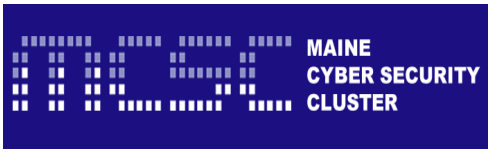
Small Business Cyber Security Guide

Cyber Security Organization
Maine Cyber Security Cluster
University of Southern Maine



News & Alerts

August 13, 2014 - "IRS Repeats Warning about Phone Scams"
http://www.irs.gov/uac/Newsroom/IRS-Repeats-Warning-about-Phone-Scams

> The IRS is still receiving reports from people about this scam and they have identified about "1,100 victims who have lost an estimated $5 million". Characteristics: Scammers use fake names and IRS badge numbers. Scammers may be able to recite the last four digits of a victims Social Security number. Scammers spoof the IRS toll-free number on caller ID to make it appear that its the IRS calling. Scammers sometimes send bogus IRS emails to some victims to support their bogus calls. Victims hear background noise of other calls being conducted to mimic a call site. After threatening victims with jail time or drivers license revocation, scammers hang up and others soon call back pretending to be from the local police or DMV, and the caller ID supports their claim. If you have received correspondence similar to the above, call and report the incident to TIGTA at 1.800.366.4484.

July 31, 2014: - New Backoff Point-of-Sale Malware Alert
https://www.pcicomplianceguide.org/new-backoff-point-of-sale-malware-alert/

US-Cert Synopsis:

> The malware has the potential to impact any point-of-sale (POS) system where the business is utilizing (or has previously utilized) a remote access tool such as Microsofts Remote Desktop, Apple Remote Desktop, Chrome Remote Desktop, Splashtop 2, Pulseway and LogMEIn.
>
> The malware, called Backoff, has been found in at least 3 separate POS data breach investigations
>
> There are multiple variants of the malware and merchants are advised to take the necessary, immediate precautions to prevent exposure or limit the damage of a breach that could already be in progress at their business
>
> POS systems are currently under attack by the Backoff POS malware and its four other variants. This malware gains access through the remote connection that processes credit card payments, installs malware that scrapes the credit card data from RAM (where it is decrypted for processing)in the POS system, it then sends it to the cyber criminal and removes itself from the system. This malware has the potential to cause great harm because even if your system and software is thoroughly up-to-date, anti-virus software still does not detected it. Information security professionals recommend a defense in depth approach to mitigating risk to retail payment systems.

Check out the report from https://www.us-cert.gov/sites/default/files/publications/BackoffPointOfSaleMalware_0.pdf

---

July 13, 2014 - "US Credit Card Fraud Is Spiking Ahead Of EMV Secure Chip Introduction"
http://www.forbes.com/sites/tomgroenfeldt/2014/07/17/us-credit-card-fraud-is-spiking-ahead-of-emv-secure-chip-introduction/

> Industry experts think that by October 2015, when responsibility for card losses on mag stripe cards shifts to merchants, about 70 percent of the US cards in use will have EMV chips, leaving less opportunity for fraud.

July 10, 2014 - "How Microsoft's support lifecycles affect you and your business"
http://www.zdnet.com/how-microsofts-support-lifecycles-affect-you-and-your-business-7000031426/

July 8, 2014 - "Microsoft warns of pending support deadlines for Windows 7, Office 2010 SP1, Windows Server 2003, and more"
http://www.zdnet.com/microsoft-warns-of-pending-support-deadlines-for-windows-7-office-2010-sp1-windows-server-2003-and-more-7000031348/

> Microsoft mainstream support ends January 13, 2015 for several programs, including Windows 7, Windows Server 2008 and 2008 R2, Microsoft Exchange Server 2010, Windows Storage Server 2008, (all versions).
> Some other applications and support expiration dates to be aware of are:
>
> - **Windows Server 2003, ends July 14, 2015.**
> - **Windows 7, Windows Server 2008 and 2008 R2, Windows Storage Server 2008, (all versions) all support ends January 14, 2015.**

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. It gives great tips that are free to implement and apply for almost everyone.

Due to the vast number of topics covered we do not go into the technical details of implementing the suggestions given. Many of these recommendations 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 do an internet search on Google.com or Deeperweb.com.

Please note that all the applications in this guide refer to them with default settings.

Please report any errors, concerns, or suggestions for this guide by email to the student run, Cyber Security Organization for the University of Southern Maine at csousmgmail.com with "GUIDE" in the subject line.

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.

Thanks to Rick Gamache for providing technical insight and suggestions.

Thanks to Kimberly Reali for technical insights and creating a one page tri-fold version.

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.

