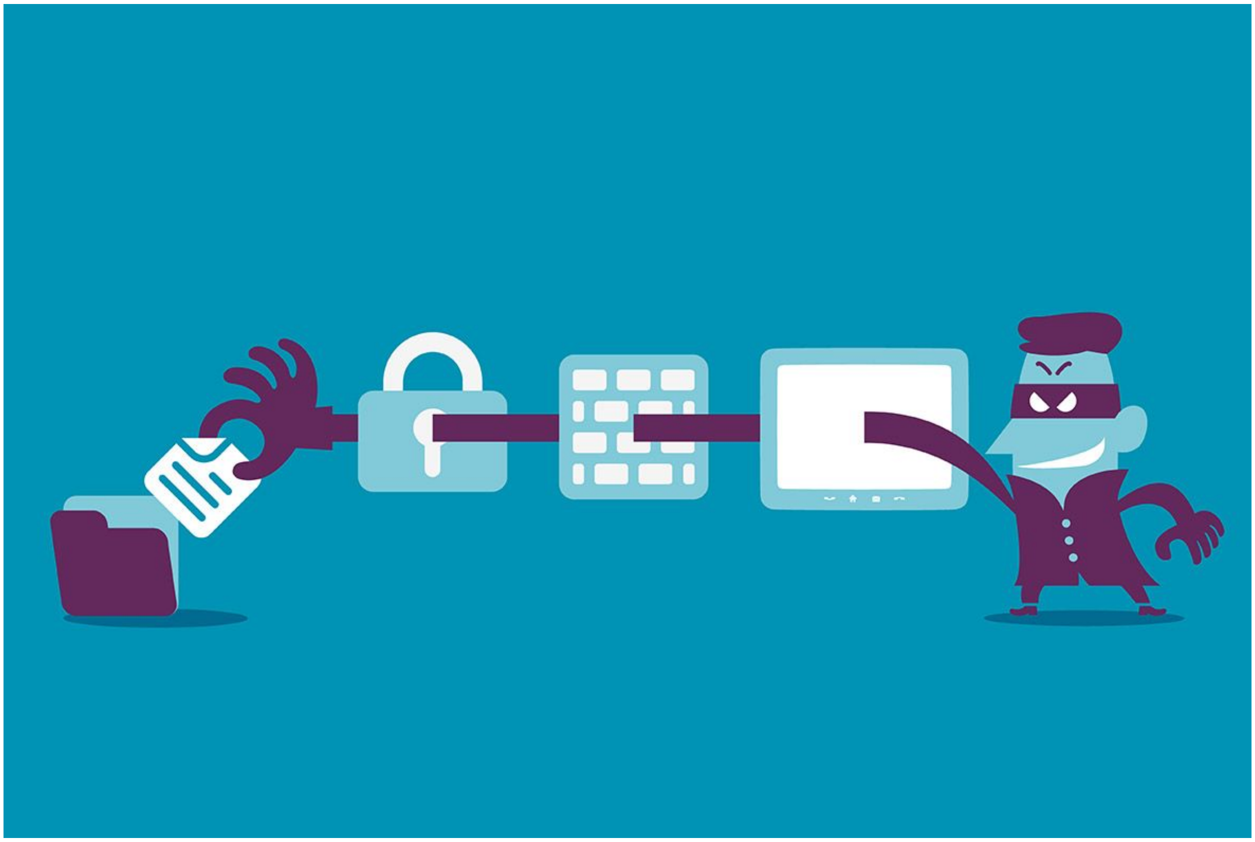
University of Missouri-St. Louis

Introduction to Information Security
Undergraduate Group Research Paper



Ahmed Almohammadi, Jibril Anifowoshe, Andrew Huebner, Alex Oliver, Omar Salih, and Raoul Wilbanks

FS17-INFSYS3848-E01

Dr. Shaji Khan

December 15th, 2017

Table of Contents

Executive Summary - Where we're headed

The internet is a big part of our lives. It is a powerful tool used for business and entertainment, and we have many different ways of accessing these needs through it. Unfortunately, many devices used to access the internet are susceptible to the ever growing threat of malware. Malware comes in many shapes, has different names, and can impact both regular people and businesses alike. Ransomware, boot-sector viruses, and spyware are but a few forms of malware that can affect the regular user in different ways. E-businesses are not immune to the potential threat of malware either. These attacks cost businesses billions of dollars in damages, so they have to be prepared to fight any threats that come their way.

