Dalton Scharff

Professor Quirin

CS 0590: Social Implications of Computing Technology

15 March 2017

The Psychology of Security

As an employee for the University of Pittsburgh’s student technology help desk, I get to see computers infected with a variety of malicious software. Often on the very same machine, I will find any number of antivirus/antimalware products that are supposed to protect the user from this very situation. As of 2015, the antivirus industry was valued at $106 billion and projections only show that number growing (Roy). With each of these companies making bold claims about the strength and security of their products, it begs the question as to why the amount of malware as well as antimalware programs continues to increase. Has no one found the perfect algorithm to protect its users from cyber threats?

Digital security can be closely compared to physical security, just instead of deadbolts and padlocks, think of passwords and protocols. Just like rules, it almost seems as if locks were made to be broken. No matter how large and secure, all it takes is the right shim, bolt cutters, or skilled lock pick to gain entry. Yet, I sleep soundly at night only after the one puny lock on my front door is engaged, even when I know that break-ins occur in similar houses throughout my neighborhood. It turns out that in the digital world, just as in the physical, there is no perfect protection against those with bad intentions. Even if I were to trade my front door with the vault door for Fort Knox, there’s always going to be a weakest link (perhaps by breaking through my windows). Likewise, if the perfect security software were created for a computer system, the weakest link would most likely end up being the user.

A single computer sitting idle will not fall victim to malware. Only when it is insecurely connected to a network or being interacted with by a user will it become vulnerable. This is because malware is created by a programmer, or ‘hacker’, on his or her own machine to purposefully to spread and cause harm. It is not simply a flaw or error in the operating system, that is, the software that communicates with the hardware of a computer. In the years prior to the ubiquity of the internet, the only way malware could spread between machines was by using a form of physical media (e.g., floppy disk, CD, or USB drive). Therefore, if one knew that the source of their physical media was legitimate, their computers would remain safe and unencumbered ("How Does A Computer Get Infected With A Virus Or Spyware?"). However, in this internet age we live in, information is easier to exchange between machines than ever. This has been extremely beneficial on many fronts, but has opened a new way for hackers to access our personal data.

Still, as previously mentioned, infecting a computer with malware requires user intervention. If you have ever searched the internet for free software (legal or not), then you have most certainly seen those fake, flashy download links whilst browsing. They draw the eye and are often larger and more obvious than the actual legitimate download link. This, as you can imagine, is done on purpose to encourage naive or inattentive users to install malware onto their machine. There are many other ways that harmful software gets onto a computer, such as opening email attachments, accepting terms and clicking checkboxes without reading, and downloading legitimate software that has been infected with a virus ("How Does A Computer Get Infected With A Virus Or Spyware?"). While some antimalware software and internet browsers have network monitoring to try and dissuade users from navigating to and downloading from certain websites, often it is not until the software is on the computer that it can be deemed as potentially harmful.

Even with the ‘best’ antimalware software, no system can be completely protected. Antimalware software works by scanning a computer’s file system and cross-referencing locally stored files to a database of known potentially unwanted programs, or PUPs (Walton). If you happen to use the antimalware program Malwarebytes, provided for free by your friendly neighborhood Pitt help desk consultants, you may notice that it updates quite often. In fact, Malwarebytes updates their database multiple times each day to provide its users with the most up to date security. Since the companies creating the databases of PUPs are not also creating the malware, they can only retroactively add information to the database after it is discovered. This means that a machine must first become infected with malware for it to be added to the database (Walton).

Since no perfect solution to prevent a malware infection on a machine exists, it is the responsibility of the user to apply best practices. On a personal machine, the risk of malware, or at least the damage that can be done by malware, is low. The data stored on my personal computer’s hard drive does not contain government secrets or new patent ideas. However, when dealing with businesses or government, this can become a much larger issue.

Large enterprises must deal with vast amounts of technological security in order to keep their intellectual property, records, and other private information away from prying eyes (“Don’t Be A Billy”). When a company owns and manages all the computers on their network, this makes security a bit easier. On corporation-administered laptops, the information technology department can set restrictions on its users, such as not allowing for software installation without the administrator password. While this is often seen as an inconvenience by the user because it blocks completely legitimate software from being installed, it also blocks the installation of malware, keeping that user as well as the rest of the company safe (“Best Practices For Enterprise Security”).