Update credits:

August 2014: Nicole Kearns, Vice President of CSO and Undergraduate of Technology Management and Kimberly Reali, President of CSO and Undergraduate of Technology Management

Introduction

Few small businesses today can function without technology, and most of it involves the public Internet. The Internet is a great venue for businesses and offers several benefits; yet, it also presents challenges and risks that are often difficult for many small businesses 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 these best practices. Cyber security intrusions are very real and are increasing daily. The number of small businesses becoming victims of cyber crimes has increased. This victimization occurs either through scams, fraud, theft, or other malicious criminal activity, and if you are breached, you will need to be aware of the laws that pertain to your business to help affected consumers protect themselves and to avoid potential law suits.

According to tripwire.com's: *Q1 2014: 176 Million Records Compromised*, "The Business sector accounted for 98.3% of the number of records exposed There were 669 incidents reported during the first three months of 2014 exposing 176 million records."

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. communications systems company called Primary Systems in St. Louis, Missouri. Concrete was robbed of over $100,000 due to a cyber robbery.
- Between November 27 and December 15, 2013, criminals gained unauthorized access to Target's system compromising over 40 million credit and debit card numbers.
- August 2014, 4.5 million patient records were stolen from Community Health Services, Inc. by the Chinese through the Heartbleed vulnerability

Securing the Human

Small businesses make up 99.7% of all businesses in the United States according 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 to learn about and implement 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, insecure network settings, using business machines to access personal websites and social media sites, insecure cellphone use on network, and/or lack of basic security guidelines, policies and awareness training for employees.

The "bad actors" and criminals on the Internet realize that small businesses often do not take many of the basic security steps, making them more vulnerable because there is less rigor associated with the protection, monitoring, and maintenance of their networks, servers, workstations and employees. There are also budget constraints that businesses of all sizes face. Small business owners and operators need to maintain a basic level of cyber defense for the safety of their business, security of their customers and protection of their brand image.

If the courts consider your company neglectful in how the disaster was addressed, there may be legal consequences for your company. Most reasonable people are understanding that there are circumstances that are beyond your control. It is impossible to plan for everything, but by

employing prevention, mitigation, and recovery steps, you can drastically reduce your risk of comprise. Most of this guide was focused on prevention.

Cyber security needs to become a priority. 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 customers suffering financial loss or identity theft and of your business being breached. Beyond taking these defensive steps, small business owners must develop, enforce, and revise their policies, provide training to their employees, and stay informed about relevant threat standards, policies, and procedures.

To stay on top of threats, scams, and exploits in real time see our groupspace with live streams from reputable sources. http://groupspaces.com/CyberSecurityOrg

Small Business Operational Security

This information was found on:
http://www.nsa.gov/public_info/media_center/ia/video/bestpractice/Transcript.html
http://computer-net-working-security.blogspot.com
http://fas.org/irp/nsa/best_practices.pdf

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 Wi-Fi 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 do not know each other.

- **Use separate emails for work and home.**

Using unique username for your home and work email addresses will make it harder for either of your accounts to be targeted and compromised.

- **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.

Secure Your Small Businesses Quick Start

First, start with making a map of your network, take an inventory of the technology your business uses and review the *"14 Key Steps to Better Secure Your Company*" below. Second, build security policies and incident response plans to secure your business, your customers and recover 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 and may go unnoticed for months, or even years.

14 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 process credit cards through a point of sale (POS) system must be connected to a non-wireless dedicated network. Public wi-fi must also be on its own dedicated network. If you process payroll in house, install the payroll system on a separate computer not connected to any public wi-fi, POS system or external or internal networks. All other daily tasks can be performed on its own separate network. If using wireless networking for anything other than public wi-fi, disable the SSID broadcasting on your router so your network can not be found or breached.
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," spoofed or fake sites:
    - 208.67.220.220 and 208.67.222.222 (OpenDNS)
    - 156.154.70.22 and 156.154.71.22 (Comodo DNS)
    - 8.8.8.8 and 8.8.4.4 (Google DNS)
3. If possible, change any default username or passwords on computers, printers, routers, smart phones, or any other devices to something stronger. For more information about passwords view the chapter on passwords in this guide.
    - Do not let your browser remember passwords and try to use a unique password for each account. However, if you must use the same passwords try to make modifications to it such as "goo<favoritepassowrd>" for a google account. Consider using a password manager such as lastpass, which is also available for mobile devices.
4. Keep all operating systems and software up-to-date and use antivirus protection for your system.
    - One of the most popular antivirus software is avast but there are other excellent protection programs. Set software to run daily scans automatically.

- Check your Microsoft Software versions against their new Lifecycle dates to be sure you are still receiving support and security updates.