The biggest vulnerabilities are due to the habits of end users, and educating them on how to avoid potential malware attacks are some of the first steps that needs to be implemented. One way to understand why people are so susceptible to malware is to understand why and how they get infected in the first place. This is an important step, but many business are ineffective in educating their end users. Because of this, business often implement their own defenses against malware and try to make the process for their employees as simple as possible. Some defenses include the backing up of hardware and making it difficult for attackers to access their network in various ways.

Despite the current conventional approaches to these problems, end users seem to continue to be very vulnerable to these attacks. Creating end user awareness has been a big problem because employees are often more concerned about their specific tasks rather than focusing on what many consider to be IT responsibilities. Companies do try and educate their employees, but often they are ineffective, and we will discuss why we think this is. Despite the many failed attempts to help internet users avoid trouble in the form malware, there is still hope. Business can implement creative solutions to engage their employees which will add an extra layer of defense onto the existing measures already taken by IT departments. We will discuss what we believe to be some problems regarding end-user awareness and education, but before attempting to solve this problem, the problem has to first be understood. Malware is the threat, and the following sections will discuss what it is in detail, why people fail at defending themselves against it, and how the problem can be solved. The following write up will discuss malware in more detail before ultimately circling back to the issue of end users.

An Introduction to Malware

Before discussing why malware matters, we need to know what it is. Malware is a software that intends to damage the system that you are using by stealing the data you have on your device, or harming you in some other way. Another symptom of malware is that it could make your system slow and inefficient. Malware can sometimes be described as spyware, a virus, or even have its own name like "Pegasus". The website known as Radware states that the first malware, known specifically as "The creeper", was discovered in 1971. The creeper displays a screen daring you to capture it, but it caused no harm. Hackers have continued to develop malware over time to become more harmful. Malware is used nowadays to damage users' systems and to steal data.

As mentioned, one example of a malware is Pegasus. The spyware was first found in August 2016. Pegasus got exposed after an attack that failed against a human rights defender. After investigating it, some details about the spyware was revealed. The spyware is capable of reading the text messages on a phone, tracing the phone, stealing passwords, stealing call data, and stealing general information from many other applications that are installed on the phone. In many cases it is very difficult to detect ample amount of malware on the web. Malware can impact everyday users and massive businesses as well.

Why Malware Matters

Impact on Everyday Users - How to Pick On the Little Guy

An important first step for end users to stay safe is to realize why knowing about malware is important. This is an important step because we must alert users what is really at stake in a malware attack, and users will want to avoid malware, not only on their home computers, but while they are at the organization as well. Most users consider their files, privacy, system, and money important, and they stand to lose any or all of these things due to malware.

Common types of malware include ransomware, boot-sector viruses, and spyware. A quick overview of each reveals they all have the ability to seriously disrupt a user's workflow and data. Ransomware affects the entire drive by encrypting people's files. Boot-sector viruses mess with a drive's boot sector, making it unbootable. Lastly, spyware monitors a user's activity, and can even interfere with their computing.

Ransomware has become a very popular form of attack, especially in recent years. When a user is targeted, their files are encrypted, and a ransom is demanded to get the encryption key to decrypt the files. Without this key, there is no way to retrieve the files ("What is ransomware? - Definition from WhatIs.com," 2017). One such example is a ransomware by the name of WannaCry, where attackers would encrypt the files, then demand the ransom in bitcoin, which is very common because transactions using bitcoin are untraceable. Additionally, after a specific amount of time passes, the ransom doubles, and after 7 days, the files are destroyed. Users suffering from this type of malware can not only lose their files, but also a significant amount of money should they choose to pay the ransom (Sherr, 2017).

By contrast, boot-sector viruses tamper with the boot sector of a hard drive, causing the computer to be unable to boot (Fisher, 2017). This type of virus was more popular in the days of DOS, and one infamous example was the Michelangelo virus, which on March 6th, would overwrite the first 100 sectors of the hard drive with nulls, making the data on the drive inaccessible. Users affected with this type of virus would lose their files, and possibly the system entirely, since the OS would not be able to be loaded ("Memories of the Michelangelo virus," 2012).

