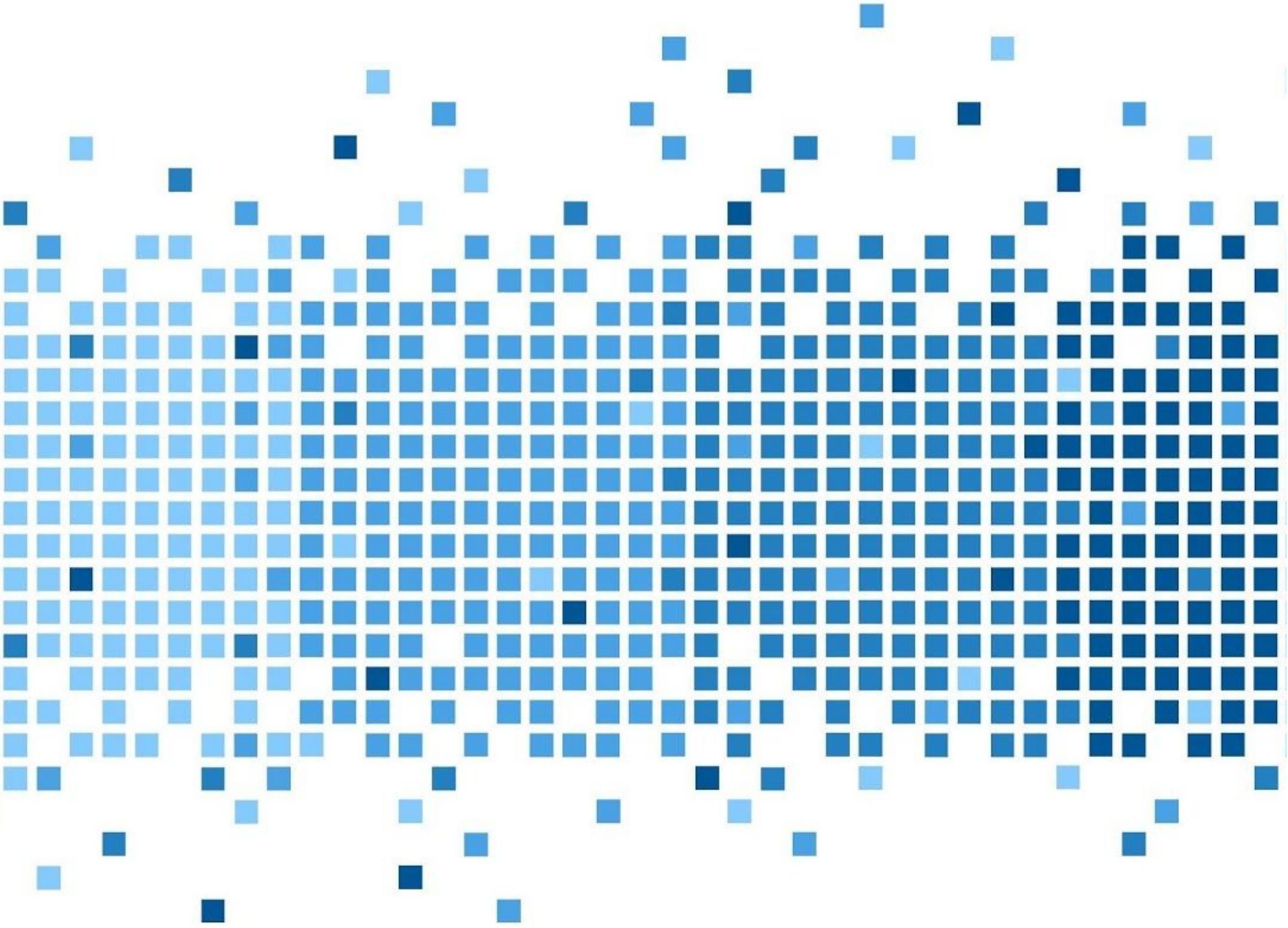
CHAMPLAIN COLLEGE | LCDi Leahy Center for Digital Investigation

Online Small Business Security



175 Lakeside Ave, Room 300A
Burlington, Vermont 05401
Phone: (802) 865-5744
Fax: (802) 865-6446
http://www.lcdi.champlain.edu

12/14/2018

Disclaimer

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

Contents

Introduction

The Online Safety/Security team from the Leahy Center for Digital Investigation (LCDI) researched online safety and cybersecurity tips for small businesses, particularly in Vermont. As many businesses rely heavily on technology, the need and awareness for tighter online security is increasing to prevent the threat of attacks or exploitations made by cybercriminals. As of September 2018, it was reported that three businesses fall victim to ransomware every two minutes across the nation ("New Data Shows"). Vermont has been targeted by a multitude of cyber attacks in the past years, such as ransomware, phishing attacks, software penetration, and other common viruses. Cybercrime costs businesses worldwide over $600 billion in damages annually, which is a statistic that can hopefully be decreased through greater awareness about the need for cybersecurity ("New Data Shows"). This research intends to inform and educate small business owners about the cyber threats that have become more imminent in the past years.

Background

Small business security has emerged as an important topic in cyber-safety recently because of many cyber attacks that exploit the vulnerabilities of small businesses, such as an attack in May 2017 on Arrow Tech -- a local defense contractor located in South Burlington, Vermont. In 2017, the FBI published a report, the *IC3 2017 Internet Crime Report*, outlining the importance of public awareness, including maintaining security over "files containing financial accounts, passwords, and personal data, like health records, social security numbers, and tax information" ("iC3"). McAfee security representative Gary Davis explained the importance of updating devices in order to patch known vulnerabilities (Davis), and small business security expert William Deutsch clarified that no matter how secure the digital aspect of a system is, physical security is still just as, if not more, important (Deutsch).

Lemonnier explained that many small businesses in Vermont have also fallen victim to ransomware, a type of malware that holds business' data hostage in exchange for money or ransom, trojans, a malware that disguises itself as legitimate software, spyware, a malware that spies on the actions on a device, and other malicious viruses (Lemonnier).

Purpose and Scope

In this research, we address information security including how to virtually and physically secure a small business's network and information. We inform small businesses about the dangers of unprotected networks and how to avoid and respond to attacks a small business might experience. The research we conducted is applicable to help strengthen the security of Small Businesses and to implement useful security suggestions.

Terminology

Antivirus - Software that detects and removes virus-infected files as well as potentially unwanted programs from a computer ("Antivirus").

Bandwidth - The maximum data transfer rate of a network or Internet connection. It measures how much data can be sent over a specific connection in a given amount of time ("Bandwidth").