5. Don't install any software you did not go looking for. Keep your software up to date, and check to see if your software is still supported. Remove or uninstall software you are no longer using.
6. Use Google Chrome or Chromium for an Internet browser. If you must use Internet Explorer or Firefox, keep in mind they are a major targets so you must keep them up to date and configured properly (Internet Explorer 8 is no longer supported.) Also use browser addons to extend and harden its security (ghostery and lastpass).
7. Use BAT, Thunderbird, or Webmail for email applications. If you must use Outlook be sure support has not expired. (Support has ended for Office 2010 Service Pack 1)
8. Before clicking any link check the actual address by hovering the cursor over a link (bottom left in Chrome and Internet Explorer 10 and 11), make sure it looks legitimate.
9. 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 legitimate.
10. If you need remote access to your business network, install a Virtual Private Network (VPN) on all your machines (except POS), and network them using the HAMACHI VPN (FREE) at https://secure.logmein.com/products/hamachi/ which will provide encrypted connections to your own network, and set a limit to the number of users, workstations and/or devices that can log in.
11. If you get a pop-up telling you "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).
12. USB Recommendations:
    - Don't allow autorun.
    - Don't plug in home USBs.
    - Don't share USBs.
13. Maintain a "Clean Desk Policy", which means ensuring that sensitive information is not readily available for viewing at your employees' desk. Ways this can be accomplished is by having a policy where employees must log out of their computers when they are away from the desk, not having a computer monitor facing the doorway, and not leaving paperwork with sensitive information on the desk.
14. Run scans on your computers to see if there are any issues that need to be addressed.

Putting these changes in place can seem challenging or difficult for some small business owners. If you feel you need assistance, don't hesitatet. The cost of a security consultant is far less than the cost of a breach. See the chapter about "Hiring a Security Consultant".

Additional information about the items above can be found in this guide. We have also provided links to resources that can be very useful and we will work on keeping these updated for you.

To learn more about securing your business assets and training employees, see the links below:

NIST Small Business Security Awareness Videos - Free
http://csrc.nist.gov/groups/SMA/sbc/library.html#04

OnGuard Online - Free
http://www.onguardonline.gov/features/feature-0007-featured-info-small-business

For small business videos, tutorials and training, refer to the "Employee and Contractor" chapter for free and affordable training for the workplace.

InfreGard Awareness - $24.95
https://www.infragardawareness.com/
InfraGard, offers online workplace security awareness training as well as a free course for individuals.

PCI Security Awareness Education program"PCI Essentials" - $99.00
https://www.securityinnovation.com/products/pci-training/pci-essentials-awareness-training.html

Cyber security is more than a checklist, and waiting until you've been compromised may be too late for your business. It is a constant effort by employees and business owners to keep defenses strong. Following good cyber security practices will make it harder for anyone to compromise your systems. It is important that you create, maintain, update and enforce employee policies and response plans that are appropriate for your business.

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, along with all your 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 Suites

There are many different antivirus protects available, and below we list the most popular

Kaspersky
http://usa.kaspersky.com/business-security

Avast
http://www.avast.com/business

BullGuard
https://www.bullguard.com/

Panda
http://www.pandasecurity.com/antivirus-for-small-business

ESet
http://www.eset.com/us/business/

F-Secure
http://www2.f-secure.com/en/web/business_global/products

G Data
https://www.gdatasoftware.com/onlineshop/b2b/g-data-smallbusiness-security.html

Note that prices may vary depending on the number of machines you have and what services your business requires. Each product will have its strengths and weaknesses, therefore research will be required before selecting the right protection for your business.

AntiMalware Software

We are researching more information on antimalware software. [cite here] MalwareBytes is the most popular antimarleware software

MalwareBytes
http://www.malwarebytes.org/

Passwords

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

Building a Password

Passwords are an important part of daily Internet use, especially in business settings. Almost every account and computer in a business should be password protected. So how do we make good passwords? Passwords require a bit of careful thought and care.

Before talking about what makes a good password, below are some tips on how to care for your passwords.

- Use different passwords for different accounts and email addresses.
- Change your passwords often.
- Say NO if asked to "remember" your password and use lastpass instead.
- Don't store your passwords on your computer or on paper near computers.
- If you must write a password down, lock it away! (It is 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.

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 that criminals are very resourceful and are creating new tools to crack your password every day.

You need to stay current on the latest advice on creating strong passwords. The following are suggestions to get you started.

- **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? Try lastpass, it encrypts passwords and remembers them for you.

- 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.
- if you must use the same password:

  - Append a website's first 3 letters in front - Google would be "goo<favouritepassword>", Facebook would be "fac<favoritepassword>".
  - Append the word with digits in between the letters, like "fourscore" to "f1o1u1r1s1c1o1r1e" or "f1o2u3r4s5c6o7r8e" using a different sequence for each account.

- Use words or sentences that are easy to remember, but don't use all of the letters. Use every other letter.
- Use passwords that type out a shape on the keyboard that you will remember, like a \might start at a digit in the top row and letters going down at an angle, then / would be with the caps lock on, and starting with another digit {character] then turn caps on and do the same at the opposite angle and numbers or letters in the middle.
- Hold the shift key down for parts of the password

Avoiding Scams, Frauds, 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 fraudulent emails.

