.com/examples-continuity-operations-plans-13528.html

DOE: Data Breach Response Checklist
http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf

DHS: Disasters
http://www.dhs.gov/topic/disasters

FEMA: Preparedness Planning for Your Business
http://www.ready.gov/business

MSN: What to Do If Your Business Gets Hacked
http://businessonmain.msn.com/browseresources/articles/onlinebusiness.aspx?cp-documentid=31726409

NCSL: State Security Breach Notification Laws
http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

NIST: Computer Security Incident Handling Guide
http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

NIST: Contingency Planning Guide for Federal Information Systems
http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

SBA: Disaster Recovery Plan
http://www.sba.gov/sites/default/files/Disaster%20Recovery%20Plan%202012.pdf

SBS: What if my Business Get Hacked
http://www.securityforsmallbusiness.com/blog/what-if-my-business-gets-hacked.aspx

General / More Info

DHS: State and Local Law Enforcement Resource Catalog
http://www.dhs.gov/sites/default/files/publications/Policy-OSLLE/OSLLE%20Resource%20Catalog%20-%201-18-2013.pdf

FBI: Local Offices
http://www.fbi.gov/contact-us/field

FCC: How to Protect Yourself Online
http://www.fcc.gov/guides/how-protect-yourself-online

FTC: Bureau of Consumer Protection Business Center
http://business.ftc.gov/

Microsoft Business Hub
http://www.microsoftbusinesshub.com/?fbid=7sVpa8DZY7y

National Cyber Security Alliance: Resources
http://www.staysafeonline.org/stay-safe-online/resources/

National Cyber Security Alliance: IMPLEMENT A CYBERSECURITY PLAN
http://www.staysafeonline.org/business-safe-online/implement-a-cybersecurity-plan/

NSA: Best Practices for Keeping Your Home Network Secure
http://www.nsa.gov/ia/_files/factsheets/Best_Practices_Datasheets.pdf

NIST: Technical Guide to Information Security Testing and Assessment
http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

NIST: Small Business Corner
http://csrc.nist.gov/groups/SMA/sbc/index.html

NIST: ITL Security Bulletins
http://csrc.nist.gov/publications/PubsITLSB.html

On Guard Online: Small Business Resources
http://onguardonline.gov/features/feature-0007-featured-info-small-business

PCI: Security Standards Council
https://www.pcisecuritystandards.org

SBA: How Small Businesses Can Protect and Secure Customer Information
http://www.sba.gov/community/blogs/community-blogs/business-law-advisor/how-small-businesses-can-protect-and-secure-cus

Smallbizdaily: 6 tips to avoid social networking security disasters
http://www.smallbizdaily.com/9318/6-tips-to-avoid-social-networking-security-disasters

US-CERT: Tips
http://www.us-cert.gov/cas/tips/

U.S. Chamber of Commerce: Internet Security Essentials for Small Business
http://www.uschamber.com/issues/technology/internet-security-essentials-business

USSS: Secret Service Field Office
http://www.secretservice.gov/field_offices.shtml

Wiki: Tiny URLs
http://en.wikipedia.org/wiki/TinyURL

Wiki: Bitly
http://en.wikipedia.org/wiki/Bitly

Wiki: QR Codes
http://en.wikipedia.org/wiki/QRcode

Guides / Templates

AllClear ID: Incident Response Workbook
https://www.allclearid.com/data-breach/data-breach-response-plan

FCC: Small Biz Cyber Planner 2.0
http://www.fcc.gov/cyberplanner

Ready: Business Continuity and Disaster Preparedness Plan
http://www.ready.gov/sites/default/files/documents/files/sampleplan.pdf

SACOG: Continuity of Operations Plan
http://www.sacog.org/coop/

VISA: Business Guide to Data Security
http://usa.visa.com/merchants/risk_management/data_security_demo/popup.html

Scams / Hoaxes / Phishing

Apple: Identifying fraudulent "phishing" email
http://support.apple.com/kb/HT4933

Hoax Slayer: How Nigerian Loan Scams Work
http://www.hoax-slayer.com/nigerian-scams.html#nigerian-scams

Hoax Slayer: Latest Email Hoaxes - Current Internet Scams
http://www.hoax-slayer.com/

IRS: Report Phishing
http://www.irs.gov/uac/Report-Phishing

Microsoft: How to recognize phishing email messages, links, or phone calls
http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx

Snopes: Internet reference for urban legends, folklore, myths, rumors, and misinformation
http://www.snopes.com/

Social Media

American Express: Hey, Small-Business Owner: Maybe Social Media Isn't For You
https://www.openforum.com/articles/hey-small-business-owner-maybe-social-media-isnt-for-you

Facebook: Security Tips
http://www.facebook.com/help/379220725465972/

SBS: Social Media Security Tips for Small Business
http://www.securityforsmallbusiness.com/blog/social-media-security-tips-for-small-business.aspx

Software / Apps

AVG (antivirus)
http://www.avg.com

Chrome Webstore: NotScripts
https://chrome.google.com/webstore/detail/notscripts/odjhifogjcknibkahlpidmdajjpkkcfn?hl=en

Hamachi (Virtual Private Network)
https://secure.logmein.com/products/hamachi/default.aspx

LastPass (password management)
http://www.lastpass.com

Lojack: Lojack for Laptops
http://www.lojack.com/Laptops

NoScript: NoScript Firefox extension
http://noscript.net/

TrueCrypt: Free open-source disk encryption software
http://www.truecrypt.org/

Top Ten Reviews: 2013 Best Internet Security Suites Software Reviews
http://internet-security-suite-review.toptenreviews.com/

Wiki: Pwn2Own
http://en.wikipedia.org/wiki/Pwn2Own

Technical Configurations

Apple: Understanding data protection
http://support.apple.com/kb/HT4175

Microsoft: How to disable the Autorun functionality in Windows
http://support.microsoft.com/kb/967715

NSA: Data Execution Prevention
http://www.nsa.gov/ia/_files/factsheets/I733-TR-043R-2007.pdf

Website / URL Checkers

Comodo: Site Inspector
http://siteinspector.comodo.com/

McAfee: Threat Center
http://www.mcafee.com/us/mcafee-labs/threat-intelligence.aspx

Norton: Safe Web
https://safeweb.norton.com/