BIOS - "Basic Input Output System" of a PC. This is usually a number of machine code routines that are stored in ROM and are available for execution upon startup, containing commands for reading the physical disk sector by sector ("BIOS").
Client - "A device that is connected to a network is referred to as a client" ("Client").
DDoS - A Denial of Service Attack that attempts to make a particular machine or network resource unavailable to intended users by two or more clients ("Distributed Denial of Service").
Dynamic Host Configuration Protocol (DHCP) - A client/server protocol that provides an IP address. ("Dynamic Host Configuration Protocol").
Firewall - Network security device that regulates network traffic that gets filtered through the network, using security rules to block or allow the specific traffic ("What is a Firewall").
Firmware - A program what is permanently installed into the hardware of a device ("Firmware")
Gateway - A hardware device that serves as a pathway between two networks ("Gateway")
Internet Service Provider (ISP) - A provider of access to or connection to the internet ("Internet Service Provider")
IP Address - An electronic identifier for a specific computer or device on the World Wide Web or any other network ("IP Address")
Malware - Any malicious software that is used to interrupt computer operation, gather information, or gain access to systems. ("Malware")
Network - A group of computers linked so they are able to share files, services, or other resources ("Network")
Packet Sniffer - Also known as protocol analyzers. Packet sniffers are tools used to monitor network traffic and diagnose network problems (O'Donnell)
Phishing - A fraudulent Social Engineering technique, where the attacker will act like a reputable source or individual through emails or other forms of communication (Rouse)
RAM - (Random Access Memory), An integrated circuit into which volatile data can be read or written by a microprocessor or other device ("Random Access Memory (RAM)")
Ransomware - A certain type of malware that denies access to data in the attempt to extort money from an individual/company ("Ransomware & Cyber Blackmail")
Remote Access - The ability to log in to a computer from another computer. ("What is Remote Access")
Social Engineering - Non-technical techniques intent to lure users to sending them personal information, confidential data, money, or to letting the users to allow them to infect their computers with malware ("Social Engineering")
Trojan Horse - A malicious program disguised as a reputable progamed. Usually, carried out by social engineering ("Malware")
Virus - A malware program that when executed will place itself into other computer programs or data files. Viruses can perform various harmful activities ("Malware")
VPN - Extends a private network across a public network (Poladian)

Updates

Each workstation, including its operating system and software, needs to be updated regularly to prevent holes in security from encouraging any kinds of attacks. By controlling the updates of each computer, the system administrator can regulate and maintain better security for the entire enterprise. There are several steps pertaining to updates and software regulation that one may take in order to increase the overall security of both individual computers and entire networks (Davis). Updating any mobile applications and devices that are affiliated with the business, hold sensitive information, or are connected to the business' network are also important steps to keep in mind to harden the security of the network.

Several aspects of a computer need to be maintained with up-to-date patch versions, including the operating system, web browsers, software, and anti-spyware or antivirus programs (de Saxe). The purpose of updates is to patch any potential bugs and vulnerabilities in older versions that may be exploited by attackers. There are sources online where users post known exploitations of any program, and by updating these programs to patch the known vulnerabilities, the business would significantly diminish the possibility of becoming victim to cyber attack (Davis). In 2017, a credit-report company called Equifax revealed an illegitimate access to its database, known as the Equifax Data Breach. The breach exposed the Social Security numbers, drivers licences, birth dates, and home addresses of over 148 million Americans as a consequence of a known vulnerability in the agency's web application (Davis). By not taking the few minutes to update the company's network-data inspection system, the system administrator caused significant damage to the agency and a leak of information of millions of people (Fleischman).

New threats are constantly developing and evolving, so frequently running updates on anti-virus applications in addition to normal software remains vital. Anti-virus applications are meant to detect the presence of viruses or malware in a system, so keeping them as up-to-date as possible would keep them equipped with the necessary tools and information to stop attacks from newer malware.

Web browsers act as gateways between the internet and the work machine. Frequently, viruses and cyber attacks are performed through the internet, getting spread through unsecured downloads or unsafe webpages, so a web browser should be equipped to handle the threat of potential attacks. The best way to do so is to maintain the most frequent available versions of the browser, which may be found usually on the top-right corner of the browser interface, under Settings. Often, the browser will notify the user when a new update is available.

Other fronts that remain important to update include mobile devices and applications. Nearly every employee introduces personal devices into the workplace and often connect to the company's network, which provide a new gateway into the company. Similarly to the applications on a computer, the apps on a mobile device need to be secured and updated; a vulnerability in such apps may create a path to inject malware into a network that may affect the rest of the company, its employees, and its information. Furthermore, the operating systems of the mobile devices need to be updated as frequently as new updates come available for similar reasons.

Additionally, it becomes easier for the system administrator and the other users to keep devices and applications up-to-date by enabling auto-updates. These tasks implement when a new update becomes available for the given piece of software or firmware, providing users with the most frequent checks in security with little work done. However, hackers can remotely disable these automatic updates once in a system, which weakens the power of the user and the security of the system; "you could face an inside attack and have your antivirus software turned off manually… [meaning that] hackers and cyber criminals have easier access to your computer while also having the ability to roam freely" (de Saxe). Hence, it is important to routinely check that antivirus is enabled and that the most recent versions of software and applications are installed (de Saxe).

Backups

Backing up Data

A backup is when a system administrator copies a set of data--such as a hard drive of a machine--onto another secured drive to keep data secured in the event of a system breach. To better protect data, files, and software information, companies should consider creating backups of systems routinely. This way, in the event of a potential system failure or drive crash, the backed up data in an external location would not be damaged ("Backing Up Files"). Backups are essential parts to protect important data safe from catastrophes such as hard drive crashes, corruptions, or natural deterioration, network crashes, cyber attacks, or computer overflows ("Backup: Your Most Important Task"). Different types of external backups are available to suit each business' needs based on space and functions needed and funds available. Especially with the greater affordability of external local storage, it is made easier to back up essential data to avoid the risks of being attacked, corrupted, stolen, or lost ("The importance of data back-up").

Before considering how to back-up data, it is important to consider how much data the company will need to store. Full backups allow the user to backup all data from one system into another location; they optimize restoration time and availability of the system in exchange for more needed space and increased initial backup time. Differential backups only back up the data changed since the last full backup, making them slower and more redundant. Incremental backups are similar to differential backups, in that they back up the data that has been updated or changed since any other backup occurred, including the last full backup, incremental backup, or differential backup, making backup time more time and space efficient. Both differential and incremental backups provide faster execution and less space requirements at the cost of having slower data-recovery-time ("Types of Backup"). Given the resources available to the company, the system administrator may determine the most efficient types of backup for the system, taking into consideration the available space, time restraints, reason for the backup, and amount of data that needs to be backed up ("The importance of data back-up").

Several types of platforms exist with which a company may back up data, depending on the amount, type, and necessary security of data and availability of funds.

Cloud backup is one very common way to store data; since it is at an off-site location, it protects information from compromised facility as it stores data on a "cloud" service, such as the internet, rather than on a physical drive. Usually, online storages only offer 5GB of free storage, with more space available at a greater cost.