Additionally, spyware will monitor user activities and even hijack said activity and redirect users to other places. Some, such as Hot as Hell, will dial toll numbers and cost the user money ("What is spyware? - Definition from WhatIs.com," 2017). Internet Optimizer hijacked error pages and redirected them to a controlling server. Keyloggers also track keystrokes and are able to steal information through what the user types, including passwords. Because of this, users would lose money through the toll lines, and privacy through the keyloggers tracking everything they type ("Top 10 Spyware Threats," 2007).

This is just a small sample of malware that a user can be infected with and can seriously mess with their files, money, privacy, and their system. In order to keep all this from happening, we have to be aware of this, and keep malware off of the systems. Businesses are affected as well, as the ransomware has affected entire systems such as airports and hospitals.

Impact on Business - Billions in Losses

Today, malware is the most dominant issue in the e-Business arena. It has affected many aspects of a business from the end user to online services. These businesses have become victims of stolen assets, billions of dollars lost, personal identities stolen and breaching of the CIA triad. Malware has been so impactful that businesses have tried to combat the assault. For the most part, these responses have been playing catch up. Some of these responses have not been sufficient enough to combat the malware. A lot needs to be done quickly in order to stop the devastating destruction malware has on businesses.

E-commerce has been very important in the 21st century because it has contributed greatly to the world economy. In 2016 alone, e-commerce has generated 1.86 trillion US dollars worldwide and is projected to increase roughly 2.5 times more to 4.48 trillion US dollars in 2021 ("Global Retail E-Commerce Market Size," 2017). There is a lot of money to be made in e-commerce to say the least. In order for an e-Business to thrive, it needs access to the internet and web for it to continue its growth. There are lots of positives that come from the web. Lately, e-business have been using the web to further grow their business. Unfortunately this attracts negatives like malware. Malware has been so impactful on businesses that in 2007, it has done 67.2 billion USD in damages directly and indirectly. In addition to this, businesses have invested 7.8 billion USD to fix and repair all the damages that malware has cost them (Pan, 2009). Not only are businesses affected financially, but the confidentiality of classified material can be stolen, or the availability of data to be lost could lead to theft of personal information about customers or staff of your organization.

The CIA triad refers to confidentiality, integrity, and availability. If a business is attacked by malware it is a breach on the CIA Triad. Confidentiality refers to the right of those who have the authority to access specific information and those who don't have authority, do not have access. If a malware attack steals customers' identification then the confidentiality of information has been breached (Chai, 2012). Integrity is the safeguarding of information. Integrity can be compromised when malware alters data like money transactions. An Item can cost $1000.00, but malware can alter code and information to have the Item only transact $100.00. Lastly, availability refers to the timely access to information (Chai, 2012). Malware has the ability to shut down entire computer system which will make information unavailable.

Many businesses these days need to preserve their CIA triad. If they don't, their company and brand can be damaged which leads to a loss of customers and money.

Plenty of customers will now try to avoid a business if they have learned that their customers' credit card information has been stolen. Some companies are at risk of facing fines if they are unable to keep data from being breached. Adobe fell victim to this incident as they were fined 1 million USD for a data breach back in 2013 for having more than 3 million encrypted customer credit card records stolen (Larson, 2017). This will obviously result in a loss for business with the consumers. Anthem Incorporated, a healthcare business, suffered from a malware attack in February of 2015. The attack compromised, "80 million current and former customers". The attack stole information about Social Security numbers, addresses, birthdates, and employee information. The Anthem brand was damaged and suffered from heavy losses from the attack. Big companies like Anthem and Adobe are big enough to recover from these attacks (Walters, 2015). Small businesses, however, have a much harder time to recover and could potentially be unable to recover. Most small business fall prey to ransomware. Experts in the information security field estimate that small businesses account for more than 60% of all malware attacks. On average small business lost over $100,000 dollars within 25 hours of being infected of the ransomware (Larson, 2017).

Many of these attacks are carried out because of the end user. A Microsoft employee, Dandelion, said that weakest link to malware infection is human stupidity that lead to many successful social engineering attacks (Pan, 2009). Many businesses now take action to stress to their employees to practice good security habits through education and reminders to prevent further attacks. A lot of this includes reading emails carefully and report any suspicious email to the higher ups in your business. Small and large businesses install the latest versions of anti-malware software which will help prevent most current mainstream malware attacks. With all that said, malware will always be ahead in the game and business will always have to play catch up in order to protect their business and their assets.