Spelling and Bad Grammar

When a company sends out a mass email usually the email is edited for spelling, grammar, and other mistakes. Mispelled words or incomplete sentences is almost always a sign that it is not legitamate.

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." Criminals often use a sense of urgency to pressure their victims to act quickly without thinking through what they are being asked to do.

Beware of Links in Your 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 be unaware of it. Check the link by hovering over the link and the actual URL will be in the lower left or your Chrome browser. Links could send you to a .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, 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 it is too good to be true, it probably is.

Is this legitimate?

Scams can be avoided by asking the simple question, "Is this legitimate?" Most scams involve a bad person trying to get you to do their bidding. A good way to check for legitimacy is to contact the company directly. 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 the number or contact provided on the website.

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.

Internet Crime Complaint Center
http://www.ic3.gov/default.aspx

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

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

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. The content below is from http://fas.org/irp/nsa/best_practices.pdf

http://www.nsa.gov/public_info/media_center/ia/video/bestpractice/Transcript.html

Network Security Fundamentals

Connect to the ISP provided 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.

- **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 or 8.8.4.4 (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.

- **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."

- **Separate High Value Devices to a 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 only accounting transactions and only accounting transactions.

Depending on the size of your network you may want to use three routers in a "Y" configuration. Keep in mind that the middle router connecting to the Internet should be faster than the other two, this will reduce a bottleneck effect.

Wireless Security Fundamentals

"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 addresses for all authorized hosts must be configured on the wireless access point."

There are two ways for this which are blacklisting and whitelisting. Blacklisting involves creating a list of websites that employees cannot access on the work network, while whitelisting does the opposite restricting employees to accessing only approved websites.

- **Reduce wireless Range**

"Limiting the transmit power of the wireless access point will reduce the area of operation or usable signal strength, of the wireless network. This capability curtails the home wireless network from extending beyond the borders of a home for example, into a parking lot or adjacent buildings."

- **Turn off SSID broadcast**

"SSID cloaking is a means to hide 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."

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. Microsoft is ending support for many of their older products, so check your Microsoft software versions against Microsoft's new Lifecycle database to be sure you are still receiving feature and security updates.

- **Avoid Microsoft Internet Explorer**

Internet Explorer is a major target and using older versions of IEincreases your risk. Remember that Microsoft no longer provides support for IE 8, which means vulnerabilities are no longer addressed making it easier for criminals to compromise your this version.

If a person wants to write malicious code that will affect the most people, they will write it for an out of date browser.

Sometimes it is necessary to use Internet Explorer for things like POS systems that's ok, but use Internet Explorer for website you know to be safe. If you are going to a site you have never heard of or been to before, use Google Chrome with NoScript, or Firefox with NoScript.

- **Google Chrome is currently the best choice**

The Pwn2Own competition Pwn2Own has tested the vulnerabilities of web browsers like Chrome, Firefox, and Internet Explorer. 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. One change you should make though, is to enable secure certificates because Chrome has this disabled by default. Firefox and IE are enabled by default.

- **IOS Browsing**

Be sure you using at least iOS Safari 6.1.6 (Safari iOS 7 has a "Fraud Warning" service built into it).

- **Login 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 give the user a better experience, some may not. Malicious scripts are used to exploit your system while you visit a malicious website. NoScript for Firefox is an addon 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 whether 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 legitimate?" or, "Does this link go where it says it goes?" To see where the link really goes, hover your cursor over the link and in the lower left corner of your browser destination address.

A malicious link may have incorrect spelling compared to the real site. Sometimes it's a zero replacing "o" or a "1" replacing a lowercase "L" as in the case of bannk0famerica.com or g00g1e.com. 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 can be found at ShortURL here http://www.shorturl.com/

Three examples of URL Shorteners are:

Bitly
https://bitly.com

TinyURL
http://tinyurl.com

Google URL Shortener
https://goo.gl/

A good explanation of QR Codes can be found at https://www.the-qrcode-generator.com/.

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 Web Inspector
http://siteinspector.comodo.com/

Site Advisor
https://www.siteadvisor.com/

Web of Trust
https://www.mywot.com/

E-Mail Security Fundamentals

E-Mail is a fundamental part of nearly all small businesses and it is one of the most used techniques by hackers. It is a form of social engineering because they often play on your emotions after a Natural disaster and even during holidays. Small businesses are easy targets because email addresses for businesses can be found right on their website.

Currently, a new type of spear phishing has made #1 on Proofpoint's "Top 10 list of Advanced Threats Impacting Business Today", media spear phishing. This attack uses twitter to generate a link from a legitimate looking business, but it redirects you to an infected site instead.

- **When posting company contact information on a website, use titles or positions rather than employee names and if possible, setup a separate email account for website emails.**
- **If possible, use a webform with captcha for information requests.**
- **Don't send or accept sensitive information via email unless you are using PGP encryption keys**

The Internet Crime Complaint Center (IC3) provides a subscription for the latest scam alerts.

