**Best Practices for Network Security**

Corbin Osman

American Public University System

ISSC421 – Computer and Network Security

Dr. Shoraka

09/24/2023

**Introduction**

Technology around the world continues to grow at rapid and exponential rates. Businesses, organizations, institutions, and even homes contain various forms of technology, ranging from accounts, devices, servers, and networks. With the vast changes and growth in technology, it is important that security of devices and networks remains a priority. Confidential and sensitive data, along with business and personal resources, are often contained within these systems and networks, and both users and administrators alike should focus on ensuring their security.

This paper will focus on technology networks and some of the strong practices to secure them from unauthorized parties and access. The field of networks and the importance of securing them will first be explored, followed by several forms of network security. Security best practices will then be addressed in both the home and professional environments, and the paper will conclude with a summary and review of the material learned. The scope and purpose of the paper are to help readers learn about the importance of network security and teach strong practices to secure them. Establishing strong network security practices allows individuals and businesses alike to protect against attacks and viruses, protect confidential and sensitive information, and secure accounts, systems, and networks from unauthorized access.

**Definition of Network Security**

To understand network security and what it entails, it is first crucial to understand what a technological or digital network is. A simple definition is that a network consists of two or more computers which are connected to exchange electronic communications, share files, and access resources (Winkelman, 2013). A network can contain various components, such as user accounts, computer devices, internet routers, mobile devices, and external drives. Additional components that may be present within a digital network are gateways, bridges, switches, and access points (English, 2022). These devices and components can be used together to form a network in which electronic communication and functions can be performed.

Network security is the process of securing a network and the devices contained within to meet the needs of the network’s users and protect information and resources. Network security is best achieved when technologies, processes, policies and devices are combined, and the designed security works to protect a home or professional network from unauthorized access and changes, potential network attacks, and unnecessary downtime or loss of resources (Swanagan, 2023). Common components of a network that should be secured are devices such as laptops, desktop computers, and mobile devices, user and administrator accounts, network and server hardware, and external hardware. Securing each of these components will increase the overall level of security across the network.

**Importance of Network Security**

The security of a network and its components is critical in both personal and professional environments. The devices and accounts individuals use on a daily basis often contain confidential and sensitive personal and business information, which are common targets of attackers and malicious actors. They may also target systems and accounts for personal use, whether they be local computer user and administrator accounts or personal online website accounts. Network security helps to keep this confidential and sensitive information safe from attackers while also ensuring that the network remains secure and available for authenticated users (Barney, 2022). User accounts can be secured so that their true owners have trusted access to their accounts and resources without worry of unauthorized interference.

In home environments, malicious parties may try to gain access to a network for various reasons. They may be searching for personally identifiable information, such as one’s social security number, date of birth, medical information, and bank and credit account numbers. This information could be used for personal gain, or attackers may sell it to others. Additionally, attackers may target a network with the goal of taking it over. Their intent may be to hijack a network temporarily or permanently for personal gain, and both are possibilities that users should be prepared for.

Business environments also contain and share confidential and sensitive information about clients, employees, and business plans. Malicious parties may attempt to capture and use this information, along with other unsecured data they may be able to locate. Attackers may also try gaining access to user and administrator accounts to make changes to network settings and devices. For these and other reasons, securing any type of network is a crucial step in protecting against potential threats and vulnerabilities.

**Forms of Network Security**

Now that an understanding of network security is in place, let us look at different forms of network security and how they are utilized. In a simple network, one can expect to find user and administrator accounts, computer devices and systems, and network hardware and software. Knowing how each of these functions in a network is important to decide which forms of security will be used to protect and secure them.

**User Accounts**

In both personal and professional environments, user accounts are a core part of computer devices. These accounts allow individuals to access a computer system and perform various tasks and activities. A personal account might be found on a laptop or desktop computer within one’s home, whereas business accounts might be found on business computers and devices. Securing these accounts will help to prevent unauthorized individuals from accessing the accounts and the devices they are on, which in turn helps to protect and secure the data and information contained in them. For home and business users, this involves using strong credentials and regularly changing them. In business environments, policies can be set that require users to routinely update their credentials. When designing credentials such as passwords, use a combination of letters, numbers, and symbols for the characters to increase credential security (Freedman, 2023). Where possible, it is also helpful to implement two-factor or multi-factor authentication for accounts. This further ensures that the individuals accessing the accounts are the legitimate users who own them.