Current Approaches to this Problem - Thank Your IT Staff

Right now there are many approaches businesses take to prevent the spread of malware. Some defenses are simply staying up to date on software and patches, making sure to have anti-virus/malware software installed with the latest signatures, and having basic common sense. For example, perhaps it is unwise to click on a link from an unknown source. Users can hover over URLs to confirm they go where they claim to go. Users also should be careful around shady websites that might have pirated software for example. Users should also not give out too much information about themselves or their business online, as this would give attackers more information on how they can attack.

It is important to stay up to date on the latest patches and the latest versions of the operating system you are using. A good way to do this is to make sure the computer is always connected to the network and does not go into sleep mode. Each update or patch will have additional security added in. Updates to operating systems are deployed so it can fix exploitable vulnerabilities that can be taken advantage of through malware. Anti-virus software is great for already known malware. Typically companies that create antivirus software have a database of already known malware based off their digital signature. Anti-virus software will be able to detect any malware by matching the signature of the malware on your computer to their database. If new malware is discovered then the company needs to update their database. Backing up your hard drive or cloud server on a regular basis is very important. A malware attack may hold your computer hostage and you are unable to gain access. Backing up your computer will allow you to restore your hard drive to an earlier state before you were infected. If you do not backup your hard drive then your computer can very well be a lost cause and will be unable to be restored to an earlier state ("How To Prevent A Malware Attack On Your Business," 2017). Lastly, encrypting your hard drive can protect your computer in an event of a breach. Most computers have full hard drive encryptions for use. If a malware attack wanted to expose all your customers, it would fail because of the data encryption. However, the best way to prevent malware attacks is education through the user.

Another way businesses try to avoid malware is by trying to make sure their network is secure. This is so attackers cannot introduce malware to a network drive. Attackers should not easily be able to connect to a business's network through Wi-Fi. Secure passwords and only allowing the connection of specific devices will help keep the network safe. It is imperative that default password for the router is changed. If a password is given out, it should be changed after the fact. Physical ports also pose a threat if they are not secure. An unknown entity should not be able to connect their devices physically to a network through a port. A business can manage ports by only letting ports stay open at specific locations or specific times. Alternatively, ports can be locked out automatically when unknown devices are physically connected. Thumb drives with malware can also pose a threat to a network, and these thumb drives can be controlled in a few ways. Dell Data Protection is an example of an application that has the ability to block all thumb drives that are connected to a computer, only allowing them to transfer data through the permission of the network security team of a business. Similar services can do things such as lock out an entire computer as soon as a thumb drive is connected, while at the same time notifying network administrators.

The Gap - IT Staff Need Help

While existing measure to prevent malware exist, many of which are implemented directly by IT departments, creating end user awareness is one of the most difficult tasks that businesses should, but often cannot, implement. Employees often just expect everything to work and don't treat the threat of malware as seriously as they should. This can stem from the fact that employees often want to focus on their own specific tasks and expect network security responsibilities to fall into the hands of IT professionals. The reality is that IT professionals can often only do so much due to the nature of the internet, and end users as a whole need to take some responsibility to reduce threats.

Creating awareness around a subject is another way of saying educating. End users, in this case, need to be educated on what malware is and what threats they pose. Educators, like

Professor Eric Mazur of Harvard Graduate School of Education agree that learning and retention is more effective through active learning (Anderson, 2014). Though end users would rather focus on their own responsibilities rather than focus on "computer stuff", it's important for them to set some time to the side to learn about malware without IT staff being overbearing. The level of involvement and engagement in this case can be a little difficult to gauge. End users cannot be expected to take a full course on information security, but their involvement should be more than just reading an email sent out by the CIO. The more money and time spent on creating end user awareness, the more prepared and knowledgeable the end user will be. A middle ground can be found in dedicating a day of training.

One of the biggest tasks of IT professionals running training modules is convincing the end users that malware threats are real. Often people live in the bubble of, "it won't happen to me", but time and time again, even the biggest and seemingly most untouchable companies are attacked due to low end user awareness. Training on end user awareness of malware needs to make the threat of malware feel more personal rather than something to be handled by the IT staff. Perhaps even a controlled demonstration of malware being sent out to ends users will be effective in showing end users what not to do.

Pegasus specifically is a dangerous malware because it provides full access to a phone. As dangerous as Pegasus was, being infected by it was pretty preventable in the way most malware is also preventable. Pegasus was a case of trying not to click on the wrong thing and making sure patches were downloaded promptly to prevent infection. This sort of malware could pose a great threat to a business that provides company phones, and training provided by companies to their end users could use Pegasus as an example of how such a preventable mistake could cause so much damage to a business, and how it is essential to keep up with the most up to date patches. Pegasus is a great example of malware that can get past an IT department's defensive measure, but would struggle to get passed attentive and educated employees.

