Small Business Security

By:

Brian Little

Lewis University

MSIS Technical Capstone

68-590K

Abstract

This paper provides an easy to implement primer for small business security. The goal is to show small businesses how to keep their data secure by presenting the material in a way that can be understood by anyone, regardless of their technical background. This paper breaks down current research on small business security into the following topics: passwords, internet and email use, computer security, data security, and network security. Current information on these topics is generally given in a brief description, which does not allow a small business to immediately make changes to their security. The security topics are broken down into chapters for easy reference and explanations are presented in an easy to read fashion. The paper references topics that have been known for several years, yet these topics are still issues for today's small businesses. The topics that are covered should be considered as the baseline for any small business. Future research can elaborate on these introductory security suggestions by offering more advanced options for small businesses.

Table of Contents

Table of Figures

Introduction

Literature Review

Numerous articles provide recommendations to increase security in small businesses. Certain recommendations, such as using secure passwords, securing internet and email, general computer security, data security and network security seem to be recurring [1, 2, 3, 4, 5, 6]. Data is a company's most important asset, whether it's customer information, financial information, or even intellectual property [4]. This data needs to be protected using multiple layers of security [5, 6].

Current information on passwords suggests changing default passwords that are set by the manufacturer, changing passwords frequently, using different passwords for different accounts, and how to make a strong password [1, 2, 5, 6].

Secure web browsing, limiting sites employees can access, limiting download capabilities, and manually typing in internet addresses are important suggestions [2, 5]. Secure email practice deals with taking care in clicking on links in emails and downloading attachments [2]. Viruses and malware can be transmitted via email and employees need to have a solid understanding on acceptable email use, otherwise malicious software may find its way into the business [2].

Computer security is a big priority for small businesses. Keeping software and operating systems patched and up to date is extremely important [5]. Without these updates, software and operating systems may be vulnerable to attacks. Creating separate user accounts for each user and limiting data that users can access are important. Only certain users (trusted IT staff and key personnel) should have administrative privileges [1]. Software installation should be done by

administrators and not left up to the individual user. Anti-virus and anti-malware programs will help fight off malicious software intrusions on individual computers [4, 5, 6]. A software firewall on each system will help supplement hardware firewalls and some operating systems come with the firewall as part of the operating system [2]. People that use their cell phones (whether personal or company issued) for business use need to be careful. Mobile security consists of password protecting the device, encrypting data and installing security applications [1].

Data security must be a priority for small businesses; otherwise a simple data breach could have their customers lose trust in them. Businesses can't run without a solid customer base. Limiting access to confidential or sensitive information is very important [5]. Each user should be restricted on the amount of data they can access. Another security feature for keeping data safe is by using encryption [6]. Making regular backups of important business data is vital [4, 6]. If a business is attacked, and their data is compromised, damaged or destroyed, then a backup will help get the business back up and running.

Network security consists of protecting the company's network from intrusions and other network based attacks. This can be done by using hardware firewalls to restrict network traffic, securing the Wi-Fi to keep unwelcome guests off of the network, changing default passwords, using WPA2 encryption, not broadcasting the SSID (service set identification), disabling the Wi-Fi protected Setup (WPS), creating a guest network, and disallowing admin access from the wireless network [3]. Small businesses should have a hardware firewall installed between their internal networks and the internet [2]. WPA2 encryption uses stronger encryption that is more secure than WPA and WEP encryption [3].

One of the weakest points in a company's security is their employees. It's important to train and educate employees on security expectations of the business [4, 5, 6]. Administrators can utilize recommendations that are currently available, as well as resources found in this paper to help improve employee involvement in security.

Though some of these topics may seem elementary, numerous articles [1, 2, 3, 4, 5, 6] list these topics as the top security recommendations for small businesses. This paper will provide a security template for small businesses to follow. Current information provides only basic suggestions in a few sentences or less. The paper will present the most common security issues small businesses face and provide solutions to these problems. The chapters are broken down into Passwords, Secure Web Browsing and Email, Computer Security, Data Security and Network Security.

Chapter Overviews

The first chapter covers passwords. Passwords are always a topic of conversation, yet we still hear about breaches involving insecure passwords. Keeping unauthorized individuals out of computers and networks is a key point in small business security. Insecure, default, and weak passwords will be discussed, along with a solution on how to create strong passwords. Passwords managers and two factor authentication will also be covered.

The second chapter covers secure web browsing and secure email. Secure web browsing topics include updating web browsers, disabling risky browser features, information on cookies and additional tools that may help employees practice safe web browsing. Secure email topics include spam, phishing, and alternative email software.

The third chapter covers computer security. Computer security focuses on the security of the computer that the employee(s) is using. User accounts, software, software updates, software firewalls, mobile security and endpoint security will be discussed.

The fourth chapter covers data security. Using encryption in small business will be discussed, including secure internet connections, encrypting cloud storage, encrypting email, and encrypting common business documents. Also backing data up locally and in the cloud are explained, as well as companies that provide online data backup services.

The final content chapter covers network security. Basic network security is discussed, including routers, changing default usernames and passwords, using encryption, using a complex passphrase, the SSID and WPS features on routers, firewalls, virtual private networks, unified threat management, and managed security service providers.

The current research for small business security deals with security topics that fit into one of the above categories. Detailed explanations will be given in each chapter that will allow people with varying skill levels to immediately begin implementing features that will help increase their small businesses' security.

Chapter 1: Passwords

Introduction

Passwords are an extremely important feature to keep unauthorized individuals out of computers and networks. They can be used to protect access to a computer, email, online accounts, and networks. This form of authentication is common; however it is sometimes the only barrier between a user and confidential or private information [7]. Using no password, default passwords, and insecure passwords sets a business up to be compromised. Worms and viruses are being designed to exploit systems by guessing weak passwords [7]. A strong password will help prevent hackers and malicious software from gaining access to computers, accounts and networks. Although it's usually recommended that you change your password regularly, it may be better not to participate in this practice [8,9]. A password manager can be a very helpful tool in creating strong passwords. Two factor authentication should also be used if it is available [8,10, 11].

Insecure Passwords

Using no password, default passwords, and weak passwords create vulnerabilities for businesses. If hardware or software is shipped without using a password, then one should be created during the first use of the product. Default passwords are well known by many [12, 13] and also need to be changed immediately. Weak passwords are those they can be easily "guessed" or compromised through different types of attacks, such as brute force.

Default Passwords

When a business buys hardware or software, a username and password are shipped with them. Vendors will use identical passwords for their products, which are often simple and

publicly available [12]. These passwords are used for the initial testing, installation and configuration operations. Vendors recommend changing the default password prior to using the product [12]. Several websites list various default usernames and passwords for a variety of vendors. One site [13] claims to have 2000 passwords for 488 vendors. These include popular vendors such as Cisco, Netgear, LinkSys, Microsoft, Linux, Apple and Oracle. Any business that is using products from well known vendors should look at these websites and immediately change their usernames and passwords.

Weak Passwords

Weak passwords create vulnerabilities for a business. If an unauthorized user can break a bad password, then they will have access to an unauthorized area or information. When creating a password, you do not use the following criteria [10, 14]:

- Information about the business – Employee names and personal information, business name, addresses, phone numbers, or the network name itself ("Business" shouldn't be the password for "Business Network")
- Easily guessed passwords: Password, user, admin, letmein, temp
- Dictionary words
- Adjacent keyboard combinations, such as: "123456", "qwerty", "asdfghjkl;"
- Don't use the same password for different accounts
- Don't let employees store their passwords in a plain text file on their computer

Hackers can create their own password cracking dictionaries by using business information, including employee names or general information about the business. Do not use any combination of address, phone number or business name when choosing a password. Publicly

available information about the business will help hackers create dictionaries specific to individual businesses. Dictionary words are poor choices for passwords, due to numerous dictionaries being available to hackers. Also, hackers understand that people are using common suffixes such as "1", "4u,", "69", "abc", "!" to add to their passwords in an attempt to make them stronger [10]. Hackers are able to compile any type of dictionary you can imagine. There are even dictionaries that check for various capitalizations and common substitutions such as "$"for "s", "@" for "a", and "0" for "o" [10]. Password cracking is evolving to accommodate the recommendations that are in place to create strong passwords. Even passwords that use a combination of words are no longer safe [10]. Employees should use different passwords for different logins they have. If a password is cracked, this will help prevent an attacker from gaining access to all of the employees and the businesses' resources.

Secure Passwords

Secure passwords use a combination of words, numbers, symbols, upper-case and lower-case letters [14]. Brute force attacks, which use dictionaries, can run through many passwords in a short amount of time. Generally, the shorter the password, the less time it will take for it to be cracked. Powerful cracking tools are able to test tens of millions of password combinations per second [14]. Websites recommend using at least 8 characters for a password, but using more characters will make the password harder to crack.

Using characters from a sentence can make a good password. For example, using the first letter from each word of the last sentence would make: "Ucfascmagp". Use a website [15] to test the security of this password. This particular password is estimated to be cracked in approximately one year using a desktop PC. Adding the number "1" to the end of the password ("Ucfascmagp1") increases the anticipated cracking time to 412 years. Now, let's make this

password more secure by adding symbols and changing some of the cases of the letters. Our new password looks like this: UcFa!scMag&p1. Anticipated time to crack this password with a desktop PC? As shown in Figure 1, approximately 26 million years!

