**IT, Security Threats, and General Internet Safety**

Information technology is a somewhat new field, which means that the general understanding of what it is may be lacking. To put it in the ~~most~~ simplest of terms, information technology is the study of computers and other digital devices. Though, that may be misleading, because is it not true that computer science also studies computers? The definition of information technology can be further refined by determining the difference between the two somewhat related fields. Information technology at its core focuses more on installing and maintaining an already designed computer system, this is in contrast to the field of computer science, which can include more of the design and development aspects of a computer system (Bhaumik). That being said, how would an information technology professional go about maintaining a computer system, and what would they have to maintain against? Security threats are a well-established issue within the field of information technology that professionals have to protect and maintain against. These threats are neutralized by using network security tactics and strategies that include firewalls, as well as increasingly complex forms of authentication. Protection against security threats can also be handed off to individual users, by using virtual private networks and private browsers on the internet.

Knowing how to protect oneself on the internet is important, but it is first necessary to gain a good working knowledge regarding some security threats, including what types exist and which ones are most prevalent. The types of security threats can be broken down into six different categories: viruses and worms, denial of service attacks, identity and password theft, data interception and modification, bandwidth piracy, and critical infrastructure attacks (Askoy, 300). Though, this paper will only describe worms, viruses, and identity theft in more detail, because among the threats listed, these are the most common. A worm is a very dangerous type of security attack because it is self-propagating and self-replicating, as well as being autonomous (Askoy 300). Autonomous, in this context, means that a worm is able to spread among computers without needing to be activated, like a virus would. For this reason, worms are generally more dangerous than viruses. Computer viruses work in a similar way to human biological viruses, they infect and then they spread (Wang, 47). A person would have to be in contact with an infected person to be infected themselves. In the case of a computer though, a file or program is the component that is infected, and the infection is only able to spread if said file is opened, or an infected program is executed (Askoy, 300). Viruses are commonly spread using a trojan horse, that is a seemingly authentic file or program (300). An example of a virus and trojan horse type of security attack in action would be if a company employee received a seemingly legitimate file on their internal email system from a hacker, that in turn was opened, releasing the damaging malware onto the company owned computer system. These types of attacks are particularly dangerous because they require specific antivirus software to prevent against them. Though, the way computer viruses operate contrasts vastly with how the process of identity theft works. Regarding identity theft, the threat is based less in actual malware like a virus or worm, and more in the physical world. While it is true that a hacker could use some form of software to gain unauthorized access to a system, it is also possible for a hacker to physically go and find a person’s system access information (302). An example of identity theft could simply be a hacker looking over the shoulder of an authorized company employee, and then using their information to gain unauthorized access to the company’s system (302). While each of these types of security threats can be described in increasingly complex detail, having a basic understanding is enough to grasp the importance of having a good, working security system. Describing these threats, even in brief, also highlights how important it is to have information technology professionals protecting sensitive information.

Regarding network security, there are three main categories that almost all approaches can fall into: privacy, access control, and authentication (Askoy, 304). Encryption is the main branch of privacy because it makes information only accessible by people who hold an encryption key (304). The information is private due to the encryption, hence the name. The overall process of encryption can be complicated, but in short, it scrambles information between the sender and receiver (304). The main branch of access control is the use of firewalls. If a person were only to have access to one type of security, a firewall would most likely be recommended because “A firewall is one of the most important network security measures that an institution or individual user can install.” (307). A firewall is like a filter for a computer network (Shinder, 54). This access control method is so important for network security because it filters out unwanted network traffic, while still allowing network traffic that you do want to go through (Shinder, 54). The last aspect of network security, authentication, has a branch called biometric identification (Askoy, 311). Biometric identification is also an extremely effective form of network security. Biometrics, as the name suggests, uses a human’s unique characteristics to secure some form of computer system (311). An easy example of this is fingerprint and facial recognition on iPhones and other similar devices. The above described network security options are in some ways accessible to the average, everyday user, but it there are definitely more user-friendly options for personal network security that don’t involve learning how to install a firewall.

Accessible personal network security is rooted in having a good understanding how to be safe on the internet. Many of the forementioned types of network security become inaccessible if a person does not have the technical skill set to install and work with these systems. This is where basic and inexpensive internet safety tools come into play. If encryption and firewalls are out of someone’s reach, but they still want to be safe on the internet, they can use a virtual private network and a private browser to achieve their desired security. A VPN is an increasingly popular internet protection service, available to be used on a wide array of devices. It works by masking a user’s real identity, connecting to a secondary server that is in a different geographic location (Held, 2). When using a VPN, a user could be located in New York, but their computer would say that they were located in London. This is useful for general internet protection, but a virtual private network may not protect against malware. Using a private browser is also a good way to stay safe and anonymous on the internet. The browser called Tor is said to be one of the best, but it is also known to slow down internet connection. VPNs and private browsers are just two things someone can use to increase their safety on the internet but being safe on the internet in turn increases overall network security and lessens susceptibility to malware that could be very damaging.

Information technology faces a large seemingly overwhelming issue when it comes to security threats, like viruses, worms, and identity theft. But by using various types of network security, professionals within the field can combat against them. Firewalls, encryption, and different types of authentication are all extremely effective methods of network security that allow them to do so. Individual users are also able to gain a more secure personal network simply by using a VPN or a private browser.

Works Cited

Aksoy, Pelin, and Laura DeNardis. Information technology in Theory. Boston, Mass: Thomson Course Technology, 2008. Print.

Bhaumik , Kaushik. “What's The Difference? Computer Science vs Information technology.” *Computer Science vs Information technology? Career Outlook*, 22 May 2019, www.fieldengineer.com/blogs/whats-the-difference-computer-science-vs-information-technology.

Held, Gilbert. Virtual Private Networking a Construction, Operation and Utilization Guide. John Wiley, 2004.

Shinder, Thomas W. Best Damn Firewall Book Period. Syngress, 2007.

Wang, Wally. Steal This Computer Book 4.0 What They Won't Tell You about the Internet. 4th ed., No Starch Press, 2006.