Online backups work best with smaller amounts of data and when used over internet connection; however, online backups are not optimal for private or sensitive data, as they are reliant on third-party applications or companies to store the data (Ngo). Some operating systems offer cloud syncing and backup services, such as Microsoft's OneDrive application, equipped on most Windows machines, or Apple's Time Machine application, available for Macintosh computers. Other companies offer cloud storage at little to no cost, such as Google Drive, Dropbox, Backblaze, Carbonite, iCloud, and CrashPlan (Nield).

There are also several options for local backups, ranging through the use of external solid state drives (SDD), external hard drives (HDD), or even flash drives. Other possible options include CDs, DVDs, or Blu-ray. These drives typically hold a limited storage space, depending on the device, so system administrators need to gauge the practicality of using one form of drive over another.

Backups Vs Redundancy

Compared to backups, "redundancy" is a different approach to having a safetynet for company data. Consumer-grade redundancy may be described as "digital storage means using more internal drives than necessary to store the information, or in other words, storing the same data in more than one place" (Ngo). The purpose of redundancy is to have an available way to ensure and recover the data in the case of a disk failure. The most popular redundancy setup uses "Redundant Array of Independent Disks" (RAID); it provides insurance, depending on the type of RAID implemented, that multiple hard disks are available to backup data despite several disk failures (Ngo).

The pros of redundancy are that it "protects data against drive failure in real time… [while] offering an immediate type of data protection" (Ngo). Drive failures can happen at any time, especially since drives and their information are susceptible to attack, so it remains important to implement redundancy or RAID to save company data from an unexpected drive failure. The cons of redundancy are that they may be costly to a company. For example, in order to set up a RAID system, a company would need to purchase multiple drives, rather than only one. Furthermore, redundancy does not protect against physical damage. Physical damages, such as a fire or flood in the business facility, may harm all the drives and yield the data on them irretrievable. Another con is the amount of time needed to initialize redundancy; the redundancy system needs to parse through the existing storage and make copies of everything, making the initial setup take a longer time (Ngo).

The 3-2-1 Rule

The 3-2-1 Rule approach to data storage and backup systems introduces an efficient way to implement security over data. It is broken up into three aspects that strengthen security of the data a company may wish to back up.

3: Keep *three* copies of important data (One primary, two backups)
All types of computer storage eventually fail. This includes hard drives, SSDs, flash drives, etc. "There isn't a means of storing computer data that's absolutely infallible" (ExplainingComputers 00:59-01:03). This is why companies need to have multiple copies to protect data from the potential of drive failure.

2: Save the files on *two* local types of media

Hard drives are susceptible to mechanical problems, whereas optical media tend to deteriorate over long periods of time from simple wear-and-tear. When storing data, it is recommended to have two of the three copies saved on local mediums, preferably read-only devices (Yev). Having different types of media helps protect against different types of damage (ExplainingComputers 02:29-03:00). Keeping these storage devices on-site is efficient because it allows quick replacement of drives if necessary with minimum data loss (Yev).

1: Store *one* copy off-site (this can include online)
Physical dangers, such as theft, flood, and fire, remain as threats to external drives kept on-site just as they pose a threat to the drives in the computer, which is why companies are encouraged to keep the third external drive to be kept off-site. At least one copy of data should be physically separated from the other copies, such as through the process of taking a hard drive or flash drive to a separate location out of the office, or using a cloud service to store data online (ExplainingComputers 03:00-04:30).

Network Information

Networks hold a great importance when maintaining security over a business of any size. A breach in the company's network can impact the entire system, opening the floodgates for attacks to be administered through wireless networks to each workstation connected. Therefore, it remains vastly important to secure the network and its assets to protect business and personal information on the system.

Network Accounts and Settings

Network accounts are the first place to start to secure the network from intruders. The first step is preventing any non-employee from having access to the company's network by creating a guest network for visitors and customers. The public network should not hold or be connected to any sensitive or company information, and taking this precaution may dramatically decrease the chance of an internal attack. Such guest account may be paired with a login page that requires credentials from the users who sign in, including an area to input the user's name, email, and phone number, and it should also incorporate a two-step authentication to verify the email or phone number that they entered. The guest login should also include a time-out period of 24-hours, after which the user's information must be re-entered to ensure security for that account as well. The user information collected through this login may be stored in a database to trace back potential attacks.

Maintaining proper maintenance over the router and its corresponding firmware is important to keeping the network safe. Precautions may include hiding or resetting the network name (SSID) and password from the default given to the router. Network administrators may consider implementing Active Directory authentication which allows users to log in to Secure Global Desktop and offers users a faster and more secure authentication method when signing into a network, a common practice for many companies ("Active Directory Authentication"). The process may vary, but the general procedure includes logging into the ISP's router login page, navigating to the wireless settings page, entering the router's username and password (if applicable), then entering the new name and password ("How Do You Change a Router"). This should be done sooner rather than later, preferably as soon as the router is set up. Furthermore, the router typically serves as the network gateway that joins networks, effectively allowing devices and systems to access the internet ("The Definition of Network Gateway"). It is possible to change the gateway IP using DHCP to automatically re-assign the IPs of the computers on the network to protect their locations (Simmons).

Companies may wish to keep a log of all users that connect to any network within the facility to provide evidence to investigators in the case of a breach.

VPNs

VPNs are a useful security tool for businesses because they allow for different sections of a business to share information over long distances while remaining secure. This connection is accomplished by creating a "tunnel" between the user and the destination by placing packets of data that are being sent into other packets, effectively disguising them before sending them (Poladian). Should someone recognize and intercept the packet, they would not be able to read it easily because of another layer of VPNs which involves encrypting all the data being sent via these packets. Finally, VPNs mask the IP address of the sender, hiding them from attackers who may want to steal the data (Beal).

Setting up a VPN is not as complex a process as it may seem. A normal VPN costs around $7-$10 initially, with additional monthly or annual charges, summing to around $40/year (Mason). After this, system administrators must select a protocol; one of the best options would be OpenVPN because it is very secure and moderately fast, but it can be a little more complex to set up (Smith). PPTP is one of the faster protocols and easy to set up, but is widely considered insecure. L2TP is easy to set up, fairly secure, but not the fastest. IKEv2 tends to be fast and easy to set up while remaining secure, and is generally considered a good choice. For further assistance setting up the VPN, users may refer to online tutorials, product documentation, or contacting the provider of the VPN.

Additional issues with VPNs include a loss in performance and additional network costs. Performance is lost in connectivity speed; each time a user tries to connect to a website, the VPN has to first connect him or her to a private server, then to the website. When compared to browsing normally, there may be a noticeable decrease in speed. The next major disadvantage can come about if an unreliable free VPN is chosen, which may lead to a loss in anonymity. A lot of free VPNs actually trade their service for a user's data, potentially selling the information or browsing habits of their users with other companies without explicitly telling the user. As previously discussed, another drawback is the annual price to maintain a VPN.

Social Engineering

One underestimated aspect of business security is knowledge of Social Engineering. Employees should be wary of tactics utilized by hackers such as phishing scams, tailgating/piggybacking, shoulder surfing, and impersonation. These are some of the most common ways businesses are infiltrated and taken advantage of ("Security Tip").