> IC3 SCAM ALERT: JUNE 27, 2014Business E-mail CompromiseBusiness E-mail Compromise was formerly known as the "man-in-the-email scam." These emails are usually sent to upper management asking for payment of an invoice to be made by wire transfer and the sender's email is slightly spoofed to look very similar to a legitimate vendor you may use. It isn't until a companies internal fraud detection alerts victims or upper management discusses the transfer with other management personnel. The average dollar loss is $55,000 per victim.

Anti-Phishing Working Group (APWG) 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 ten days before being discovered.

According to the FCC, 60% of all emails received by companies, contain spam, phishing attempts, or otherwise unsolicited email. A securely configured 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 real-time alerts about email scams, subscribe to the FBI Internet Crime Complaint Center (IC3)

Below are some tips from the FCC's FCC's "How to Protect Yourself Online" and the NSA

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

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 is 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, this keeps spammers from knowing 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 and unique username for each email addresses. This will make it more difficult for someone targeting your work account to also target 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)

The information below was found on:

http://fas.org/irp/nsa/best_practices.pdf
http://www.nsa.gov/public_info/media_center/ia/video/bestpractice/Transcript.html

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 crucial to properly secure these devices. Below are several suggestions for improved server and workstation security.

Microsoft Lifecycle of OS and Servers:

Microsoft mainstream support ends January 13, 2015 for several programs, including: Windows 7, Windows Server 2008 and 2008 R2, Microsoft Exchange Server 2010, Windows Storage Server 2008, (all versions).

Some other applications and support expiration dates to be aware of are:

- Windows Server 2003, ends July 14, 2015
- Windows 7, Windows Server 2008 and 2008 R2, Windows Storage Server 2008, (all versions) all support ends January 14, 2020

Windows Host OS

- **Migrate to a Modern OS Systems and 64 bit Hardware Platform.**

Windows 8.1, 7, and Vista are the only Microsoft workstation OS versions still available with security support. But, Vista support will end on April 11, 2017 and Windows 7 mainstream support will end January 13, 2015, while security support ends January 14, 2020 Note: Windows XP was discontinued as of April 8, 2014.

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 and blocks malware from being able to run in certain areas of your computer system.

- **Update Automatically.**

Windows should be set to update automatically, and although you can also choose to download but ask to install can be helpful too, we don't recommend it because many people forget or don't find the time to install it.

- **Always turn workstations off when not in use.**

This will help prevent RAM scraping attacks by clearing data stored in RAM.

- **Install Security Suite**

Examples of security suites include Microsoft Security Essentials, Bitdefender, Kaspersky, Panda, AVG, Norton, F-Secure, Avast, ESET, G Data Furthermore, and BullGuard.

Note: Microsoft has also stopped providing Microsoft Security Essentials for download on Windows XP.

- **Limit Use of the Administrator Account.**
- **Use a Web Browser with Sandboxing.**
- **Update to a PDF Reader with Sandboxing Capabilities.**

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 2013 or Later**

If using Microsoft Office products for email word processing, spreadsheets, presentations, or database apllications, upgrade to Office 2013 or later.

- **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)**

To help prevent data disclosure in the event that a laptop is lost or stolen. Use of FDE programs can prevent your data from being exposed.

If you are running Windows Vista or Windows 7 (Ultimate, Pro, or Enterprise editions) or Windows Server 2008 and later, you already have Bitlocker installed for use.

For Mac OSX, FileVault2 works very well.

- **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 number of 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.

- **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.

Apple Host OS

> June 2014: "Apple's iPad and iPhone are generally considered to be safe and secure devices to use, however, a security flaw was discovered in late February 2014 that means that an attacker could intercept your data if you are using an unprotected hotspot, perhaps in Starbucks or an internet cafe". -Macworld

- **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 6, follow the instructions at: http://support.apple.com/kb/HT4175.

- **Implement FileVault2 on Mac OS Laptops**

In the event that a Mac laptop is lost or stolen, FileVault2 (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. But, be aware that this application has also been used in the Oleg Pliss in late May 2014.

Linux/Unix OS/Android 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 uFse**

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 Tsubstantial 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, i.e.: red flag.

- **Install Security Software for Linux**

Though not required for safety and security of the Android device, the installation of security software for linux devices devices is another added layer of security. A few examples of security software available for linux are the following: Kaspersky, Avast, 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.

Traveling with Personal Mobile Devices

Many establishments, such as coffee shops, hotels, or airports, 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 such as laptops, smart phones, and tablets, should utilize the cellular network, like 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 setup tunnels to a trusted virtual private network, or 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. Narrator: Whenever possible, maintain physical control over mobile devices while traveling. All portable devices are subject to physical attack given access and sufficient time. If a laptop must be left behind in a hotel room, the laptop should be powered down and have Full Disk Encryption enabled.