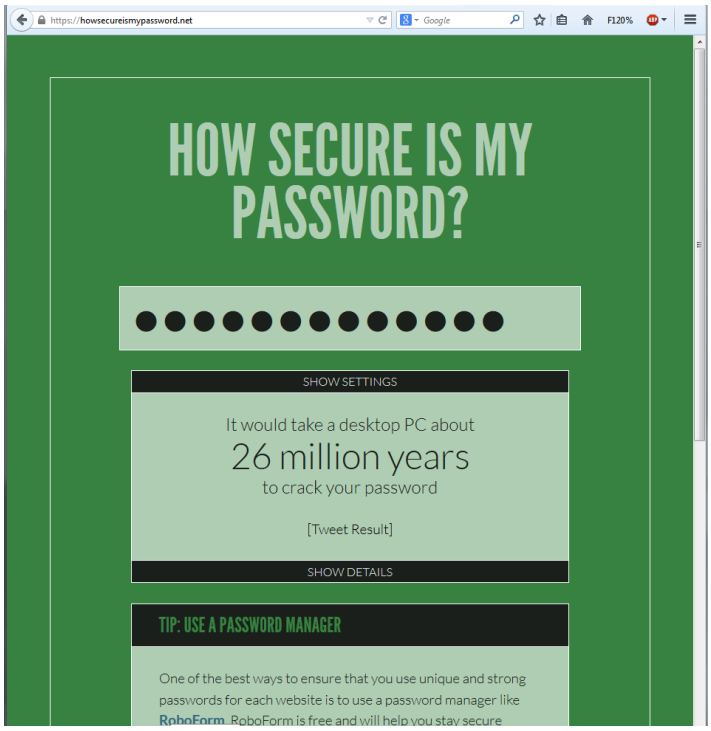


Figure 1. Secure password example [15]

That's a significantly stronger password than what we started with and all we added were two capital letters, two symbols, and one number. Do not use the chorus of a popular song, the title of a popular book, or a common phrase. The goal is to use a personally memorable sentence with some personally memorable tricks [10]. It is acceptable to write these passwords down, as long as you secure the piece of paper that the password is written on and never leave it in plain sight [14].

Password Managers

An alternative to user created passwords is a password manager. The user will have to create a strong master password, such as the one above, and once entered, the user will have access to the program. The program can randomly generate strong passwords for a variety of different logins. The user only needs to remember the master password to get into the program [14]. Some programs support cut and paste, which makes it easier for the user [10]. This feature can also prevent key loggers from capturing user typed passwords.

Two Factor Authentication

Another feature that can help authenticate a user is two factor authentication. Single factor authentication is entering a username and password. Two factor authentication requires the user to have two out of the following three:

- Something you know (Personal Identification Number (PIN), password, or a pattern)
- Something you have (ATM card, phone, fob)
- Something you are (biometric – fingerprint or voice print) [11].

Although two factor authentication can be bypassed by hackers using account recovery, it will add an extra layer of security for your accounts [11].

When To Change Passwords

A topic to consider when having users create strong passwords is how often they should change them. Changing them regularly may result in users picking weaker passwords or reusing old passwords [8,9]. A password manager will help mitigate this problem. A business will want to change passwords if the business itself has been compromised, any sites they use have been compromised, an unauthorized user accesses employees' passwords [8,9]. If a business chooses

to use a password manager, then passwords can be changed more frequently. If you are relying on your employees to create strong passwords themselves, then consider spreading out the time in between changing them.

Summary

Passwords are just one of a small business' defenses in keeping unauthorized users and software out of computers and networks. Changing default usernames and passwords should be done as soon as the new software and hardware connects to the businesses' network. Weak passwords are inviting attackers to break in, whereas strong passwords are at a minimum delaying the entry of an intruder. Use a collection of letters from a sentence, add numbers, symbols and change some letters to uppercase and some letters to lowercase to the collection of letters to make a strong password. The longer the password, the longer it will take to crack. A password manager is a good tool to help users create strong passwords. Two factor authentication should be enabled when available and will add an extra layer of security. Depending on which method a small business uses to create passwords (user, password manager), a policy can be developed on how often passwords should be changed. The focus should be on creating strong passwords, not how often it should be changed.

Chapter 2: Web Browsing and Secure Email

Introduction

The internet is a great tool that small businesses can use for a variety of different functions. Web browsing and email are two important functions that assist businesses with their daily activities. There are similar security precautions for these two functions that will help the security of a small business. Employees need to be trained on proper internet and email use; otherwise vulnerabilities can be created and taken advantage of.

Secure Web Browsing

Allowing employees to access the internet provides them with an excellent tool to assist in business activities. However, vulnerable web browsers can be attacked, putting small businesses at risk. New software vulnerabilities can be exploited and targeted at web browsers through malicious web sites [16]. It's important to keep web browsers up to date. Using the most current version of a web browser will help protect it against recently discovered security flaws. Web scripts can create vulnerabilities in web browsers. Websites use scripts to execute programs in the web browser, which allows increased functionality, as well as design embellishments, such as drop down menus [17]. These features may provide an avenue for an attacker to get malicious code into a computer. JavaScript is one of the more popular web scripts available and is considered active content. Attackers can use vulnerabilities in JavaScript to redirect users from a legitimate website to a malicious website, causing the user to download a virus or allowing the malicious website to collect user information [17]. Disabling JavaScript on unknown sites will help prevent this vulnerability. There are several add-ons available or settings can be changed within the browser itself to disable JavaScript, which will be described

below. Java and ActiveX controls are different than JavaScript, but are still considered to be active content [17]. Take care in running active content on websites that you are unfamiliar with. Employees should manually type in websites when they are conducting activities for the business. This will help ensure that the employee is going to the website they are intending to go to. They should also be careful not to go to questionable websites or visit suspicious links that may pop up. A suspicious link may be identified by placing the mouse cursor over the link itself, without clicking on it. If the link that shows up in the pop up box does not match the printed link, then you should not click on it.

Cookies

Another security concern with web browsers is cookies. Cookies collect information about your browsing (IP address, the domain you used to connect, the type of browser you're using, how often you visit a particular site) [17]. To prevent websites from collecting personal information from your business, consider blocking or limiting cookies. How to block cookies depends on the browser being used.

Google Chrome

Inside the Google Chrome web browser, there are three little lines in the upper right corner, next to the address bar, which allows you to customize Chrome. Click on this icon and a drop down menu will open. Clicking on "settings" will take you to the settings tab (you can also access the settings tab by typing in "chrome://settings" in the address bar). Scroll down and click on "Show advanced settings…". Click on "Content settings…" underneath "Privacy". This opens up a pop menu that allows you to make several adjustments to web content, including cookies, JavaScript, Plug-ins, Pop-ups and allowing sites to automatically download files (shown in Figure 2 below).

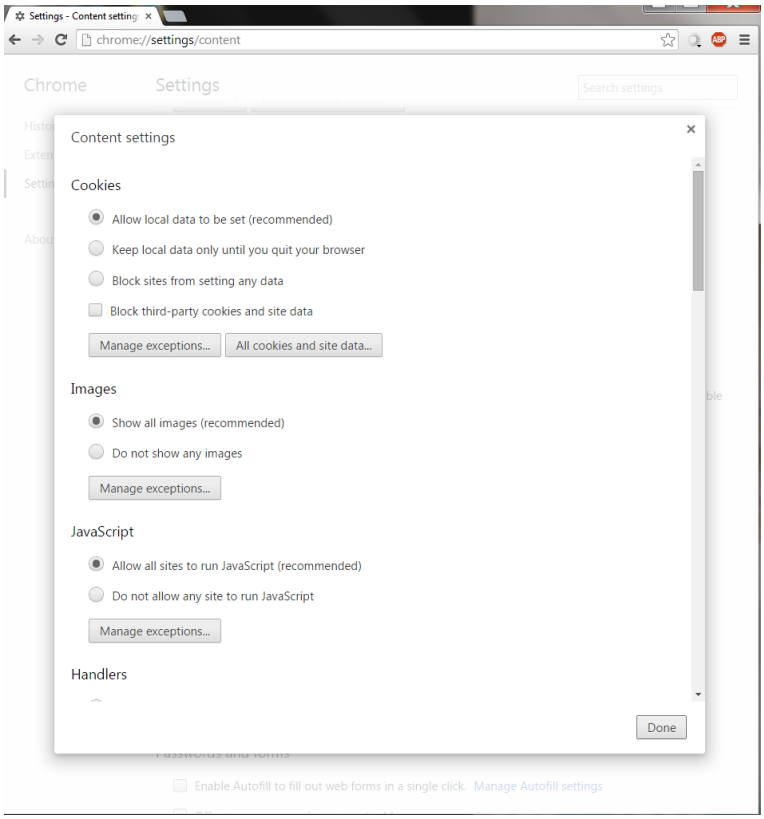


Figure 2. Google Chrome cookie settings

Chrome offers recommendations on you should be using, but it also allows you to adjust the settings to your particular needs. Under "Cookies" you can select from: Allow local data to be set (recommended), Keep local data only until you quit your browser, Block sites from setting any data, and Block third-party cookies and site data. There is also an option for cookie exceptions that let you allow, block, or clear on exit cookies on sites that you specify. For instance, if you wanted to block all cookies except for a few site that your business needs, then you can add these specific sites to exception list and click on the drop down menu and select "allow".