End-User Folly and Security Breaches - The Spread of Infection

Malware is easy to get if the user is not careful. There are many ways to get malware, such as, emails, unsecure website, unknown links, untrustworthy applications, and attackers. The first thing that makes it easy for the user to get malware is not having a good security system. Security systems can help the user avoid malware and keep the system safe. It can detect malware in the user's system and fight them. Also, visiting unreliable websites can get you infected. Websites can be full of viruses that can harm your device and get malwares all over the system. If the user wants to download any program, the user should download it from the official website. Some websites might tell you that you can download the program from here, but instead it might be an easy way to send you some malware.

Moreover, suspicious emails are one of the easiest ways to get infected by malware. A lot of people get emails from unknown sources and it gets them infected easily. The email can say anything just to make sure that you click anything to get infected by malware. Links are also one of the ways the user can get infected by malware. Some links could have viruses and they get the user infected as soon as the user click it. Links are easy to spread through the social media, the user can get them in twitter, facebook, or whatsapp. Users should not click in any link before making sure that they know the source of it. Downloading applications could get the user infected by malware. Some applications have malware on them, and as soon as the user download them, they get infected.

Local Area Networks (LANs) are a group of locally connected computers that can share information over a private network. If one computer becomes infected with malware, all other computers in the LAN may quickly become infected as well. Also, if you're using a client for instant messaging (IM) and peer-to-peer (P2P) file-sharing online systems activities, malware may spread to your computer (Savage, 2012). Social networks allow malware authors to take advantage of having the ability of infecting the massive user-data networks with worms. If a social website account is infected with a worm, just about anyone who visits a poster's profile page could "catch" the worm on their system. Some of the most sophisticated malware spreads through well disguised screen pop-ups that look like genuine alerts or messages. Malware can be easily spread if you share computer storage media with others, such as USB drives, DVDs, and CDs. While it may seem safe to open a CD of photos from a colleague, it's always best to scan unfamiliar files first for possible corruptions or security risks before you copy or open them (Savage, 2012). Mobile malware threats have become increasingly prevalent, as more people use their smartphones and tablets as mini-computers, helping malware problems proliferate across additional platforms. Malicious codes also spread into a system through pirated software. In majority of the cases, software seems to be legitimate, when downloaded, instead they are big trouble for your system.

Our Innovative Approach - A Combination of Solutions

One of the biggest "gaps" that exist is that users often just do not care because they do not consider malware to be a real threat. An interesting way to show employees of a company just how easy it is to infect them is to get the IT department involved as white hat hackers. Businesses often provide company emails for their employees. An IT department could craft their own harmless "malware" and send them out to these employee emails. The email would include an attachment that looks somewhat familiar to and related to their work. The malware would not cause actual harm, but it would identify the employee that opened an attachment they should not have. Alternatively, the email can have a link to a website which could also identify which employee clicked on the link. This memorable approach of educating end users on the dangers of malware will show and involve the employees, allow them to learn from their mistakes, and show them what to avoid in the future.

Simply sending out fake emails or web links to track and educate users may not be enough, however. Users need more of an incentive rather than corporate speak of "malware is bad, be careful". Positive reinforcement is one of the best ways to produce new behavioral habits, and this method of improving individual behavior can be implemented into the white hat hacker process. If an IT department decides to track their employees, a reward system can be implemented for employees that exhibit safe habits over an extended period of time while at their workstations. For example, perhaps an employee has not visited a dangerous website or downloaded any malware through an email attachment for a year. A reward for doing this would be to give double salary for one month in a year or maybe more vacation days. Of course these rewards need to be flexible and a business's assets need to be taken into consideration. If wage increases are too expensive, the IT department can host a dinner party for those that work safely. Another way of rewarding the user is to reward them with additional vacation days. Every employee wants additional vacation days to spend time with family and friends. These rewards are real incentives because they essentially make their lives better. If the business really values information security, perhaps rewards can be given out more often, or that they can be more extravagant.

An alternative to positive reinforcement would be to punish employees that do not do a good job of avoiding malware. This method of interacting with employees will not be as effective, however, and could negatively affect the work environment. Something minor like showing a public list of employees that have been infected by malware might give incentives to browse more carefully. The threat of demotion or even being dismissed from a job are also ways to change behavior. These approaches are harsh, however, and will probably only work for companies that place extreme value in information security. We do not recommend a negative approach.