Social Networking

Phishing attacks are becoming more popular on social media sites and employee education alone is not enough. Enforceable policies need to be maintained, updated and enforced. Statistics show that 87 percent of small businesses do not have a formal written "Internet Use Policy" for employees and 70 percent do not have policies for employee social media use, according to staysafeonline.

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**

Unless you trust the source, avoid including links to other pages on your page. You do not want your business to be associated with a potentially malicious source, and your business has a responsibility to take steps to reasonably ensure the safety of your visitors. You do not want to allow spammers to advertise themselves on your page: never allow physical links on your form fields.

- **Use a different email**

Email scams are one of the most popular forms of hacking and gathering personal information. If one of your accounts is compromised, it should not affect the other unless you are using the same password, which is something that should never be reused.

- **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 does not 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.

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

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

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 that can be connected to an individual person. For example, a Social Security, or driver's license 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. Driver license numbers.
4. Personally identifiable information pertaining to individuals (employees, applicants, parental, and 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. 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 to assist law enforcement to recover the laptop if it is stolen.

- **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.

- **Your employees are your best defense.**

Small businesses are usually small for everyone to know each other; therefore, an employee badge system may not be needed. Your employees need to be taught about social engineering and to be alert for unauthorized personnel. For example, if a person dressed as a UPS carrier arrives during a time when the 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 defense. Encourage people to question whether a person should be here and wonder if this really the boss on the phone.

Payment Cards and Point of Sale Systems

Businesses that store, process and transmit credit card data must comply with PCI DSS requirements to ensure credit card information is being transmitted securely by using end-to-end encryption. This means the data is encrypted when received, while stored and when transmitted to merchants. These businesses are required to comply with new PCI DSS 3.0 requirements by the **December 31, 2014** deadline.

- **Is your business ready?**

Although, the "Verizon 2014 PCI Compliance Report" reports that 77% of managers surveyed believed they were currently PCI compliant, and NTT Com Security survey reported that only 10% of those companies passed their baseline assessments while 70% of them were not even aware of the December 31 deadline. Dont be surprised, be prepared!

- **Are you sure your business is ready?**

POS systems are currently under attack by the "Backoff" POS malware and its four other variants. This malware gains access through the remote connection that processes credit card payments, installs malware that scrapes the credit card data from RAM (where it is decrypted for processing)in the POS system, it then sends it to the cyber criminal and removes itself from the system. This malware has the potential to cause great harm because even if your system and software is thoroughly up-to-date, anti-virus software still does not detected it.

- **How important are these requirements?**

Many small businesses believe they are not a target because they dont have valuable assets, however to cyber criminals that means less protection against attacks and breaches and easier access. In fact, Symantecs 2013 survey reports that 30% of all breaches were against small business and about 60% of them had to close within six months after. Verizon's survey further revealed POS intrusions, web app attacks, cyber espionage and card skimmers as top concerns for 2014 and coined 2013 as the "year of the retailer breach". These new PCI Compliance requirements could not have come at a better time. Although, small businesses may see these changes and painstaking work, it should be considered sustainable security that will save your business and your customers valuable time and money.

- **What's next?**

There is a new technology that has become popular in Europe and Canada and now it will become the standard in the US in 2015. All small businesses should be aware of and prepare for new VISA, Mastercard and American Express Counterfeit Liability Shift Policies taking effect on October 1, 2015 (effective October 1, 2017 for Automated Fuel Dispensers). You have probably heard of the "smartcard" or EMV chip cards, well now 44% of all cards are EMV chip cards and 74% of all terminals are EMV chip-capable and that number is expected to reach 100 million by the end of 2014. The credit card companies are adopting a new policy that will penalize consumers and businesses who are breached and do not have this technology in use. This sounds like bad news, but the effect of this new technology had drastically reduced card skimming in Canada from CAD$142m in 2009 to CAD$38.5m in 2012. This will be the strongest protection you and your customers can get and will protect your business from costly losses. Learn more at Fox Business News.

There are 12 key items on the new PCI DSS 3.0 Requirement. Most of them address good information security practices while others emphasis employee training, policies and documentation of networks.

Below is a quick reference of key requirements:

- the first section now requires business to maintain a current diagram to identify all networks, devices and system components between the payment system and other networks, including wireless.
- Install, monitor and maintain a firewall configured for security card processing
- Do not use vendor defaults for passwords and other security measures.
- Encrypt all cardholder information being stored prior to transmitting batch, then be sure all information has been removed.
- Create, maintain, update and enforce policies and training for all employees (ex. cyber-response plan, access policy, acceptable use policy, etc)
- Be sure all cardholder data is encrypted while in transit over the networks.
- Be sure antivirus and malware software is installed and updated daily.
- Assign all users unique passwords that conform to policies and monitor their
- Enforce frequent monitoring and testing of security and processes.