JavaScript

Also within the "Content settings" menu, you can "Allow all sites to run JavaScript" or "Do not allow any site to run JavaScript". You can also create exceptions for specific sites to allow or block JavaScript. Click on "Done", close the tab, and your settings will be applied.

Firefox

Firefox has three small lines in the upper right corner of the browser, next to the address bar. This opens a menu to make changes to your web browser. Click on the icon, then click "Options". This will open a pop-up menu, as seen in Figure 3 below.

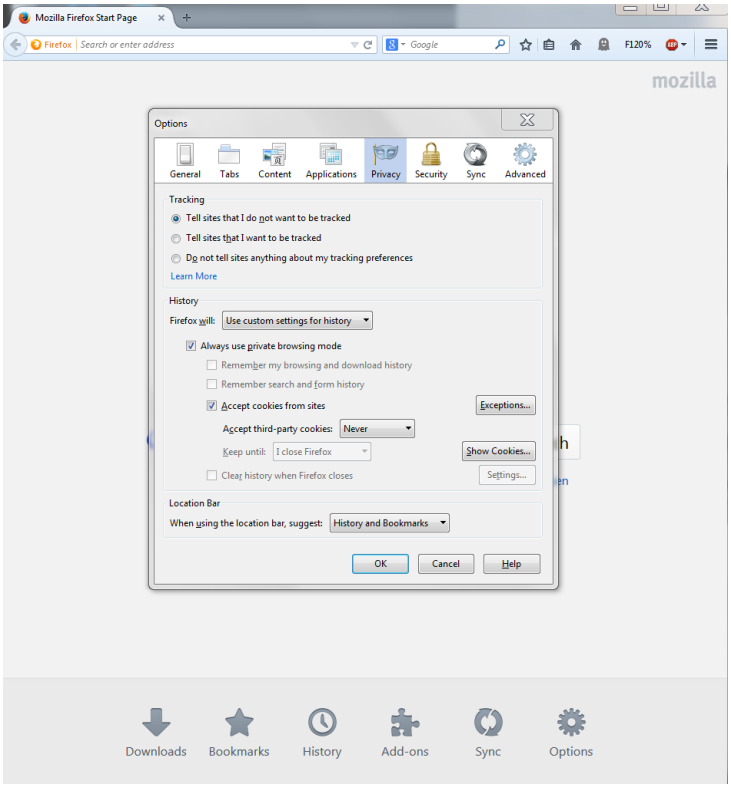


Figure 3. Firefox cookie settings

You will see several icons near the top of the window. Locate the one that says "Privacy" and click on it. This will open options for the web browser to change history and

cookie settings. You have the option to Accept cookies from sites, Accept third-party cookies (Never, Always, From Visited) and you can even select how long you want to keep the cookies (e.g. until you close Firefox). There is an "Exceptions" icon that will allow you to add specific websites. The options are block, allow for session, and allow. Again, this is helpful if you want to apply general settings to all sites (e.g. block), but want to allow a few sites for your business to use. Also, within the "Security" tab, you have the option to Block reported attack sites and Block reported web forgeries (check the box to apply). Click "OK" and the settings will be applied.

Additional Browser Tools

Chrome and Firefox have tools called extensions or add-ons that you can add to your web browser. Both browsers off similar features that can help you make your browsing more secure. For instance, there is an extension/add-on called "Web of Trust". This gives you a reputation rating that is color coded (Red – bad, Green – Good) based on the trustworthiness of a site and also if it is safe for kids (which would mean that is safe for the workplace). Figure 4 below shows the Web of Trust result for the add-ons page for Firefox.

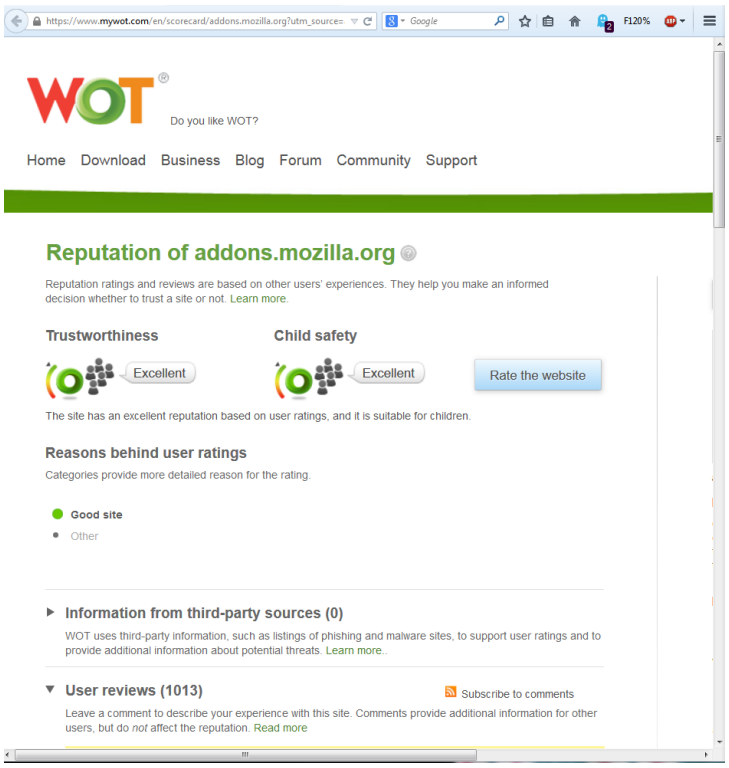


Figure 4. Web of Trust example

Another nice extension/add-on is "Adblock Plus". This tool allows you to block all sorts of ads and banners that pop up on various websites. This will help prevent employees from clicking on ads that may redirect the employee to a malicious website. An extension/add-on that blocks scripts would also be useful. For example, Firefox uses a tool called "NoScript" that allows the user to decide what type of active content to run. If an employee is on a trusted website, they can choose to allow or forbid whatever active content is being displayed on the page. If used carefully, this tool will help prevent attacks on the web browser.

Secure Email

A business needs email to communicate with employees, customers, potential customers and other businesses. Employees must understand the importance of practicing safe email habits. Employees need to take care in opening suspicious emails. A few signs that an email is

suspicious: the email greeting is generic and reads something like “Dear valued customer” instead of “Dear Mr. Jones”; the message comes in to a different email address than what was given to the sender; emails from customers or companies that you have previous correspondence with that appear different than what you’ve previously seen [19].

Spam

If an employee suspects that an email is spam, they should immediately delete it. Spam can contain malware that can spread through the business’ network. Disabling the email’s preview pane and reading emails in plain text is another option to use if users think they are dealing with spam [18]. Email filters and rules can be adjusted in the email program to help send spam to specific folders (junk mail) instead of going to the Inbox.

Phishing

Phishing emails can be recognized by one of the following qualities: an email that requests confidential information, the use of scare tactics to entice a response, or no personalization within the email [18]. Employees should never provide confidential information via email. If there is a request that may seem suspicious, the employee should take additional steps to verify the email is legit. For example, the employee can ask for a phone number, and then use online resources to verify the phone number. Once verified, the employee can contact the questionable entity and verify that a legitimate request was made. Malware can also be transferred through Email. Malware can come from a legitimate, known email address. The person sending the email may not realize they are infected with malware. If employees receive an email they aren’t expecting, or an attachment they aren’t expecting, they should proceed with caution. As with browsing the web, caution should be taken when web links are included within emails. A common phishing technique is to include links in emails that appear to go to

legitimate sites, however if you place the mouse cursor over the link, the true website will appear [19]. Figure 5 shows what this looks like:

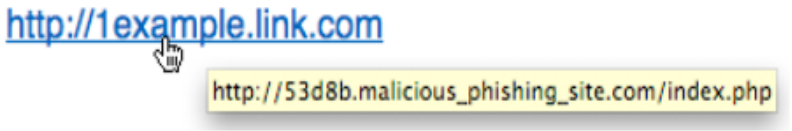


Figure 5. Phishing example [19]

If the website that appears in the popup window is questionable or does not match what is printed within the email, then it should not be clicked on. Employees should delete suspicious or unwanted emails, email attachments should be scanned with an antivirus program, and security patches should be kept up to date [18].

Alternative email software

Small businesses should also consider using a reputable company that provides secure email. Secure email may provide encryption, administration console, compliance reports, email trackers and logs, email expiration dating and archiving [20]. These products should be chosen with the customers in mind. If the customers find it too difficult to use, then it may not be well accepted. There are many companies that provide this software (Voltage, DataMotion, Proofpoint, Trend Micro, Symantec, Sophos), but a small business should decide on one that meets all of its requirements [20]. A small business should focus on the following list of features when choosing email encryption software:

Security

- Software that provides user-based or policy based encryption
- Software that automatically block emails that contain sensitive information

- Software that provides secure email and additional layers of security (e.g. protection for email data stored at a data center)

Customer Experience

- Simple to use for the customer
  - Does not require the customer to download software
  - Does not require the customer to maneuver through a complicated process
- Allows customers to send secure return emails and request passwords without administrator involvement

Administration Tools

- Simple to use
- Function alongside popular business solutions (Salesforce, Groupwise, etc.)
- Work across platforms with all email types, regardless of device (PC, mobile phone, tablet)
- Work in conjunction with content and internet filters [20].