Should an employee receive a email that seems strange or out of place, that email must not be opened. Following any links or opening any files within the email should be avoided at any cost, especially those that suggest to change or confirm passwords, or other information; suspicious emails must be deleted, with the trash being emptied afterward. Instead, if a user wishes to change or check the information from the source allegedly sending the email, it would be more secure to search and log on to official websites rather than following attached links. If it is uncertain whether or not an email is to be trusted, users should contact the supposed sender to verify it or communicating with the office manager before proceeding ("Social Engineering"). A company can use an email filtering system and/or a virus scanner to help combat untrustworthy emails and spam.

Phishing scams are one of the most dangerous social engineering ploys. An example of a phishing technique is a phone call scam where attackers claim to be the IRS over the phone and state, "the individual owes the Federal Government funds due to a tax audit, or mistake in back taxes," when in reality, the victim does not necessarily owe money to any such organization (Henry). These attacks can be done through phone, email, text, or any means of communication. Even giving out marital status in these phishing scams can be detrimental. To avoid these scams, users must not give out any information that could be tied to a person's profession, personal, or family life to protect the privacy of one's family and personal life (Henry).

Another facet of Social Engineering would be the ways intruders physically gain access to the system. Attackers could do this by "piggybacking," or tailgating, someone into a facility; this entails following someone into a room that he or she should not be able to access. The authorized individual may hold the door open to be polite, while the intruder enters the room without verifying his or her identity, after which they have full access to the facility to retrieve business information, passwords, or sensitive data, inject viruses into workstations or the network, or break, corrupt, or damage equipment. Another method of Social Engineering that may take place within a facility is called "shoulder surfing," where a malicious individual searches an employee's desk or looks over the employee's shoulder onto their computer screen to retrieve passwords or other important information. To prevent these attacks, employees must know not to let potentially unauthorized people into the building without identification, and to store sensitive data mindfully so to not expose it to pass-byers (Henry).

Finally, Social Engineers may pretend to be trusted parties to manipulate users, a technique known as "impersonation," similar to Phishing. Individuals must be careful with unexpected phone calls or texts that request information and receive confirmation on the identity of the questionable sources, while abstaining from providing passwords or other information over phone, text, email, or other fashion ("Security Tip").

Malware

Virus

A virus is a type of malware that is executed when it is inserted into other computer programs or computer data files. Once in the system, the virus performs harmful activities, such as stealing hard drive space, wasting CPU time, stealing private information, corrupting data, or gaining administrative access in a network ("Malware").

Viruses encompass a broader term of malicious software, including worms, which can replicate themselves with the help of an outside source (Cooper). Viruses may infect a computer via email and text message attachments, downloads, scam links on social media, and application downloads ("What is a Computer Virus").

The most common function of viruses is the illegal copying of data (Cooper), but other examples are the resident virus (e.g. CMJ, Meve, MrKlunky, Randex), which would live in the RAM of the computer system it is occupying. It corrupts files and programs, making them unusable. Another type of virus is a multipartite virus, which easily spreads throughout the computer system and performs unauthorized actions on the system. These viruses can infect programs. Encrypted viruses use malicious codes to block the antivirus' ability to detect the virus. The viruses are only able to be detected when they unencrypt themselves to replicate inside the system they already infected. Luckily, they do not delete files on the computer system, but hey do lower the computer performance greatly. The FAT virus ruins the file allocation system, where the files and their information are stored. Directory viruses alter file paths, so when the programs run, the virus also runs in the background. Directory viruses make locating the original application once the system has been infected difficult (Hernandez).

To determine whether a computer system has been infected with a virus, check for frequent pop-up windows encouraging the users to visit odd sites or download antivirus systems, changes to homepages, mass emails (i.e. email bombs), frequent crashes on the computer system, unusually slow computer performance, unknown programs start appearing once the computer system turns on, and unusual activities (e.g. password changes). In order to avoid being infected by a virus, antiviruses are imperative along with not clicking or downloading from unknown sources ("What is a Computer Virus").

Trojan Horse

A Trojan Horse is malware that is disguised as legitimate software as a masquerade. Often, one is obtained by posing to be a desired application on an untrustworthy source, waiting to be installed into the victim's computer. Trojan Horses make the computer more vulnerable to future attacks and can even make a network of infected computers used for criminal purposes ("What is a Trojan Virus?").

To avoid getting Trojan Horses, only download software from recognizable, legitimate sources. Do not open any email attachments from unrecognized emails; even images can hold Trojan Horses. Delete any emails that urge users to download something and permanently delete the email from the trash folder ("Avoiding a Trojan Virus").

If a computer is suspected to have been infected with a Trojan Horse, there are some key symptoms of their presence on a system. First, if the computer greatly slows down and gets pop-ups and ads often, it is probable that it has been infected. Also, if new programs or applications are installed without permission, the homepage or default browser has been changed, or strange emails and texts are sent from a user's account without the user doing it, the system has likely been infected ("How Can I Know"). While these are not the only signs of a Trojan Horse, these are the most noticeable and most common effects they have on a network.

If a computer has been infected by a Trojan Horse, check to make sure that all recently downloaded items have come from a legitimate source. If they have not, boot the computer into safe mode. On Windows 10, hold “Shift” and click “Restart” from the menu in the bottom left corner of the screen. For earlier versions of Windows, while restarting the computer, repeatedly press F8 and select “safe mode” when prompted. When in safe mode, click “add or remove programs”, and remove recently downloaded programs that have come from untrustworthy sources, then restart the computer (Geier). If it is unclear which installed programs are the source of the Trojan Horse, download an antivirus and perform a full system scan of the computer. It should detect the source of the virus, and it can be removed. If the antivirus cannot detect the source of the virus, another option is to perform a factory restore. Note that all files will be permanently lost if this is done. If a factory restore must be done, try to back up as few files as possible. Any file could be infected with a Trojan Horse, and backing up more files only increases the possibility of the computer being infected once more.

Ransomware

Ransomware is a type of virus where data is made inaccessible or stolen and a ransom must be paid to regain access. It is most commonly used to make the following data inaccessible: credit card and account information, contact information, and files like pictures or videos (Lemonnier). The attacker goes after such information because they hope it is important or sentimental enough that the victim will pay the fee without question.

To prevent ransomware attacks, train employees to have safe computer habits. Have them abide by strict email policies. Train them to be aware of the dangers of phishing (see: Social Engineering) and to be cautious of what they use their email for. Prevent employees from using their work email to sign up for deals or shopping newsletters. Keep computer systems updated and either replace or review firewalls every five years. Lastly, keep full backups of data offline and disconnected from the network (Lord). That way, if the system is compromised, the backups would not be at risk as well.