- **How can you prepare employees?**

There are several on-line training programs available that fit a small business budget and can be completed on-line. Below are very reliable recommendations.

NIST Small Business Security Awareness videos - Free

OnGaurd Online for small business videos, tutorials and affordable training for the workplace. - Free

InfraGard Awareness Security Awareness Course" by InfraGard, offers online workplace security awareness training as well as a free course for individuals. -$24.95

PCI Security Awareness Education program"PCI Essentials" - $99.00.

PCI Standards:

The PCI Standards Council maintains a list of PTS approved hardware, PA-DSS approved software and qualified PCI Compliant Auditors who can help access your environment for PCI-DSS 3.0 Compliance.

Self Assessment Questionaire (SAQ v3.0)

Therefore it is important that you become aware of these requirements and if you need help meeting requirements, consult a Certified QSA or Security consultant. For help locating a qualified professional, check the "Employee and Contractor" chapter of this guide.

Remember: Compliance does not mean security, therefore we have listed other important measures you should take.

- Remove all unnecessary applications from payment processing systems (IE, browsers, games, etc).

- Segregate the POS network from all other networks (if there are no other devices in this network, complying with the first requirement become much easier.)
- Stay informed about industry news at the PCI Security Standards Council and subscribe to USCert alerts
- Be sure to turn all systems off when not being used and at least once a day to clear memory.
- Check your payment system software and hardware against PCI Security Approved lists

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.
- Never use vendor default login for POS software.
- Use strong, unique passwords and change them frequently.
- Use up-to-date firewall and anti-virus technologies.

Make sure your POS system is using a securely updated system for remote access and eliminate remote access when you don't need it so criminals cannot infiltrate your system from the Internet.

The 2 main goals for business today is not just PCI Compliance but advancing good information security practices also and the "PCI Security Standards Council" is the best source of information to help small business meet these goals.

USCERT Alerts released in 2014:

Backoff Point-of-Sale Malware - July 31, 2014 (revised August 18, 2014)

Malware Targeting Point of Sale Systems - January 02, 2014

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

Helpful links

PCI Resources:

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

Passwords for Payments
https://www.pcisecuritystandards.org/smb/passwords_for_payments.html The Passwords

for Payments (P4P) initiative will educate small businesses on how to use strong passwords on point-of-sale devices and computers to reduce their chances of being breached.

PCI Small Business Resource
https://www.pcisecuritystandards.org/smb/

Protecting Cardholder Data Is Good For Your Business - video
https://www.pcisecuritystandards.org/smb/video.php?v=KWDbcxpU2y8

- **EMV Resources**

To learn more about **Europay Mastercard VISA**
http://www.emv-connection.com EMV Connections

For more information about security awareness for employees, check the "Employee and Contractor" chapter of this guide.

Some of this information was obtained from Business Wire and DHS Build Security In

Incident Response and Disaster Recovery

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 measuresif 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. Children's' 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

As soon as you discovered or even suspect a breach, you should perform the following steps:

1. 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.

2. Leave the infected machine running

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

3. Call your Security Consultant and/or law enforcement

   Usually breaches will fall under Secret Service jurisdiction, start with local law enforcement.

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

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

4. Check Reporting Requirements for your State. Each state has different reporting requirements depending on the situation. The National Conference of State Legislature (NCSL) has links to the state security breach notification laws.

5. Inform affected parties

   Be sure to consult with investigating authorities prior to notifying effecting parties. You may be required to hold off on notification to avoid jeopardizing the investigation.

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

6. Consult with your Attorney You should have an attorney that has experience in Privacy and Data Security law and is aware of current PCI Requirements.

7. 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 hard drive 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.

8. 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.

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.

Introduction to Disaster Recovery

Disaster recovery is about preparation, and knowing what to do when an incident becomes a disaster. A disaster is when your business operations are disrupted longer than your maximum tolerable downtime (MTD), or the period when you can afford to lose a process before your business is in danger of shutting down. Unfortunately, disaster recovery is an area that is overlooked because disasters are a rare occurrence. There is a perception that time and money could be spent elsewhere, and keeping the plan current is an ongoing investment. However, the investment is in the durability of your business.

Even if you take proper preparations, there is always a chance that something will be overlooked or missed even with proper preparation and your business needs to be flexible enough to address the unexpected. For example, over 1,000 businesses have been affected by the backoff malware even with an up-to-date system. It was only in August 2014 that antivirus vendors started being able to detect the latest variant of the malware. This is why you need to plan for different types of compromise. Large scale geographic disasters such as earthquakes, tornadoes, ice storm, hurricanes can not only destroy your equipment and resulting in data loss, but can also result in lengthy downtime and costly recovery.

More information on developing a disaster recovery plan will be addressed in our upcoming disaster recovery guide. Below we list what we see as the key disaster recovery principles.