Summary

Secure web browsing and secure email primarily rely on employee awareness. Certain controls such as restricting web scripts from running will help prevent web browser attacks. Disabling cookies will help keep personal business information from getting into the wrong hands. A user should never click on a suspicious link, whether it's on a web page or in an email. Suspicious looking emails and attachments, even from legitimate users should be carefully analyzed before opening. If in doubt, the email preview pane should be disabled and emails should be opened in plain text. Email filters will help reduce spam and antivirus software will

help prevent malicious attachments from being opened. Web browsers and email programs should be up to date to ensure the most recent security patches are in place. Secure email encryption software can be used to increase email security.

Chapter 3: Computer Security

Introduction

Computer security is a big priority for small businesses. A business can save itself a lot of headache by limiting the data that users can access. Only certain users (trusted IT staff and key personnel) should have administrative privileges [1]. Software installation should be done by administrators and not left up to the individual user. Keeping software and operating systems patched and up to date is extremely important [5]. Without these updates, software and systems may be vulnerable to attacks. Anti-virus and anti-malware programs will help fight off malicious software intrusions on individual computers [4, 5, 6]. A software firewall on each system will help supplement hardware firewalls and some operating systems come with the firewall as part of the operating system [2]. Mobile security consists of password protecting the device, encrypting data and installing security applications [1]. Regardless of the type of "computer" that is being used, certain security features need to be implemented in order to protect data.

User Accounts

One of the first things a small business will do when giving an employee access to a computer is determining how that employee will interact with the computer. This will be done by creating an account for that employee. For small businesses that use Windows, either an administrative account can be used or a standard user account can be used. An administrator account allows complete control over the computer and allows the user to install software and make changes that affect all users on the system [21]. A standard user can only use the software installed by the administrator and the changes they make only affect their account and not all

users on the system [21]. This is important because employees should not be able to make changes to other accounts on the system. An employee may not realize a simple settings adjustment or software installation can create a vulnerability in the system. Each user on the system should have their own account by assigning specific usernames to each account. Usernames should be unique in the sense that they should be different than all other usernames on the system [22]. Depending on the size of the organization, different naming schemes can be used. A few examples: first name (brian); last name (little); first initial followed by last name (blittle); or last name followed by department or department code (littlemsis or little68k) [22]. If a business is using a Linux based operating system, then it needs to be determined what permissions will be given to employees. Employees should have the least amount of access and permissions needed to complete their jobs. Front desk workers should not have access to payroll; payroll should not have access to customer data, etc. When setting up user accounts for Linux, permissions can be assigned to files based on different categories. The following permissions can be given to users: (r) – read a file, (w) – write to a file, (x) – execute a file [22]. These can be assigned based on which category the user is assigned to (owner of the file or application, the group that owns the file or application, or everyone that has access to the system) [22]. Assigning proper permissions to users will help keep systems secure.

Software

A business uses different pieces of software for a variety of reasons. When it's time to install new software or update to a newer version of software, the only person that should be allowed to install and update this software is the administrator. Users with standard accounts will not be able to update software for the system or download unapproved and potentially malicious software.

Software Updates

Software updates (or patches) are released for a variety of reasons: upgrading a piece of software to the latest version with new features, improvements in the application's stability, or to fix a bug or security hole within the program [23]. These updates help make software more secure by fixing known problems. It's important to update the software as soon as possible, as there are hackers out there that will be looking to exploit the vulnerabilities. When a program hasn't been used for awhile, it's a good idea to check for any recent updates. Sometimes programs only check for updates while they are running [23]. Any program the business regularly uses, including web browsers, should be updated as soon as possible. Operating systems should be updated as well. Operating systems can be configured to alert you that new updates are available, but you can also check manually if you wish. If a company no longer provides updates for its older operating systems, new vulnerabilities will never be patched [23]. It's important for small businesses to use operating systems that still have updates being released.

Anti-Virus

Another security feature that small business should utilize is anti-virus software. Anti-virus software will help prevent, detect and remediate malware infections [24]. Viruses can make your computer run slower, erase your files, crash your computer, or make your information unavailable to you [25]. Updating this software is especially important, to make sure that you are protected against the newest known viruses. The software may not be shipped with the most recent updates, but manufacturers of anti-virus software release updates on a regular basis [25]. Be sure to update the software as soon as an update is available. Anti-virus programs also help protect against other types of malware, including worms, Trojan horses, rootkits, spyware,

keyloggers, ransomware and adware [24]. Check the user license agreements on the anti-virus software to see how many computers you are able to protect with one license.

Software Firewall

A software firewall checks information coming in from the internet or a network and either allows it or blocks it, based on its settings [26]. This can prevent malicious software from getting into and out of your computer. When the firewall allows a program, the program can communicate through the firewall by opening one or more ports [26]. Blocking a program does not allow it to communicate through the firewall, which helps with the security of the computer. Certain versions of Windows come with the firewall already on and configured [26]. However, you may want to allow or disallow specific programs through the firewall, so the settings may need to be changed. To get to the Windows Firewall:

- Go to "Control Panel"
    - Click on "System and Security"
        - Click on "Windows Firewall"
            - Click on "Allow a program or feature through Windows Firewall"

An example of a Windows Firewall is in Figure 6:

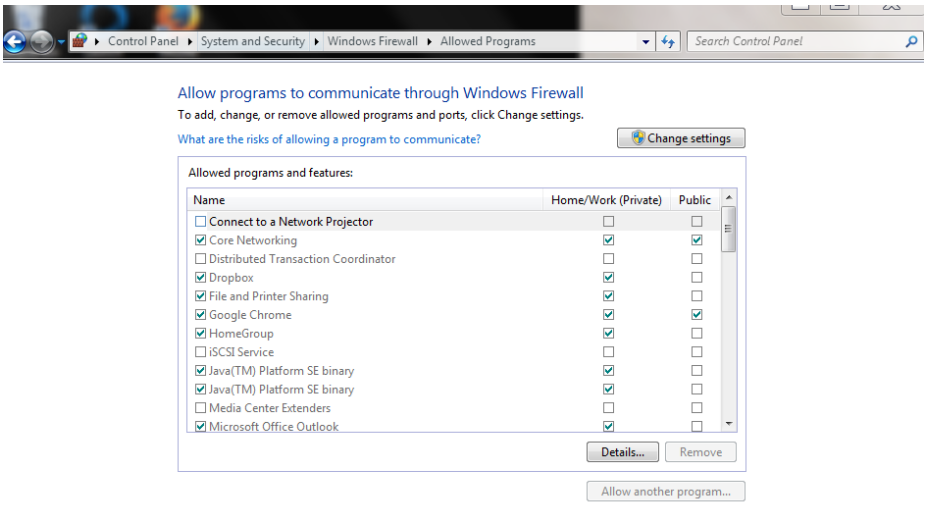


Figure 6. Windows Firewall example

Software firewalls should be left on, even if a hardware firewall is being used. For instance, if the network your business is on is using a router firewall, then this will help protect against computers from the internet. However, if an employee or guest uses their own computer to access the business' network, then the router firewall won't protect against malware that is brought in by the guest's computer, because the guest's computer will already be behind the network firewall [26].

Mobile Security

Mobile devices can be useful tools to help increase productivity in a business. Mobile devices may include smartphones, tablets, or laptop computers. However, the portability, access connectivity, data storage and processing power make these devices a security risk [27]. Theft is a big concern, not only for the device itself, but also for the information that is on that device. Laptops can use the features that were discussed in early sections. Mobile devices such as smartphones, should have the following features enabled: a secure password with auto lockout for incorrect password attempts, a remote wipe features to wipe any sensitive data that is on the

device, the device should not be "jailbroken" as key security features will be disabled, an anti-virus can be used if your device's operating system supports it, and wireless access such as Bluetooth and Wi-Fi should be disabled when not in use [27]. All employees should abide by these suggestions if they intend on using their smartphone or similar device to access or store company information on them. Also, software or applications should be approved by the business, especially on devices owned by the business. Certain permissions may allow access to confidential or sensitive information [27]. Educating employees about smart social media use is also a good idea. Company secrets can be easily given away if an employee irresponsibly posts restricted information on social media.

Endpoint Security

Another option for businesses to use in order to tie all the above recommendations together is "endpoint security". Endpoint security is a client/server concept that focuses on protecting a network's devices (computers, servers, etc.) by monitoring their status, activities, software, authorization and authentication [28]. This goes beyond just "anti-virus" software and is a more comprehensive approach to small business security. Endpoint security software can include anti-virus, antispyware, firewalls, a host intrusion prevention system, browsing protection, USB device control, user device authentication, user access rights, remote management, mobile management and policy creation (for example, banning access to specific websites) [28, 29]. Like anti-virus software, the endpoint security software will be installed on each computer that needs protection. Unlike anti-virus software, this software can be centrally managed, which may help reduce security issues because the administrator can enforce settings, view detailed reports and troubleshoot PCs remotely [29]. This is more convenient than addressing each computer individually and physically. Different software companies offer

different levels and options of security, so once a small business decides what type of protection it wants, it can pick one based off of its needs. Several companies that offer these products are Avast!, AVG, Symantec, Bitdefender, Kaspersky, Panda, Webroot and F-Secure [29].