When responding to ransomware, companies and individuals should contact a legal team before taking action. It is impossible to gauge the intentions of the attacker, as they may continue further blackmail or refuse to return data; copies of data may be made, and there remains the threat of disclosure of the copies unless more money is transferred (“Ransomware - What is It”). Generally, companies should not pay the ransom, as advised by the FBI, including hospitals and healthcare agencies in addition to smaller businesses (“Ransomware”). Once the hacker is dealt with by professionals, system administrators should configure permission rights on the computer, implement Software Restriction Policies (SRP) or Controlled Folder Access to prevent ransomware to execute, and run anti-malware or antivirus programs such as Malwarebytes to remove the ransomware. Furthermore, it is important to report the incident to the Attorney General’s office no later than 45 days after the discovery of the breach if law enforcement is required, as mandatory in the state of Vermont (“Privacy and Data Security”).

Installing Malware

Nearly every instance of malware on a computer or system is the product of human error; more likely than not, malware gets installed as a result of a user clicking on a link or email that carries the malware from another malicious user (Grimes). This is the case for most viruses, Trojan Horses, ransomware, and other types of malware. As a result, these malwares are hidden within the files of the computer, often disguised as benevolent software, after which, they wreak malicious activity, such as stealing information, deleting computer data, locking user data or programs, copying personal information and credentials, allowing remote access to malicious users, and more.

One may choose to routinely check any new software on his or her computer to find disguised malware. In order to check the questionable software on a computer, one may choose to use online resources such as https://www.shouldiremoveit.com/ to search and check programs that may seem unfamiliar.

Types of Attacks

DDoS Attack

Distributed Denial of Service (DDoS) is a special kind of denial of service attack where multiple IP addresses attack a single server to overload its bandwidth and hinder performance. The purpose is to make a certain machine or network unusable or unavailable to regular users ("Distributed Denial of Service"). Denial of Service is using one IP address to attack a server instead of multiple addresses to bring down a system or a service, acting as a "traffic jam" for any incoming requests. A DDoS attack tends to be very hard to prevent, as the server is flooded with pings from multiple IP addresses of different locations, reflecting in the performance of a system undergoing the attack ("What is a DDoS").

To prevent being a victim of DDoS, network administrators should apply a spam filter on company websites and monitor traffic on the router frequently. The company may wish to purchase extra bandwidth to accommodate for traffic disabling the network or website and to yield more reaction time in the case of an attack.

To see if a system is undergoing a DDoS attack, system administrators should look for large spikes in traffic and slow connection speeds to web servers (Rubens). It may also be apparent if the website receives high amount of spam emails or becomes disabled ("Distributed Denial of Service"). In order to respond, ban IPs that are trying to access the website too quickly or call the ISP if there is an apparent attack. If the attack gets out of hand and the prevention measures do not mitigate the situation, call a DDoS mitigation specialist (Rubens).

Man-in-the-Middle Attack

A man-in-the-middle attack (MITM attack) consists of three individuals: a victim who is trying to communicate with another, the intended receiver of the conversation, and the attacker who is intercepting the messages. However, the key is that the victim has no idea of the last individual—the attacker ("What is a man-in-the-middle attack"). An MITM attack is very similar to if the mailman decided to open all of the paystatements before they were delivered, write down the important, personal information, and then deciding to mail it to the original individual it was meant to be delivered to ("Man in the Middle"). The attack requires either an unsecured or a poorly secured WiFi router, such as a public WiFi hotspot ("What is a man-in-the-middle attack"), or the attackers may create their own malicious WiFi hotspots to intercept the information sent—or rather "open the mail of the sender" ("Man in the Middle"). Next, to read the "mail", or the information being sent across the network, the attacker needs to decrypt it, which may be done through malware sent to the victim through phishing techniques ("What is a man-in-the-middle attack"), or phony websites ("Man in the Middle").

In order to prevent such an attack, all WiFi routers and modems should have their passwords changed from the default password. Employees should pay attention to which websites they are accessing and make sure the websites are secured (HTTP vs. HTTPS) and avoid using unsecure websites on company WiFi. Employees should especially be wary of entering personal information and clicking on email links from unknown senders, and when an application is not in use, employees should be instructed to immediately log out of the program ("Man in the Middle").

Brute Force Attacks

A brute force attack, also known as a dictionary attack, is one of the reasons why password security is so imperative. In such an attack, the perpetrator uses a trial-and-error method in order to procure password information, usually using an automated software that generates a substantial amount of consecutive guesses in order to obtain the data. By doing so, the attacker may be able to obtain encrypted data ("What is a Brute Force Attack"), steal valuable information, or shut the server/website down. Once they have the login credentials, the attacker may also infect the site with malicious scripts with other objectives beyond what is listed previously (Rehman). Even though brute force attacks tend to be very slow due to the style of the attack, the attack itself is very simple to perform and with enough given time they will almost always work ("Brute Force Attack").

However, the defense for this particular attack is relatively simple. The longer the password string, and the more complex it is, the longer it will take the hacker and the automated software to hack into the system and obtain their desired goal, and at a certain point it would be more beneficial to try to procure such information by other methods (see Man-in-the-Middle Attacks) ("Brute Force Attack"). To avoid such an attack, it is important to require certain password lengths from all of the employees and password complexities (see User Accounts), and also to limit login attempts to lockout the attacker. Businesses should also implement using a captcha to filter out machines and actual employees that are trying to log into their accounts, and use two-factor authentication (Rehman). It's also strongly suggested to lock out IP addresses that have too many failed login attempts that incorporates a delay into the automated software, which decreases the effectiveness and to not allow employees to recycle old passwords. Businesses should also encrypt all personal and sensitive data with strong encryption keys in order to dissuade such attacks ("Brute Force Attack").

User Accounts

User accounts are the interface between the user and the workstation. They hold information such as user-specific credentials, passwords, and information, while also giving each user access to computer services such as Web Browsers, Applications, and the business' local Network.

When creating user accounts for employees, the employer should have a unique default password that will direct the user to a prompt to change his or her password immediately. The employee then should create a password that follows proper password conventions, which include containing at least fourteen characters, a combination of both uppercase and lowercase letters, and at least one number and symbol; additionally, passwords should not include common words that can be found in a dictionary ("How to Keep Your Online"). The employer should also set up two step authentication for all employees, where the employee will receive a text or email with a passcode upon attempting to log in, so they can verify it really is them. Employers need to take extra precaution when firing a person who had administrative access to the network, as they may be vengeful and be a threat to the network; the employer should be required to delete accounts of employees who are no longer working for them.

System Administrators should require employees to change their passwords often; the business should have a maximum password "life" policy that requires employees to change user password between 7 and 28 days after it is updated. New passwords -- both for applications and system login -- should be unique, follow strong password conventions, and not have already been used on the system. Employees must not write passwords down anywhere that can be viewed publicly, such as on notepads or papers around the office for interest of physical security (see: Physical Security). Furthermore, System Administrators should arrange for user accounts to be locked out after three failed login attempts and have the account automatically log off when the system is inactive for ten minutes ("PASSWORDS DO's and DON'Ts").