Key Disaster Recovery Principles

A disaster recovery plan is not only important for your business's resiliency, but an obligation as well legally, ethically, and the sake of your business. Every second your computer systems are offline is money and time lost, and, on top of money lost from downtime, you need to be able to access your businesses information such as employee payroll, client billing and contacts, taxes, and supplier contact.

The main goal of disaster recovery is business continuity, where your business is on life support until you can restore normal operations.

- **After disaster happens is too late**

Successful disaster recovery is all about planning and prioritization. Without a recovery plan, your employees may not to get your systems back online in a timely matter. Your customers may turn to your competition for services if they are unable to reach your business. Downtime is synonymous to loss of revenue.

The basic steps of disaster recover are:

1. Select your incidence response and disaster recovery teams and planning committee.
2. Risk Assessment.
3. Evaluate and record your resources and assets.
4. Determine the maximum tolerable downtime and recovery point objectives.
5. List of contacts of who needs to be involved.
6. Review the plan.
7. Test the plan.
8. Revise plan.

Your employees may not know what needs to be prioritize without a documented plan in place. This leaves room for mistakes that can make your business further vulnerable to liability. If your business can demonstrate that there were procedures in place and thought was put into the plan, the courts will be more understanding.

Through mapping out your resources to your business process, your employees will better understand what they need to prioritize to help bring your computer systems back online.

- **Backup your data in more than one geographic area**

If your data is only in one physical place, it is as good as not existing at all when a disaster takes down your network. You do not have just the threats from outside of your network, but there are threats from the physical realm as well. It is not only the electronic dangers you need to be concerned about, but there are dangers that exist in the physical realm as well. There are dangers that exist from both humans and the environment. Humans can sabotage your equipment and the environment can cause large scale damage in a short amount of time.

- **Get employee buy-in**

Your employees are your most important asset when your business needs to recover from a disaster. If they do not understand the plan or why certain preventative procedures and policies are necessary which can lead them to not take them seriously until it is too late.

The best way to gain employee buy-in is for your employees to see that leadership is taking disaster recovery seriously as well. Running an awareness campaign and showing active support for your security policies, will help foster a sense of support. It will show that your policies are not meant to be a hindrance to a job, because there is a legitimate reason why they are in place.

- **Test and review your plan**

Your disaster recovery plan needs to be a living breathing document that can adapt as your business evolves and circumstances change. You need to test, review, and update your plan on an quarterly bases. An outdated plan is as good as no plan at all, because there are new and evolving threats introduced. Governments will introduce new legislation that may call for a more comprehensive plan.

Creating a disaster recovery plan is a comprehensive project, but there are templates available to ease the process of developing the plan. The specifics can only be determine by your business, but there may be best practices that you are expected to follow for your industry.

Helpful Links

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

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

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

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

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

Small Business Resources

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

State of Maine Cyber Resources

Maine AGl
http://www.maine.gov/ag/consumer/identity_theft/index.shtm : Privacy, Identity Theft and Data Security Breaches

Cyber Intel Sources

News: Threatpost
http://threatpost.com/
Trend Micro Threat Encyclopedia
http://about-threats.trendmicro.com/us/threatencyclopedia#malware
News: Internet Storm
https://isc.sans.edu/ **McAfee: Threat Center**
http://www.mcafee.com/us/mcafee-labs/threat-intelligence.aspx

Contractors / Employees

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://www209.americanexpress.com/merchant/services/en_US/data-security

MasterCard: Educational Webinar Series
http://www.mastercard.us/small-business/resources/index.html

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

Disasters / Events / Breaches

NCSL: National Security Breach Notification Laws
http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

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

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

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

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 Cyber Security 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

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

Tiny URLs
http://tinyurl.com/

Bitly
https://bitly.com/

QR Codes
https://www.the-qrcode-generator.com/

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/download/merchants/data-security-tips-for-small-business.pdf

Scams / Hoaxes / Phishing

OnGuard Online: Identifying fraudulent "phishing"
http://www.onguardonline.gov/articles/0003-phishing

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

IC3: Scam Alerts
http://www.ic3.gov/default.aspx

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

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

Social Media

US-CERT: Using Social Networking Services : Using Social Networking Services
https://www.us-cert.gov/sites/default/files/publications/safe_social_networking.pdf

Software / Apps

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

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

LastPass (password management)
https://lastpass.com

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

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

Site: Pwn2Own
http://www.pwn2own.com/

Technical Configurations

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

McAfee: Site Advisor
https://www.siteadvisor.com/

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

Building Your Small Business Cyber Security Plan

Federal Communications Commission: Online Form
http://www.fcc.gov/cyberforsmallbiz

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/ r

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 2.0
https://www.uschamber.com/issue-brief/internet-security-essentials-business-20

PCI Compliance
https://www.pcisecuritystandards.org