Summary

Computer security deals with keeping the computers that are used for business secure. User accounts should be created for each individual employee of the company. Employees should be assigned as a "standard" user or equivalent to help prevent that specific account from making changes to the entire computer. Software and operating systems should be updated as soon as available to ensure that the most recent security holes are patched. Anti-virus software will help prevent malicious software for damaging business' computers. A computer is even more protected when a software firewall is used to prevent certain traffic from flowing into or out of a computer. Mobile devices can help increase productivity, but can also increase risk to a business. Policies should be created that address specific issues with mobile devices, such as passwords, remote wiping of data, and using anti-virus software when available. Endpoint security software can provide a manageable way for a business to implement anti-virus, firewalls, web protection, and user access rights. Allowing these tasks to be centrally managed will make it easier for a business to use the software successfully.

Chapter 4: Data Security

Introduction

Data security must be a priority for small businesses; otherwise a simple data breach could have their customers lose trust in them. Businesses can't run without a solid customer base. Limiting access to confidential or sensitive information is very important [5]. As explained in the computer security chapter, each user should be restricted on the amount of data they can access. Encryption will help keep confidential or sensitive information out of the wrong hands. Also, making regular backups of important business data is vital [4, 6]. If a business is attacked, and their data is compromised, damaged or destroyed, then a backup will help a business return to normal activities.

Encryption

Data is a business' most important asset. Data can be employee information, office correspondence, customer information, product information, transaction information, bank account information and sensitive company information. A company can protect this data by using encryption. Encryption is the process of encoding data in a way that only a person (or computer) with a certain key can make it readable [30, 31]. Many software programs have encryption capabilities built in. You can encrypt your hard drive, external and USB thumb drives, internet traffic, cloud storage, email, Microsoft Office documents (Word, Excel, and PowerPoint), PDFs, and just about anything else that your business needs [31]. Mobile phones that come with encryption software should utilize this feature if the mobile phone contains company data.

A business can store sensitive information on a hard drive. Passwords are very important in protecting your information. A login password for Windows will not prevent data leakage because someone can steal your hard drive, plug it into a PC and access it that way [31]. A way to prevent this from happening is by encrypting the hard drive itself. Products are available for full-disk encryption, including Microsoft's BitLocker and DiskCryptor [31]. If a business is using Windows computers and BitLocker is available, then this should be used since it's already installed on the computer. To use Bitlocker, do the following steps:

- Go to "Control Panel"
    - Click on System and Security"
        - Click on "BitLocker Drive Encryption" (You can also search for "BitLocker" in Windows 8)
            - Inside the BitLocker menu, click on "Turn on BitLocker" next to the drive you want to encrypt [31].

Figure 7 shows what the final step looks like:

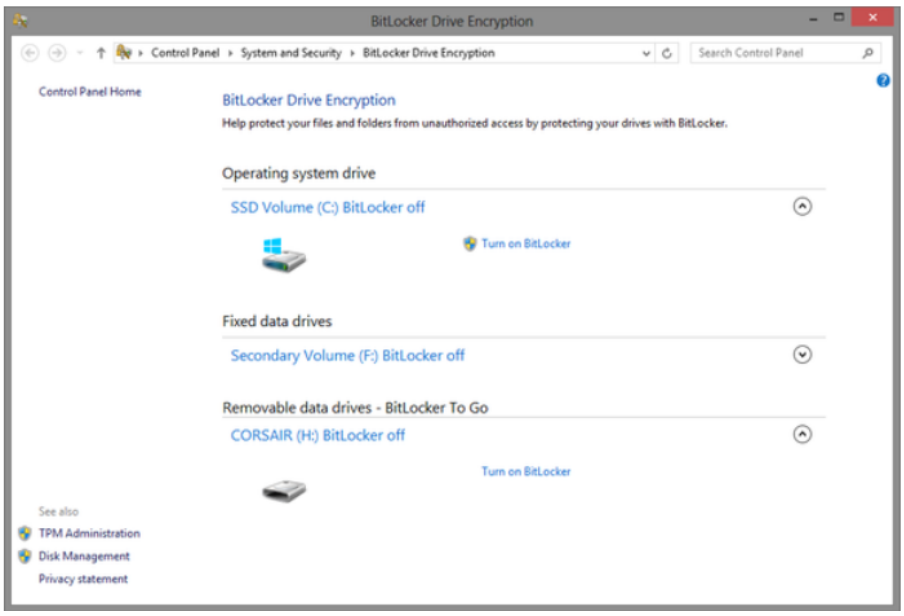


Figure 7. BitLocker example [31]

DiskCryptor is a free alternative. BitLocker To Go can also provide encryption for thumb and USB hard drives [31].

Internet Traffic

When web servers and internet browsers need to transmit sensitive information, they can use encryption to do so. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) use public key encryption to accomplish this task [30]. These types of connections should be used when any sensitive or confidential information is being passed over the internet. The employee can identify this type of connection by "https" in the address bar or a small padlock in the status bar at the bottom of the window [30]. Another way to encrypt internet traffic is by using a virtual private network (VPN). A VPN creates a secure "tunnel" that allows you to send encrypted data through [31]. This is a good alternative if employees are traveling and they can't verify that a Wi-Fi network they're using is secured and they are transmitting sensitive information. VPNs will be discussed later in the Network Security chapter.

Cloud Storage

Businesses that utilize cloud storage need to be conscious of protecting their data. Certain cloud storage providers, such as Dropbox and SugarSync, encrypt your data while it is stored on their servers [31]. Be sure to use a form of encryption to send the files to cloud storage, otherwise data can be intercepted and read in transit.

Email

Check with the email service provider the business is using to see if email encryption is included. Microsoft Outlook has a non-password based encryption system that uses digital certificates [31]. This works by having two users exchange digital certificates by sending digitally signed messages [31]. Once this is done, Outlook will encrypt and decrypt the messages sent between the two users. Figure 8 shows the box you need to check to encrypt Outlook email:

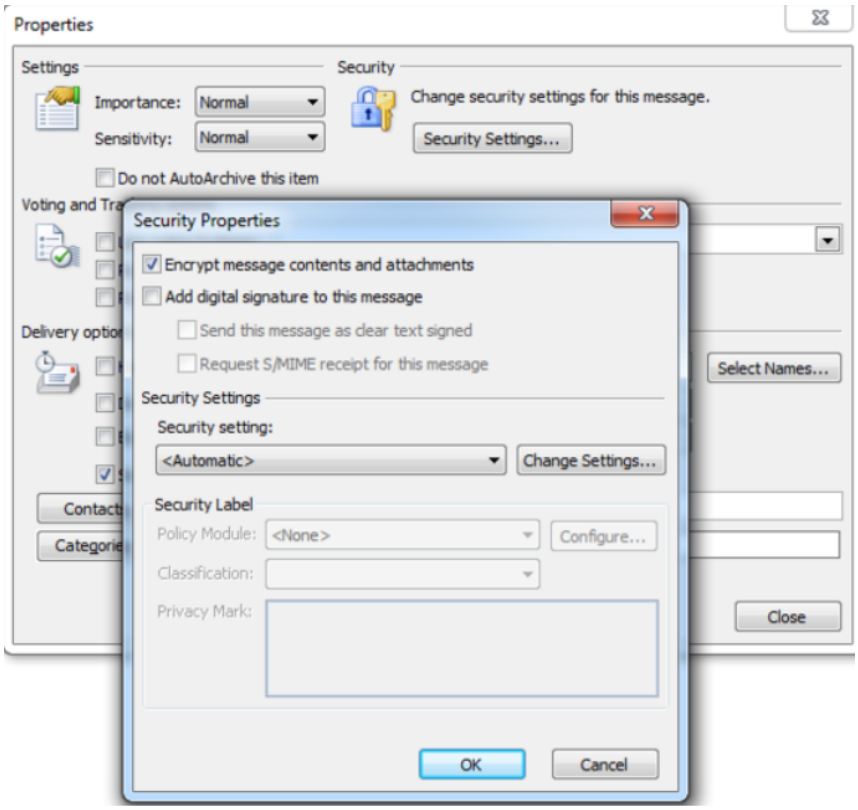


Figure 8. Encrypting Outlook email [31]

Microsoft Documents and PDFs

If a business is using Microsoft Office products, then there is an encryption feature already built in. In Office 2010 and 2013, you can encrypt Word, Excel, and PowerPoint documents using the same technique [31]. Click "File", select "Info", then click on "Protect Document", then "Encrypt with Password". Choose a strong password to encrypt the file. The recipient of the document will need the password, but do not send it through the same channel as the document [31]. For instance, if you email the document, do not send the password in the same email. Adobe uses a similar procedure to encrypt PDFs. Click on the "tools" tab in the "Protection" section, then click "Encrypt", and "Encrypt With Password". Use the same procedure for selecting and sending the password as with the Microsoft products.

Backups

Another important topic in data security is creating backups of data. If a business loses its data in a compromise or a disaster, it may not be able to recover. Data can be backed up using storage tape or external hard drives, disaster-hardened storage devices, or cloud services [32]. A business that wants full control of their backups may want to use local storage and not a cloud service. Also, if a business uses a cloud service, they must trust a third party to keep their data safe and their network may get bogged down transferring data [33].