If a user account does become compromised, meaning they have been hacked or another issue is present, a business will need to identify and secure the compromised account or accounts. First, they will need to suspend or lock the account. Then they need to investigate the account's activity through forensic programs such as *Prefetch*, LNK, WorkTime, etc. The administrative team should also reset the password to the account that has been compromised and consider backing up the important data from the drives. The security team should then run an Antivirus or Anti-malware program on the machine to solve the security breach; if the scan does not work to secure the account, deleting the User from the system may be a last resort. Some prevention tactics that will be useful to prevent future issues are to have very strong security questions for accounts, add recovery options for administrators, and to turn on activity alerts so administrators can see when suspicious activity is taking place ("Identify and Secure Compromised").

Remote-in Users

For remote in user accounts, there should be an extra layer of security. One way to have this extra layer is to require an additional password for when employees log in remotely. This additional password should change every time an employee tries to log in remotely and the employer will have the new password each time. Another way would be that employees have to request access to the system and the employer needs to allow them access to the system. These both ensure that there is careful attention to who can remote-in to the network and when. Any time that an employee remotes in, there must be a log of all their activity. This will be used in case of any issues with the account that may arise in the future and would be beneficial to the company's investigation of the account in the future (Richmond). VPNs are the best option to have a secure network for users that remote-in to work from home. Remote-in services are the most secure when they are internal and not external, internal being from work computer to another work computer and external being home computer to work computer.

To protect data from a system failure, the company needs to have a backup. Cloud services are a very good option for remote-in users. It hands off the security responsibilities to the service providers when remoting in and allows users to access data online from any location. But there is a large downside to this: the service provider can comply with subpoenas for the company's data. Some remote-in services that could be used are Windows Small Business Server, Cisco Anyconnect, Juniper Juno Pulse, or Remote Desktop Protocol/Connection (Richmond).

One major way to allow employees to remote in to their office from home is TeamViewer (personal version). The TeamViewer personal version is free for you to download. TeamViewer provides an easy to use platform for one to access their work computer from home. A downside to TeamViewer is that it is not very secure unless its security features are manually turned on. To make this free, easy to use platform secure, only run TeamViewer when using it, keep TeamViewer software up-to-date, and disable automatic startup (Fitzpatrick).

Alternatives to TeamViewer are a good idea if that alternative is free or the company can afford the cost of a remoting in service that charges a monthly fee and if they want something more secure. A few options are Windows Remote Desktop, Splashtop, Chrome Remote Desktop, and GoToMyPC. Windows Remote Desktop is compatible with Windows and Mac OS for free, however, Windows Home cannot host a connection. Splashtop is $16.99/year and is compatible with Windows, Mac OS, and Ubuntu Linux. Chrome Remote Desktop is a free browser extension, and works wherever chrome is installed, but there is a limited feature set in remoting in with Chrome. Chrome Remote Desktop cannot fix browser issues (issues with Firefox, Chrome, etc.) because it is browser based (Richmond). GoToMyPC is a remoting in service that is $66 for 2 computers per month. This allows 2-50 users, but it can only be downloaded on two computers. It has end to end encryption and comprehensive reporting. It is compatible with both Mac and PC ("GoTOMyPC").

The most secure way to remote in is using VPNs. One way to do this is with LoginTC. LoginTC was created in Canada and has a four step process to allow someone to remotely access their work computer. First, the employee attempts to login to their work account. Next, the request for access is sent to the LocinTC account. Then, an employer or manager would receive the request on either their phone or their computer. Finally the employer or manager will either allow or deny access to the work account. This is a very secure process to have people remote-in to work despite costing $3 per user per month for the business plan ("Two-Factor").

Physical Security

No cyber precautions will be good enough to protect a computer system from unlocked doors and windows. Physical access negates all security, yet there are a variety of precautions that one can take to secure the information of a small business from virtual and non-virtual breaches.

The most basic precautions one can take are to secure the premises of the business. By locking entryways (e.g. doors, windows) and preventing tailgating and piggybacking, (see: Social Engineering), the chances of a break-in are dramatically decreased. Monitoring the premises is another vital step to ensure security, such as installing security cameras or placing “no trespassing” notices on the facility to deter attempts (Deutsch).

Within the building or office, physical security may be furthered via the location of sensitive hardware. Keeping routers in a secure locked room seems simple but remains important. It is possible for an attacker to walk into a building and physically sabotage network equipment. Another safety precaution may include separating the main modem from the router to speed up connections to internet and boost functionality and performance, as well as decreasing the risk of a complete loss of connection and resources in the case of an attack on either piece of hardware. Other simple step to protect rooms may include the installation of security locks on doors, cabinets, and drawers (Bennett).

Furthermore, it is important to train employees to practice proper security protocols in order to maintain strong physical security (“How to Improve the Physical Security”). Training may include being able to recognize social engineering techniques, knowing how to take care of personal and work devices, understanding how to maintain discretion with information, and following legal contracts that outline punishments for employees or attackers who breach company security or steal information. Other important practices include installing ID Cards with identifying photograph and name to access to certain secure areas. Offering a security manual that includes a confidentiality policy will encourage employees to practice good security by reminding them of security protocols and regulations around the workplace (“How to Improve the Physical Security”).

Conclusion

The main elements of small business security are updates and the up-keeping of digital equipment and software, the importance of physical security, the uses of virtual private networks, the dangers of social engineering and different types of malware, how to avoid and respond to certain digital attacks, and how to manage user accounts for employees.

Small businesses are vulnerable to the following types of attacks: malware, DDoS attacks, Man in the Middle attacks, Brute Force attacks, and more. To combat a malware attack such as a trojan horse or ransomware, the business can create and enforce strict email policies. They can also only allow downloading software from safe, known sources and require their employees to be mindful of their safety on their computers. Small businesses can combat a DDoS attack by putting a spam filter on company websites and monitoring traffic on the router. The business can ban IPs that are trying to access the website too quickly or call the ISP or hosting provider if there is an apparent attack. To combat a MITM, the business can use strong passwords for network and local devices and only use secure and familiar websites.

A small business can keep its network secure by following the conventions in the results section and below: the business needs to update their computers' software and applications in a timely manner. They also need to keep their physical security intact with updated advances security locks; they cannot let broken locks remain broken. The business should invest in the use of VPNs, as they keep remoting in secure, and they encrypt data sent and received. The business needs to increase awareness on social engineering and receive training on what is a phishing scam. The business should install an antivirus and an anti-malware program to scan for malware on their computers. The business should create a backup of their data often so that if an attack does occur, they will not lose their data. Lastly, businesses should keep their user accounts secure. Do not give access to those who do not need it. Follow the password conventions listed above, and keep the business information, employees, and clients safe.

References

“Active Directory Authentication.” What Every Computer Scientist Should Know About Floating-Point Arithmetic, https://docs.oracle.com/cd/E19728-01/820-2550/activedir_auth.html.

“Antivirus.” *LCDI Wiki*, 25 March 2015, https://wiki.lcdi/index.php?title=Antivirus.

“Avoiding a Trojan Virus: Keeping the Gates Closed.” *Kaspersky*, Kaspersky, https://usa.kaspersky.com/resource-center/preemptive-safety/avoiding-a-trojan-virus.