Additionally, rather than asking employees to read a paper like this one on end user awareness on malware, which they may or may not do, the IT staff can set up a day focusing on the topics of: How people get affected, how malware affects people and businesses, what malware actually does after it infects a host, how businesses defend against malware, and how these measure are sometimes ineffective. One of the reasons security regarding malware is ineffective is because of unaware end users, and these training modules will hopefully remind them of the part they play in the grand scheme of information security in a memorable way.

One may argue that some employees might not care enough for rewards. Some people may be totally happy making mistakes with no repercussions. Some people believe that viruses are no big deal and they are unaware of how a virus can affect them personally. They believe that IT will always be there to solve the problem. To solve these problems we think employees should see the danger first hand in front of them. We suggest that all current employees and new hires should be given a live demo of a malicious virus.

The live demo will show first-hand how easily a malicious virus can affect your computer just by clicking a link from an email. The demo should show how the virus affects the company and the user personally. For an example; the demo shows the virus logging your keys, accessing your personal files, and accessing your camera. The malicious user virus knows what your personal data contains, your company's data, and what you look like. At this point the malicious user knows everything about and the user and can cause real harm now. The point is to not scare employees, but it is to bring attention to the dangers of malicious viruses instead of employees only knowing, "viruses are bad" with no substance to it.

One of the innovative approaches that we came up with is making competition between departments. We find it effective because most people get excited when they are challenging others. By making it a competition, everyone will try harder and do better. Also, we can add rewards every month for the department that is in first place. This competition will create a fun atmosphere at the company's work environment, which is going to make workers focus more. Workers are going to want to win, so during the competition they going to learn about malware and get ideas about it. This is going to help them avoid malware. Workers are going to recognize spam emails and unsecure websites. Instead of giving them training which some of the workers might pay attention to, we can provide something they are going to enjoy.

Employees would also need to remain on task while at work, and not just be actively looking for these things just for points or bragging rights. In order to make this more effective, instead of having the competition be an ongoing process throughout the work week, it may be more beneficial to have it be a specific program with specific events and days set up for competition. This way employees would still be able to be competitive without disrupting the flow of work. Additionally, a reward system of either pass or fail could also be implemented. The reasoning behind this is that we don't want employees to try and sabotage each other to win rewards. They should be working together to improve the company and their lives.

Since gamification will be implemented between departments, the company will also have an idea of what weaknesses exist. They can then start training or use those weaknesses to improve future uses of gamification. If there are repeat offenders, that can be brought up during reviews that training is required and a certain level of competency is required in order to allow employee access to more data or even sensitive data. Rewarding employees that are doing well with small bonuses, departmental outings, gift cards, posters, mouse pads, will also keep security on everyone's minds.

While not all seeing, IT staff often do have some degree of control on what employees can see and click on. If an employee is caught clicking on a suspicious link through an e-mail or their browser and downloads malware which is hopefully immediately quarantined by an antivirus, IT staff can kindly explain to the end user the specific nature of the malware, why they might have been targeted, and what damage the malware might have caused. Even with a day of training, it's likely that employees will still make mistakes from time to time. This is why there is also some responsibility on the IT staff to be open to continually communicating with their team. The educating process cannot end after a single training day. This type of engagement will once again push users back into their bubble of "it won't happen to me." IT staff can keep in touch with their employees to ask if, for example, they have seen anything suspicious. This involvement will make end users more likely to speak up rather than leave them in a state of, "I'll remind them when I have time".

Even trained employees will make mistakes from time to time, and the IT staff can increase their efforts to make the jobs of their employees even easier. One of the easiest ways to keep employees from visiting untrusted websites is by only allowing certain websites to go through the router in the first place. Rather than blocking all websites that might be dangerous, it would be easier to say website x, y, and z is allowed through our router. Emails also pose a threat. A system of an internal business emails can also be implemented. Employees can freely communicate with each other through email, but unknown emails will not be sent to emails without first being vetted by the IT staff or software that is on the lookout for malware. This would be very restrictive, however. Emails can also be automatically stripped of any attachments. If any information needs to be shared, a link to a location on a network drive can be shared instead. Also, blue links in emails can also turn to black text. This text will then have to be copied and pasted into a browser url. This extra step adds an extra layer of security. Browsers can also come with an image that makes it so they already have ad blockers and script blockers. Both of these will prevents unknown elements on websites from loading and potentially introducing malware to the workstation. These approaches will help employees stay on the right path with minimal effort on their part, although the inability to access any website they want or to be able to email any person they want may feel restrictive.