Local Storage

Local storage is when a business uses storage tape or external hard drives to backup their data. This type of storage allows a business to make backups locally, which can then be moved to an offsite location to help keep them safe [32]. This is especially important if a disaster (such as a fire or flood) occurs at a business which leaves all the computers inoperable. Disaster hardened storage is another way to store backups locally. A business can store backups in a fireproof safe or similar device, such as an ioSafe 214[32]. The ioSafe 214 is built to withstand fire and flood damage in order to protect the data inside. It even has the capability to sync with cloud services [32].

Cloud Storage

Cloud storage allows a business to store its information in an offsite location. Cloud service providers can offer a variety of backup features such as automatic backups that don't require user intervention, archiving, incremental backups, file managers, and access to data from remote locations [33]. Cloud storage allows employees who are traveling to have access to data away from the office, which can't be done using a local backup system. Cloud service fees are based on how much data a company is backing up [33]. However, this may be more cost

effective for a company because they don't have to buy additional storage tape, external hard drives, fireproof safes, or pay for an offsite storage location. A business should choose an online data backup service based on the needs of the business. Some things to consider are the ease of use of the service, remote access features to allow employees to access data, and excellent support [33]. If a service is difficult to use, employees may have a hard time embracing it.

Backup Service Providers

Some companies that provide online data backup services are MyPC Backup, Carbonite, SugarSync, OpenDrive, Dropbox, Ibackup and IDrive [34]. These services all offer automatic backups, backup resumes after interruption, remote access (including mobile phone access, iPhone, and Android applications), SSL secure transfer, encrypted storage, and Email support [34]. These are all important features businesses should look for in a cloud backup service. Other features that may be relevant to your business are syncing PC and mobile images, the ability to send large files, phone and or 24/7 support. Not all backup services provide these features, but if having certain features like phone support is important, then you should pick a backup service that provides this feature. Prices for these services vary, so if cost is an issue, there are several plans to choose from [34].

Summary

Securing data will help keep a company in business. Using encryption on hard drives, USB drives, for internet traffic and email, and also for cloud storage will help keep data secure. Most businesses will be able to use encryption features that are already found in the products they have. Backing up data should be done by every business. Data can be backed up locally using storage tape or external hard drives, or a cloud service can be utilized. If a company doesn't have the resources to store data locally, then a cloud service is a nice alternative that

provides features such as remote access to data that local storage does not. Backup data is not free from vulnerabilities and encryption should be used when available.

Chapter 5: Network Security

Introduction

Another concern for small business security is a business' network. Network security consists of protecting the company's network from intrusions and other network based attacks. This can be done by changing default usernames and passwords of network devices such as routers, securing the Wi-Fi to keep unwelcome guests off of the network, using WPA2 encryption, not broadcasting the SSID (service set identification), disabling the Wi-Fi protected Setup (WPS), creating a guest network, and disallowing administrative access from the wireless network [3]. Small businesses should have a hardware firewall installed between their internal networks and the internet to help restrict network traffic [2]. Virtual Private Networks will help remote employees securely connect to the business' network. Unified threat management allows an administrator to monitor and manage a wide variety of security-related applications through a single management console [35]. Managed Security Service Providers (MSSPs) provide businesses with a comprehensive set of security tools. These include: firewalls, application control, intrusion prevention, web content filtering, VPN, spyware prevention and malware defense, site to site and remote access via IPSec and SSL [36]. A brief overview of a sample small business network security design is available for small business owners to use as a guide.

Network Equipment

In order for a business to connect computers internally and externally (e.g. the internet), a business will need some equipment. At the very least, a router will get the network up and running. Different types of routers are available that allow a business to connect printers, network storage, or wireless access points for Wi-Fi coverage [37]. A small business or

consumer wireless router will be sufficient for a 1500-2000 square foot office and will accommodate up to a dozen computers and Wi-Fi devices [37]. Businesses that have more than a dozen computers or devices should look into the following equipment:

VPN router/firewall

- Offers an integrated virtual private network server
- Advanced features such as VLAN support and multiple SSIDs (Service Set Identification for wireless connections)

Unified Threat Management gateway or firewall

- Usually Ethernet (wired connection) based with a separate access point for Wi-Fi connectivity
- Used for router and internet gateway
- Provides a VPN server, firewall, virus/malware protection, content filtering, antispam functions, and intrusion detection and prevention

Ethernet Switch

- If more ethernet ports are needed (larger small businesses) than what is provided by the above, then consider using this device
- Unmanaged switch doesn't require configuration, but lacks advanced features (good for small, uncomplicated networks)
- Smart or web-managed switch allows configuration of switch ports (more advanced and useful for small to midsize businesses)
    - Supports VLAN, bandwidth control, 802.1x authentication, and SNMP

Wi-Fi

- Choose a router that uses at least 802.11n (sometimes referred to as Wireless-N) routers to ensure the business devices connected attain the highest possible speeds
- Consider a dual-band router if the business is close to other businesses
    - Allows you to choose between the 5Ghz or 2.4Ghz band, which may help alleviate some congestion (slow down) for your network [37].

Consider the amount of devices and what type of features the small business needs to help decide on the appropriate network equipment. As a small business grows, network equipment should be upgraded accordingly.

Routers

When you set up your router, you can login by checking the network connection information on your computer and locating the "default gateway" (or by using the instructions that come with the router). Once you have the address, you can type it into a web browser and have access to your router. The first step is changing the default username and password. Once this is done, numerous settings can be changed in order to help secure your network.

Default Username and Password

When you first set your business' router up, you have the option in changing some of the default settings, such as user name and password. It's important to change these immediately; otherwise your business network is vulnerable to an easily fixable attack. A quick search on the internet [13] can return numerous default usernames and passwords for a variety of network equipment vendors. Change the username to something other than "admin" or "administrator" and use a secure password to lock down your router.

Encryption

Another option that should be utilized is enabling WPA2 encryption on your router. Chances are your router gives you a variety of options for encryption (WEP, WPA, WPA2) [3]. The Wired Equivalent Privacy (WEP) encryption is the weakest of the bunch and the encryption keys can be cracked within minutes [38]. Wi-Fi Protected Access (WPA and WPA 2) are more secure than WEP. WPA's technology has recently become vulnerable; however using a strong passphrase may help prevent attackers cracking the key [38]. WPA2 uses AES-based encryption, which is more secure and harder to break than WPA [3].

Complex Passphrase

Using a complex passphrase for access to your network is also a good idea. Similar steps can be taken to create a complex passphrase as if you were creating a strong password. Use a combination of upper and lower case letters, symbols and numbers. Again, do not use common words that are found in dictionaries, as these may be susceptible to brute force attacks [3]. Brute force allows an attacker to try numerous combinations, (from a dictionary for example) until the password is cracked.

SSID and WPS

The Service Set Identification (SSID) is what is broadcasted from your router to let people know that your network is available. Turning off the broadcast so people can't see may help prevent some attacks on your network. However, it is still possible to obtain the SSID and a better suggestion is to change the default SSID and not use a common SSID name [3]. A common SSID name is usually one that is shipped with the networking equipment, or something that a lot of people tend to use. Some examples of common names are linksys, NETGEAR, dlink, FreeWiFi, belkin54g, internet, VOIP, ATT___ (various numbers), 2WIRE___(various

numbers), SSID, and staff to name a few [39]. Attackers have created lists that specifically attack these common SSID names [3]. Wi-Fi Protected Setup (WPS) is another feature that may be available on your business' router. This feature allows users to connect devices easily to the network using an 8 digit number that is printed on the router. This feature is susceptible to brute force attacks and an attacker can break the PIN code in approximately four to ten hours [3]. If the attacker is able to do this, it potentially puts your passphrase at risk, as well as the rest of your network. Disable this feature if it is available.

Firewalls

A common method for locating network vulnerabilities is scanning for open ports [40]. Ports that are not being used by the business should be closed. A firewall can help close unused ports for a business to help increase its security. One way to check if your router is equipped with firewall capabilities is to log into the router and check for "firewall" or "security" settings [40]. Once inside, you can select what type of traffic is allowed in and out of the firewall. Having the firewall sit just behind the point where network connectivity comes into the business will help filter out bad traffic before it gets into the network [40]. Also, check the settings to see if you can disable or block network pings. Network pings allow an attacker to see if network devices respond, which may allow an attacker to further investigate a possible vulnerability on your network [40]. In addition to closing ports in the router's settings menu, you can also block websites that are known to be malicious, or sites that you do not want your employees to have access to.

Other Features

Routers often come with the option of setting up a second network or a "guest" network. Depending on what type of business you do, you may have customers waiting at your business or

even requesting access to your Wi-Fi. Creating a guest network will help keep unwanted "guests" off of your main business network. You can change the passphrase to this guest network as often as you would like and disable it during off hours [3]. A guest network is an example of a virtual local area network or VLAN. VLANs allow a business to separate the network into segments [40]. This setup can also prevent employees from certain departments from accessing other departments on the network that they shouldn't have access to (sales shouldn't be accessing payroll for example). If someone gains unauthorized access, they will only have access to a portion of the network [38].