“Backing Up Files Basic Computer Information.” *Basic Computer Information*, Basic Computer Information, 2018, http://www.basiccomputerinformation.ca/backing-up-files/.

“Backup: Your Most Important Task.” *2BrightSparks*, 2BrightSparks Pte. Ltd., 2018, https://www.2brightsparks.com/tutorials/thebackupguide.html.

“Bandwidth.” *LCDI Wiki*, 5 Feb. 2015, https://wiki.lcdi/index.php?title=Bandwidth.

Beal, Vangie. “VPN – virtual private network.” *Webopedia*, ITS Business Edge, https://www.webopedia.com/TERM/V/VPN.html.

Bennett, Adam. “Why Physical Security For Your Business Is Just as Critical as Online Security.” *Entrepreneur*, Entrepreneur Media Inc., 27 Apr. 2017, www.entrepreneur.com/article/293128.

Bhattarai, Saugat. “VPN research (Term Paper)” Jan 03, 2016, https://www.researchgate.net/publication/289120789_VPN_research_Term_Paper.

“BIOS.” *LCDI Wiki*, 20 April 2015, https://wiki.lcdi/index.php?title=BIOS.

“Brute Force Attack.” Cloudflare, www.cloudflare.com/learning/security/threats/brute-force-attack/.

“Change TCP/IP Settings.” Microsoft Support, https://support.microsoft.com/en-us/help/15089/windows-change-tcp-ip-settings.

“Client.” *LCDI Wiki*, 21 Apr. 2015, https://wiki.lcdi/index.php?title=Client/.

Cooper, Stephen. “8 Common types of malware explained in plain English.” *Comparitech*, Comparitech, 21 Feb. 2018, https://www.comparitech.com/antivirus/types-of-malware/.

Davis, Gary. “Why Software Updates Are So Important.” *McAfee Blogs*, McAfee, 19 Sept. 2017, https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/software-updates-important/.

de Saxe, Marshal. “5 Reasons Why It's Important To Update Your Software Regularly.” *Saxons Blog*, Saxons, 18 July 2017, www.saxonsgroup.com.au/blog/tech/5-reasons-important-update-software-regularly/.

Deutsch, William. “What You Need to Know About Securing Your Building and Property.” *The Balance Small Business*, The Balance Small Business, 25 July 2018, www.thebalancesmb.com/how-to-secure-your-building-and-property-394590.

“Distributed Denial of Service.” *LCDI Wiki*, 7 April 2015, https://wiki.lcdi/index.php?title=Distributed_Denial_of_Service_(DDOS).

“Dynamic Host Configuration Protocol (DHCP).” *Windows IT Center*, Microsoft, 01 Sept. 2018, https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top.

ExplainingComputers “Data Backup: The 3-2-1 Rule” Youtube, https://www.youtube.com/watch?v=rFO6NyLIP7M.

“Firmware.” *Techopedia*, Techopedia, https://www.techopedia.com/definition/2137/firmware.

Fitzpatrick, Jason. “How to Lock Down TeamViewer for More Secure Remote Access.” *How-To Geek*, How-To Geek, 6 Dec. 2017, www.howtogeek.com/257376/how-to-lock-down-teamviewer-for-more-secure-remote-access/.

Fleischman, Glenn. “Equifax Data Breach, One Year Later: Obvious Errors and No Real Changes, New Report Says.” Fortune, Fortune, 8 Sept. 2018, www.fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary/.

Geier, Eric. “How to Rescue Your PC from Ransomware.” *PCWorld*, IDG, 3 Apr. 2017, www.pcworld.com/article/2084002/security/how-to-rescue-your-pc-from-ransomware.html.

“GoToMyPC Remote Access - Remote Desktop Software for Mac or PC.” *GoToMyPC Remote Access - Remote Desktop Software for Mac or PC*, LogMeIn, 2018, https://get.gotomypc.com/.

Grimes, Roger A. “How to Detect and Avoid Malware.” *CSO Online*, IDG, 25 Oct. 2017, https://identity.utexas.edu/everyone/how-to-detect-and-avoid-malware.

Henry, Jim. “Social Engineering: 5 Manipulation Techniques.” *RECOIL OFFGRID*, RECOIL OFFGRID. TEN: The Enthusiast Network. Firearms & Survivalists Lifestyle., 11 Aug. 2017, https://www.offgridweb.com/preparation/social-engineering-5-manipulation-techniques/.

Hernandez, Erika. “20 Common Types of Viruses Affecting Your Computer.” VoIP Shield, *VoIP Shield*, 15 May 2018, https://www.voipshield.com/20-common-types-of-viruses-affecting-your-computer/.

Hoffman, Chris. “Which Files Should You Back Up On Your Windows PC?” How-To Geek, How-To Geek, 2 Sept. 2017, www.howtogeek.com/howto/30173/what-files-should-you-backup-on-your-windows-pc/.

“How Can I Know If My Computer Is Infected?” *Panda Security Mediacenter*, Panda Security Mediacenter, 5 Aug. 2010, www.pandasecurity.com/mediacenter/press-releases/how-can-i-know-if-my-computer-is-infected-10-tell-tale-signs-of-infection/.

“How to Keep Your Online Business Information Secure — Some Basics.” *The Wall Street Journal*, Dow Jones & Company, guides.wsj.com/small-business/technology/how-to-keep-your-business-information-secure/.

“How to Improve the Physical Security of Your Small Business.” *Grow With Kabbage*, 12 Oct. 2016, www.kabbage.com/blog/improve-physical-security-small-business/.

“iC3 2017 Internet Crime Report.” FBI, http://pdf.ic3.gov/2017_IC3Report.pdf.

“Identify and Secure Compromised Accounts - G Suite Administrator Help.” *Google*, Google, 2018, https://support.google.com/a/answer/2984349?hl=en.

“Internet Service Provider (ISP).” *LCDI Wiki*, 10 Feb. 2015, https://wiki.lcdi/index.php?title=Internet_Service_Provider_(ISP).

“IP Address.” *LCDI Wiki*, 16 March 2015, https://wiki.lcdi/index.php?title=IP_Address.

Larson, Quincy. “How to Set up a VPN in 10 Minutes for Free (and Why You Urgently Need One).” *FreeCodeCamp*, Free Code Cam, 27 Mar. 2017, https://medium.freecodecamp.org/how-to-set-up-a-vpn-in-5-minutes-for-free-and-why-you-urgently-need-one-d5cdba361907.

Lemonnier, Jonathan. “What Is Malware? How Malware Works & How to Remove It.” *What Is a Computer Virus? | The Ultimate Guide to PC Viruses | AVG*, AVG, 6 June 2015, www.avg.com/en/signal/what-is-malware.

Little, Brian. *Small Business Security*. Lewis University, nd. Web. Sept.-Oct. 2018. <http://www.cs.lewisu.edu/mathcs/msisprojects/papers/SMBSecurity_BrianLittle.pdf>.