Some companies allow workers to use their personal devices instead of a company controlled laptop. This has its advantages, such as reducing the need for technology training sessions as well as reducing corporate spending, but can lead to increased lapses in security. If a user’s device has malware installed when it connects to the company’s network, then the whole cyber infrastructure may be at risk. Letting unrestricted employee devices onto a network has been likened to “getting unwrapped candy at Halloween,” as it is impossible to know what has happened to it and where it has been. For this reason, companies often require that users install antimalware software on their system and stress the importance of keeping it regularly updated (Howley).

Even if all systems accessing a network are malware free, this still does not leave the network free from potential harm. As one could probably assume, not all the information stored on a server should be accessible to all users. Therefore, a hospital janitor who only needs to connect her phone to the Wi-Fi to play music does not need access to a patient’s files as a doctor might. This is where multiple user accounts come into play. On a home network, a single password is usually enough protection because everyone who has the password probably wants to connect to the entirety of the internet. In an enterprise setting, different people have different roles and therefore need access to different data on the company’s internal server. Most likely no one would spend the time or energy to try and hack into the aforementioned janitor’s account, but the CEO may have access to some data that is valuable to a hacker.

In the primitive days of network security (and unfortunately sometimes today), hackers could try using default passwords to hack into systems (think ‘password’ or ‘letmein’). If that didn’t work, hackers could try and guess all combinations of letters and numbers until one did the trick. These methods are called “brute force” approaches to hacking, and while still sometimes feasible today, they mostly take too long to be efficient techniques. Instead, hackers talk their way into obtaining a user’s credentials by way of social engineering. Social engineering is “a collection the techniques used to manipulate people to performing actions or divulging confidential information,” according to Microsoft technology writer Troy Arwine. “Basically, it’s applied used car sales tactics … in order to trick people [into] giving out computer passwords and security codes over the phone, by mail or in person.”

You might suspect that higherups in a company wouldn’t be senseless enough to fall for such mind games, but Arwine suggests otherwise. If you’re confident, can impersonate a help desk employee, and act like you are helping the victim, very often all one must do is ask in order to receive a password. This method is often easier and quicker than brute force. These techniques are exactly the reason why Pitt as well as other schools around the country are enacting multi-factor authentication. Instead of brute forcing or social engineering a password out of a valid user, a secondary, dynamic code must be entered or cell phone app must be interacted with before a successful sign in occurs. This greatly decreases the chances of a hacked network (Arwine).

Diving into the rabbit hole that is network security can seem scary. From lurking malware to socially skilled hackers, it is as if you are being attacked from every direction. However, with careful internet navigation, an updated antimalware program, and a strong, secret password, you should not browse in fear. Leave that stress to the IT department.

Work Cited

Arwine, Troy. "Why Social Engineering Always Works :(". *"Stay Safe" Cyber Security Blog*, 2007, https://blogs.technet.microsoft.com/staysafe/2007/08/07/why-social-engineering-always-works/.

"Best Practices For Enterprise Security". *Microsoft Developer Network*, 2017, https://msdn.microsoft.com/en-us/library/cc750076.aspx.

"Don't Be A Billy". *Youtube*, 2017, https://www.youtube.com/watch?v=nPR131wMKEo.

"How Does A Computer Get Infected With A Virus Or Spyware?". *Computer Hope*, 2017, http://www.computerhope.com/issues/ch001045.htm.

Howley, Daniel P. "Should You Allow Personal Devices On The Company Network?". *Laptopmag.Com*, 2017, http://www.laptopmag.com/articles/should-you-allow-personal-devices-on-the-company-network.

Roy, Abhirup. "Avast Worth 'Upwards Of $2 Billion'; No IPO Before 2017". *Reuters*, 2017, http://www.reuters.com/article/us-avast-ceo-idUSKCN0SN2MJ20151029.

Walton, Andy. "How Does Anti-Malware Work? | Synonym". *Classroom.Synonym.Com*, 2017, http://classroom.synonym.com/antimalware-work-15689.html.