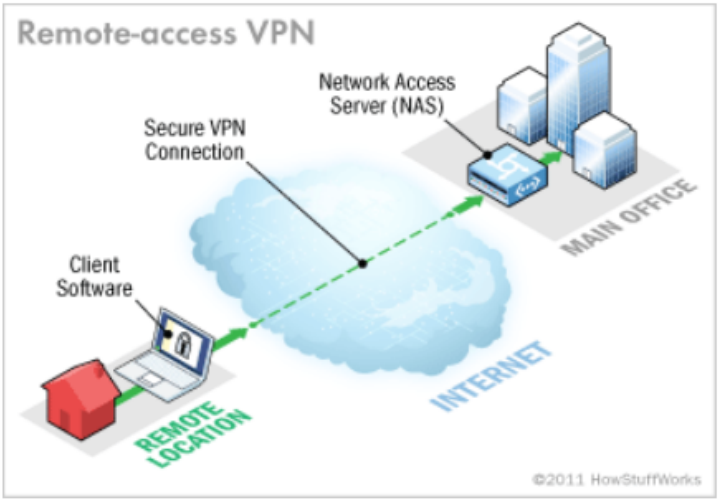
Another feature that should be utilized is not allowing administrative access from the wireless network. This may be difficult if the business IT person is traveling, as it only allows changes to be made from a locally connected computer [3]. However, this would help prevent remote attackers from making changes to the network.

As with software, routers should be updated as often as possible. Firmware updates for routers and updates for network adapters and drivers should be done periodically [38]. This will help ensure that all security features are up to date on network components.

Virtual Private Networks

Virtual Private Networks or VPNs allow remote workers to securely log in to the business' network through an encrypted tunnel [40]. This would provide the employee with the same protections they would have as if they were connected locally. When considering a VPN, some features that should be included: the VPN should protect data while it's traveling on the public network, the VPN should be reliable so employees can easily connect when necessary, and it should be scalable to accommodate a growing business [41]. If a business has the

resources, it can set up its own VPN using a server and client software. Another option is to outsource the VPN service to an enterprise service provider [41]. This may help a business without a dedicated IT staff to utilize a security tool without having to maintain it themselves. A site-to-site VPN allows offices in different, fixed locations to establish secure connections with each other [41]. This allows a company's network to be extended by making resources available for an employee that is at a different location than where the resource resides. A remote-access VPN allows an employee to connect to a private network for a remote location [41]. Figure 9 shows what a remote-access VPN looks like:



A remote-access VPN connection allows an individual user to connect to a private business network from a remote location using a laptop or desktop computer connected to the Internet.

Figure 9. Remote-access VPN [41]

Additional VPNs are available and include, PPTP, L2TP/IPsec, and SSL. Point-to-Point Tunneling Protocol (PPTP) is supported by nearly all operating systems and mobile devices with a built-in VPN client, but it does not provide the best security and users may have a problem connecting remotely to networks that don't allow VPN pass-through [37]. PPTP supports 40 bit and 128 bit encryption and any authentication supported by the point-to-point protocol [41].

Layer 2 Tunneling Protocol (L2TP)/IPsec is also supported among most operating systems and mobile devices [37]. L2TP/IPsec provides better security than PPTP, but is more difficult to configure and also has issues connecting to networks that don't allow VPN pass-through [37]. The Secure Sockets Layer (SSL) protocol allows remote users to connect via a web browser (eliminating the VPN pass-through connectivity problem) [37]. SSL can be utilized by installing a small plug-in via the web browser. Some SSL VPN methods allow a web portal that allows users to access applications and email without using a VPN client [37]. If a small business issues laptops to their employees to allow them to perform work remotely, then client software can be installed on these laptops. If an employee is working from home or using a personal laptop to conduct business matters, these employees should use SSL to help keep information in transit safe. Administrators with little knowledge of VPNs should stick with SSL or PPTP. Those that understand VPNs can utilize L2TP and SSL to securely conduct business remotely.

Unified Threat Management

Unified threat management allows an administrator to monitor and manage a wide variety of security-related applications through a single management console [35]. This can be purchased as a network device and offers a variety of network security features. Not only will it serve as a router, it can provide a VPN server and firewall, virus and malware protection, content filtering, anti-spam functions, intrusion detection and prevention, identity based access control, and SSL and SSH inspection [37]. This would wrap up most, if not all of your network needs into one area. One issue with this set up is that it can become a single point of failure for your network [35]. A business can use two devices with the same configuration to help prevent this single point of failure. UTM devices usually contain a fail-safe feature that ensures continuity and allows a connection to a secondary gateway if the main one can't be accessed [42]. Multi-

layered protection, such as dual anti-virus, intrusion prevention systems, advanced threat protection, a proxy, and a firewall also help reduce the chance of a single point of failure within UTM's [42]. Although a single point of failure is a major concern, proper planning can help reduce the risk.

Managed Security Service Providers

Managed Security Service Providers or MSSPs, provide businesses with a comprehensive set of security tools. These include: firewalls, application control, intrusion prevention, web content filtering, VPN, spyware prevention and malware defense, site to site and remote access via IPSec and SSL [36]. Similar to a UTM, MSSPs can provide just about everything that a small business requires for a safe and secure network. These providers are experts that not only provide the above services, but also follow strict guidelines and best practices within the IT security industry [36]. If a small business has no IT security experience, then an MSSP is a nice option. Choose a provider that offers services that pertain to your business needs. Several providers are Fortinet, leidos, Trustwave, Lightedge, and Earthlink [36].

Sample Small Business Network Design

If a business chooses to set their own network up, then they will need to come up with a design on how to do so. Depending on the size and needs of the business, different equipment than what is mentioned above may be needed. A sample network design containing workstations, servers, bridges, switches and a gateway is shown in Figure 10:

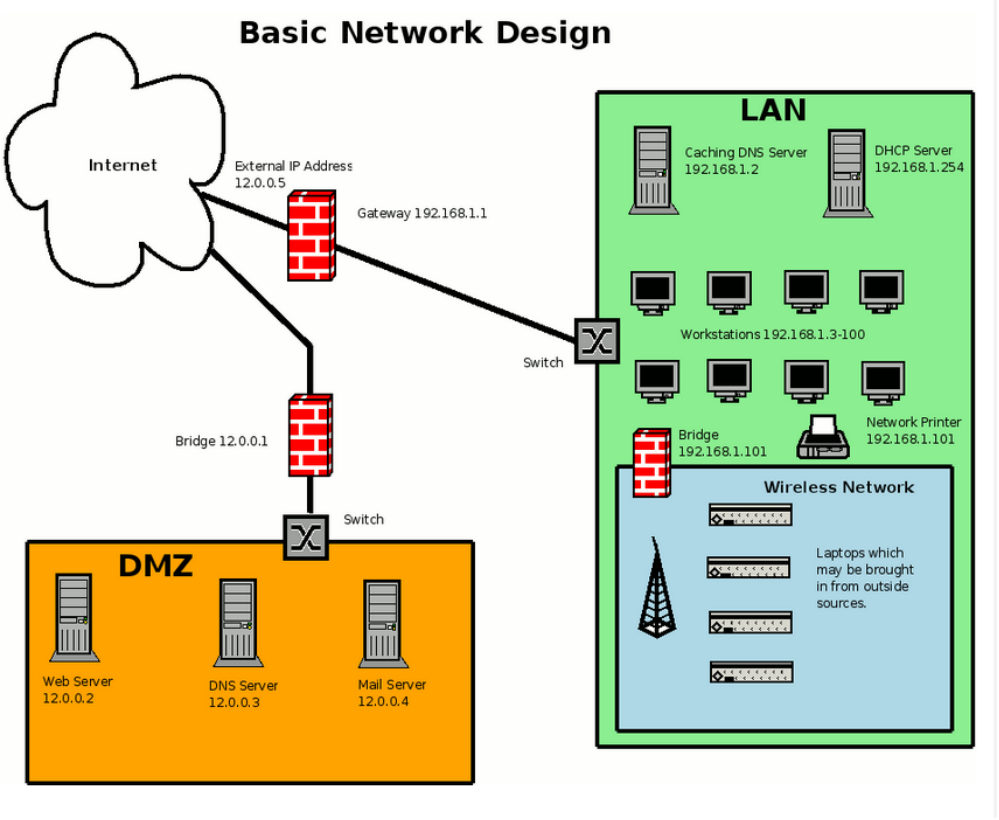


Figure 10. Sample network design [43]

This is not meant to be a "how to" on network design. This is a simple example of one possible network configuration and a brief summary of what each element entails. The gateway connects two dissimilar networks, such as the internet to the LAN (local area network) and the DMZ (demilitarized zone) which are on different networks [43]. The LAN is the area where the business' computers are located and is separate from the public network. The Caching DNS Server caches frequently accessed sites by the LAN, which allows the faster access to the resources [43]. The DHCP Server gives out IP addresses to workstations, printers, and the wireless network that allows mobile devices to connect to it [43]. The DMZ is a network that the business will use to keep public accessible servers, such as a web server (hosts the business' website), dns server (dns servers will be located on different subnets to provide backup for mail and web service), and mail server (so the business can send and receive email) [43]. The bridge

will filter MAC addresses, addresses from network cards, and iptables rules [43]. The switch separates machines so that information intended for a specific machine does not go other machines on the network, which helps increase security of the LAN [43].