Conclusion

Time and time again, companies and people have been burned due to their inability or lack of care for avoiding malware attacks. Simply following a few simple steps can result in the loss of major tangible and intangible assets. Malware is only going to become a bigger and bigger problem in the 21st century, but not all hope is lost. Of course it is not possible to avoid all malware threats when going online, but most attacks can easily be avoided if users know the basics of what to and what not to do.

Relying solely on the IT department to keep a business safe is not enough. Users are the first line of defense, and getting them involved is critical. As important as it is for IT and end users to work together to avoid security breaches, everyone must realize that no solution is perfect. Just as there will always be “bad” people, there will also be the threat of attack to a business if someone has an easy way gain something. “What is the perfect solution to prevent malware?” is the multi-million dollar question, and the answer to this simply does not exist yet. Our creative approaches on how to get end-users more involved, educated, and attentive are but a few ways to significantly reduce threats. No single one of our solutions are the end all be all, but using them as a combination of each other will surely make any business at least a little safer, and that is the best that anyone can ask for right now.

References

Anderson, J. (2014, November 17). The Benefit of Interactive Learning. Retrieved December 15, 2017, from https://www.gse.harvard.edu/news/14/11/benefit-interactive-learning

Chia, T. (2012, August 20). Confidentiality, Integrity, Availability: The three components of the CIA Triad. Retrieved December 15, 2017, from http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/

Fisher, T. (2017, March 12). What is a Boot Sector & How Do You Fix Boot Sector Errors? Retrieved December 15, 2017, from https://www.lifewire.com/what-is-a-boot-sector-2625815

Global retail e-commerce market size 2014-2021. (n.d.). Retrieved December 15, 2017, from https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

Hochstadt, A. (2017). The 20 Biggest Hacking Attacks of All Time. Retrieved December 15, 2017, from https://www.vpnmentor.com/blog/20-biggest-hacking-attacks-time/

How To Prevent A Malware Attack On Your Business. (2017, September 25). Retrieved December 15, 2017, from http://www.evolvit.co.uk/prevent-malware-attack-your-business

Larson, S. (2017, July 27). Why ransomware costs small businesses big money. Retrieved December 15, 2017, from http://money.cnn.com/2017/07/27/technology/business/ransomware-malwarebytes/index.html

Memories of the Michelangelo virus. (2012, March 06). Retrieved December 15, 2017, from https://nakedsecurity.sophos.com/2012/03/05/michelangelo-virus/

Pan, J. (n.d.). MALWARE'S IMPACT ON E-BUSINESS & M-COMMERCE: THEY MEAN

BUSINESS! Retrieved December 15, 2017, from http://www.academia.edu/934928/MALWARES_IMPACT_ON_E-BUSINESS_and_M-COMM ERCE_THEY_MEAN_BUSINESS_

R. (2017). The History of Malware. Retrieved December 05, 2017, from https://www.radware.com/resources/malware_timeline.aspx

Savage, Michelle. The PayPal Official Insider Guide to Internet Security: Spot scams and protect your online business October 1, 2012

Sherr, I. (2017, May 19). WannaCry ransomware: Everything you need to know. Retrieved December 15, 2017, from https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/

Top 10 Spyware Threats. (2007, April). Retrieved December 15, 2017, from http://whatis.techtarget.com/definition/Top-10-Spyware-Threats

Walters, R. (2015, November 11). Cyber Attacks on U.S. Companies Since November 2014. Retrieved December 15, 2017, from http://www.heritage.org/cybersecurity/report/cyber-attacks-us-companies-november-2014

What is ransomware? - Definition from WhatIs.com. (2017, September). Retrieved December 15, 2017, from http://searchsecurity.techtarget.com/definition/ransomware

What is spyware? - Definition from WhatIs.com. (2016, September). Retrieved December 15, 2017, from http://searchsecurity.techtarget.com/definition/spyware

Zaineb, A. (2010, June 22). Positive Reinforcement to Improve an Individual's Behavior! Retrieved December 15, 2017, from https://blog.commlabindia.com/elearning-design/positive-reinforcement