Lord, Nate. “Ransomware Protection & Removal: How Businesses Can Best Defend Against Ransomware Attacks.” *Digital Insider*, Digital Guardian, 27 Aug. 2018, www.digitalguardian.com/blog/ransomware-protection-attacks.

“Malware.” *LCDI Wiki*, 21 Apr. 2015, https://wiki.lcdi/index.php?title=Malware.

“Man in the Middle (MITM) Attack.” Incapsula.com, Imperva Incapsula, www.incapsula.com/web-application-security/man-in-the-middle-mitm.html.

Mason, John. “VPN Beginner's Guide.” *TheBestVPN*, The Best VPN, 23 Nov. 2017, www.thebestvpn.com/what-is-vpn-beginners-guide/.

Mitchell, Bradley. “How Do You Change a Router's Wi-Fi Name (SSID)?” Lifewire, 29 Mar. 2018, www.lifewire.com/change-the-wifi-name-ssid-on-a-router-818337.

Mitchell, Bradley. “The Definition of Network Gateway.” Lifewire, Lifewire, 15 May 2018, www.lifewire.com/definition-of-gateway-817891.

“Network.” *LCDI Wiki*, 20 April 2015, https://wiki.lcdi/index.php?title=Network.

“New Data Shows Threat of Biz Ransomware Attacks.” PYMNTS.com, PYMNTS.com, 21 Aug. 2018, www.pymnts.com/news/security-and-risk/2018/business-cybersecurity-ransomware-malware-cyberattacks/.

Ngo, Dong. “Digital Storage Basics, Part 3: Backup vs. Redundancy.” CNET, CNET, 29 Mar. 2013, www.cnet.com/how-to/digital-storage-basics-part-3-backup-vs-redundancy/.

Nield, David. “All the Best Ways to Back Up Your Data.” Gizmodo, Gizmodo.com, 28 Aug. 2018, www.gizmodo.com/all-the-best-ways-to-back-up-your-data-1796291120.

O’Donnell, Andy. “What Are Packet Sniffers and How Do They Work?” *Lifewire*, 27 Aug. 2018, https://www.lifewire.com/what-is-a-packet-sniffer-2487312.

“PASSWORDS DO's AND DON'Ts.” *Marquette University*, Marquette University, www.marquette.edu/its/help/security/password.shtml.

Phillips, Gavin. “The 5 Major VPN Protocols Explained.” *MakeUseOf*, Technology Explained, 12 Oct. 2017, www.makeuseof.com/tag/major-vpn-protocols-explained/.

Poladian, Charles. “What Is a VPN?” Mashable, Mashable, 7 Sept. 2018, https://mashable.com/review/what-is-a-vpn/#URB15qzz9Oqt.

"Privacy and Data Security." *Office of the Vermont Attorney General*, http://ago.vermont.gov/privacy-data-security/.

"Random Access Memory (RAM)." *LCDI Wiki*, 10 Feb. 2015, https://wiki.lcdi/index.php?title=Random_Access_Memory_(RAM).

Ransomware. Federal Bureau of Investigation, http://pdf.ic3.gov/Ransomware_Trifold_e-version.pdf.

"Ransomware & Cyber Blackmail." *Kaspersky Lab*, Kaspersky Lab, https://usa.kaspersky.com/resource-center/threats/ransomware.

"Ransomware - What Is It & How To Remove It." *Malwarebytes*, Malwarebytes, www.malwarebytes.com/ransomware/.

Rehman, Ibad Ur. "What Is A Brute Force Attack?" The Official Cloudways Blog, CloudwaysCDN, 22 Mar. 2018, www.cloudways.com/blog/what-is-brute-force-attack/.

Richmond, Riva. "How to Maintain Security When Employees Work Remotely." *Entrepreneur*, Entrepreneur, 22 Aug. 2012, www.entrepreneur.com/article/224241.

Rouse, Margaret, et al. "What Is Phishing? - Definition from WhatIs.com." *SearchSecurity*, TechTarget, Oct. 2017, searchsecurity.techtarget.com/definition/phishing.

Rubens, Paul. "How to Stop DDoS Attacks: 6 Tips for Fighting DDoS Attacks." *ESecurity Planet: Internet Security for IT Professionals*, ESecurity Planet, 26 June 2018, www.esecurityplanet.com/network-security/5-tips-for-fighting-ddos-attacks.html.

"Security Tip (ST04-014)." *"Plan, Do, Check, Act" | US-CERT*, US-Cert, 24 Jan. 2017, www.us-cert.gov/ncas/tips/ST04-014.

Simmons, Jay H. “5 Disadvantages of VPN That You Should Know Before Using It.” - Everything about VPN and Protecting Privacy Online, 2018, www.vpncrew.com/5-disadvantages-of-vpn-that-you-should-know-before-using-it/.

Smith, Brad. “The Best VPN Services.” *TheBestVPN*, The Best VPN, 9 July 2018, www.thebestvpn.com/.

“Social Engineering - Definition.” Kaspersky Lab, https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering.

“The Importance of Data Back-Up.” Norton , Symantec, 2018, us.norton.com/internetsecurity-how-to-the-importance-of-data-back-up.html.

“Two-Factor Authentication for Your Organization.” *LoginTC* , Cyphercor Inc , 2018, https://www.logintc.com/get-started/how-it-works.html.

“Types of Backup.” SolarWinds MSP, www.solarwindsmsp.com/content/types-of-backup.

“What Is a Brute Force Attack? - Definition from Techopedia.” Techopedia.com, www.techopedia.com/definition/18091/brute-force-attack.

“What is a Computer Virus?” *Malware*, Norton, 2018, https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html.

“What Is a Distributed Denial-of-Service (DDoS) Attack?” *Cloudflare*, Cloudflare, www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

“What Is a Firewall?” Cisco, 24 Oct. 2018, www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html.

“What is a man-in-the-middle attack?” *Norton*, 2018, https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html.

"What Is a Trojan Virus? -Definition." *Kaspersky*, Kaspersky, usa.kaspersky.com/resource-center/threats/trojans.

"What Is a User Account? - Definition from Techopedia." *Techopedia.com*, Techopedia, 2018, www.techopedia.com/definition/13458/user-account.

"What Is a VPN Client? - Definition from Techopedia." *Techopedia.com*, www.techopedia.com/definition/30752/vpn-client.

"What Is Remote Access? - Definition from Techopedia." *Techopedia.com*, Techopedia, 2018, www.techopedia.com/definition/5553/remote-access.

Williams, George. "Everything You Need to Know about the Wonderful World of Backup Technology." The Next Web, 14 Sept. 2018, thenextweb.com/contributors/2018/09/16/everything-you-need-to-know-backup-technology/.

Yev. "Backup Strategies: Why the 3-2-1 Backup Strategy Is the Best." Online Backup Security & Encryption | Backblaze, 25 Sept. 2017, www.backblaze.com/blog/the-3-2-1-backup-strategy/.