Summary

Network security is a very important aspect of small business security. Several changes can be made with equipment that is already being used by the business. An administrator can log into the router and make several changes that increase the security of the network by changing the default username and password, using WPA2 encryption, disabling the SSID and WPS, using a firewall and creating a guest network. The use of VPNs will help remote employees securely connect to the company network to access company resources. Unified threat management attempts to link all network security concerns into one central management console. This may make it easier to manage the security resources, however care must be taken to have a backup plan in case the console fails and disrupts the entire business' network. A business can opt to use an MSSP that would handle its network security. MSSPs should be carefully chosen based on the needs of the business.

Chapter 6: Summary

Any computer or network that is connected to the public internet can be vulnerable to attack. There isn't one suggestion in this paper that will prevent this from happening. However, utilizing the suggestions given will increase the security in small businesses. Secure passwords will help prevent unauthorized access. Educating employees on how to safely use the internet and email will help prevent attacks. Computer security will also help prevent attacks, whether they are from insiders or outsiders. Securing data by using encryption is a good idea for sensitive information. Making regular backups will help a company retrieve its information in case of a breach or disaster. Securing the network will prevent intruders from gaining access to a company's network and its data. All of these topics are important for small business security. Suggestions provided in this paper should be the baseline for small business security. Any attacker can look up and see that these are the most common issues for small businesses and they can use this information to plan attacks. Small businesses need to be proactive and implement these suggestions before they are attacked. Future research can be done to find alternatives for each chapter. For example, an alternative to passwords would be a good area to concentrate on, since the current password format continues to be problematic. Research can also focus on more advanced topics for small business security. An intermediate guide would be useful for small businesses that are already utilizing the suggestions in this paper.

References

[1] Federal Communications Commission. (2011, May 16). *Cybersecurity for Small Businesses* [Online]. Available: https://www.fcc.gov/cyberforsmallbiz

[2] Shirley Radack. (2009, November). *Cybersecurity Fundamentals for Small Business Owners* [Online]. Available: http://csrc.nist.gov/publications/nistbul/Nov2009_smallbusiness.pdf

[3] Paul Mah. (2013, December 4). *8 Tips to protect your business' wireless network* [Online]. Available: http://www.pcworld.com/article/2068442/8-tips-to-protect-your-business-wireless-network.html

[4] Natale Goriel. (2013, October 17). *9 Cyber Security Tips for Small Business Owners* [Online]. Available: http://www.sba.gov/blogs/9-cyber-security-tips-small-business-owners

[5] Mcafee. (2012). *Combating Small Business Security Threats: How SMBs Can Fight Cybercrime* [Online]. Available: http://www.mcafee.com/us/resources/white-papers/wp-combating-smb-threats.pdf

[6] Ramon Ray. *8 Tips to Protect Your Business and Secure Its Data* [Online]. Available: http://eval.symantec.com/mktginfo/enterprise/other_resources/b-8_tips_protect_your_business_secure_data.en-us.pdf

[7] Mindi McDowell, Shawn Hernan, and Jason Rafail. (2013, February 06). *Choosing and Protecting Passwords* [Online]. Available: https://www.us-cert.gov/ncas/tips/st04-002

[8] Chris Hoffman. (2014, April 25). *HTG Explains: Should You Change Your Passwords Regularly?* [Online]. Available: http://www.howtogeek.com/187645/htg-explains-should-you-regularly-change-your-passwords/

[9] Bruce Schneier. (2010, November 11). *Changing Passwords* [Online]. Available: https://www.schneier.com/blog/archives/2010/11/changing_passwo.html

[10] Bruce Schneier. (2014, March 3). *Choosing Secure Passwords* [Online]. Available: https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

[11] Seth Rosenblatt. (2013, May 23). *Two-factor authentication: What you need to know (FAQ)* [Online]. Available: http://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/

[12] United States Computer Emergency Readiness Team. (2013, June 24). *Risks of Default Passwords on the Internet* [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA13-175A

[13] Chris Sullo. (2014). *Default Passwords* [Online]. Available: https://www.cirt.net/passwords

[14] Brian Krebs. *Password Do's and Don'ts* [Online]. Available: http://krebsonsecurity.com/password-dos-and-donts/

[15] Small Hadron Collider. (2014). [Online]. Available: https://howsecureismypassword.net/

[16] Will Dormann and Jason Rafail. *Securing Your Web Browser* [Online]. Available: https://www.cert.org/historical/tech_tips/securing-web-browser-index.cfm

[17] Mindi McDowell. (2007, June 20). *Browsing Safely: Understanding Active Content and Cookies* [Online]. Available: https://www.us-cert.gov/ncas/tips/st04-012

[18] Symantec. (2014). *Secure Your Email* [Online]. Available: http://us.norton.com/security_response/secureemail.jsp

[19] Apple. (2013, August 2). *Identifying fraudulent "phishing" email* [Online]. Available: http://support.apple.com/kb/HT4933

[20] Randall Sutherland. (2014). *Email Encryption Software Review* [Online]. Available: http://email-encryption-software-review.toptenreviews.com/

[21] Ciprian Adrian Rusen. (2014, April 7). *Lesson 1: User Accounts, Groups, Permissions & Their Role in Sharing* [Online]. Available: http://www.howtogeek.com/school/windows-network-sharing/lesson1/all/?PageSpeed=noscript

[22] Redhat. (2014). *Introduction to System Administration* [Online]. Available: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/4/html/Introduction_To_System_Administration/ch-acctsgrps.html

[23] University of Illinois. (2014). *Updates and Patches* [Online]. Available: https://security.illinois.edu/content/updates-and-patches

[24] Margaret Rouse. (2005, September). *antivirus software* [Online]. Available: http://searchsecurity.techtarget.com/definition/antivirus-software

[25] Sans Institute. (2001). *Why Small Businesses Need to Secure Their Computers (and How to Do it!)* [Online]. Available: https://www.sans.org/reading-room/whitepapers/basics/small-businesses-secure-computers-and-it-441

[26] Microsoft. (2014). *Windows Firewall* [Online]. Available: http://windows.microsoft.com/en-us/windows7/products/features/windows-firewall

[27] Purdue University. (2011, December 28). *Mobile Devices* [Online]. Available: http://www.purdue.edu/securepurdue/bestPractices/mobileDevice.cfm

[28] Cory Janssen. *Endpoint Security* [Online]. Available: http://www.techopedia.com/definition/3165/endpoint-security

[29] Mike Williams. (2013, August 28). *Best business antivirus: 8 top paid security tools for small business* [Online]. Available:

http://www.techradar.com/us/news/software/applications/best-business-antivirus-8-top-paid-security-tools-for-small-business-1170097

[30] Jeff Tyson. (2001, April 6). *How Encryption Works* [Online]. Available: http://computer.howstuffworks.com/encryption.htm

[31] Alex Castle. (2013, January 18). *How to encrypt (almost) anything* [Online]. Available: http://www.pcworld.com/article/2025462/how-to-encrypt-almost-anything.html

[32] Paul Mah. (2013, October 1). *4 ways to disaster-proof your data backups* [Online]. Available: http://www.pcworld.com/article/2050337/5-ways-to-disaster-proof-your-data-backups.html

[33] Chad Brooks. (2013, May 31) *Online Data Backup: A Small Business Guide* [Online]. Available: http://www.businessnewsdaily.com/4565-online-data-backup-guide.html

[34] Chris Snoke. (2014). *Business Online Backup Services Review* [Online]. Available: http://business-online-backup-services-review.toptenreviews.com/?cmpid=ttr-bnd

[35] Margaret Rouse. (2014, June). *unified threat management (UTM)* [Online]. Available: http://searchmidmarketsecurity.techtarget.com/definition/unified-threat-management

[36] Fortinet. *Managed Security Service Providers (MSSPs)*[Online]. Available: http://www.fortinet.com/partners/alliances/managed_security_service_providers_mssps.html

[37] Eric Geier. (2012, February 14). *How to Choose a Router for Your Business* [Online]. Available: http://www.pcworld.com/article/249954/how_to_choose_a_router_for_your_business.html

[38] Eric Geier. (2009, July 21). *Tips to Secure Your Small Business Wi-Fi Network* [Online]. Available: http://www.ciscopress.com/articles/article.asp?p=1377835

[39] Wigle.net. (2014). *SSID Stats (top 1000)* [Online]. Available: https://wigle.net/gps/gps/Stat

[40] Sean Michael Kerner. (2011, June 02). *10 Network Security Steps for Every Small Buiness* [Online]. Available: http://www.smallbusinesscomputing.com/webmaster/article.php/3935021/10-Network-Security-Steps-for-Every-Small-Business.htm

[41] Jeff Tyson and Stephanie Crawford. (2011, April 14). *How VPNs Work* [Online]. Available: http://computer.howstuffworks.com/vpn.htm

[42] Wana Tun. (2014, October 03). *Dispelling Common Myths Surrounding UTM* [Online]. Available: http://www.cso.com.au/article/556595/dispelling-common-myths-surrounding-utm/

[43] Mike. (2010, June 3). *Network Design for a Small Business* [Online]. Available: http://beginlinux.com/blog/2010/06/network-design-for-a-small-business/