**Computer Devices and Systems**

Computer devices and their systems are also of high value and should be secured. Physical components such as desktops computers, mobile devices, and even cables and power supplies should all be secured and monitored so that unauthorized use or access is prevented. Digital components such as the operating systems, system settings and policies should be established and maintained by home users or security administrators respectively. Malicious parties may be able to gain access to computers and other devices if they are not properly secured, which could prove disastrous in both home and business environments.

**Network**

In regard to the network and all of its components, there are many ways to secure and protect them from unauthorized individuals. In home environments it can help to utilize software and services such as firewalls, VPNs, and antivirus software to secure all devices connected to the networks. These can also be of great aid in business environments where there are many devices connected to the network, and similar devices which can be of use are intrusion detection and instruction prevention systems. Additionally, administrators can establish policies and protocols that are to be followed by all employees that govern proper use of the network and everything connected to it. Routine review can also be performed to ensure that no unauthorized actions or modifications have occurred on the network or its connected devices and accounts (Naz, 2023).

**Network Security Best Practices**

Many strong practices have been mentioned previously when exploring forms of network security, and here we will further discuss best practices and good habits to employ for the securing of networks. While many of these practices can be employed in both home and professional environments, the sections will be separated for the purpose of easier reading.

**Best Practices in a Home Environment**

In home environments it is often the role of the homeowner or another within the household to set up and manage internet and network devices. User accounts, internet and router devices and settings, and computer devices are all potentially a part of the home network and should be considered with security in mind. Similar to strong user account credentials, it is important to create a strong password for the router to protect the network from unauthorized access. Regularly changing the password is also recommended in the event that third parties have gained access to the network previously. It can also be helpful to regularly review devices currently and previously connected to the network to ensure that they are familiar. If there are devices which are unrecognized, it may be best practice to remove them (Anders, 2023).

For personal accounts, there are several practices which are also good to employ to prioritize security. With credentials, it is recommended to avoid using the same password across multiple accounts, and when possible do not remain logged in to systems or online accounts that could be used by others. Avoid keeping credentials written down or stored in a location that could be accessed by others, and if there is sensitive information kept on paper ensure that it is securely stored (Seattle University).

To protect physical devices and hardware in a home, having home security such as cameras and alarms can help to deter malicious parties from entering. Locking up devices and additional hardware components when not in use can aid in keeping them secure. Locating important devices such as the router and other network components in a central, secured location will aid in protecting the devices while also offering strong connectivity to users.

**Best Practices in a Business Environment**

Moving on from the home environment, there are several strong practices that should be employed in a business setting. Starting with user accounts, it is important that each account is set up with proper permissions identifying what the account does and does not have access to. Also known as the principle of least privilege, user accounts should only be permitted to perform the functions they need in order to complete their assigned work tasks. This ensures that unauthorized actions or modifications are not accidentally or intentionally performed. To access these accounts, strong credentials and multi-factor authentication should be considered. This will help ensure that accounts can remain secure even if an attacker steals a password, as they would need to go through another form of authentication as well (Staino, 2022).

While not directly associated with a technological network, physical locations such as an office space that contains network technology can also be secured by multi-factor authentication. Additional forms of authentication such as a keycard, passcode, or biometric identification can be used together to ensure that only authorized individuals enter the secured location. This in turn helps to further secure physical hardware components that may be targeted by other parties. Important physical hardware such as routers should be secured in a central location which offer strong connectivity to users.

Business environments often have local area networks (LANs) and wide area networks (WANs), both of which should be developed with security in mind. Local area networks can utilize a firewall with a single router access point where possible to limit the broadcast of the network. Using strong security encryption such as WPA2 will help to secure network traffic for users, and having additional software such as antivirus programs can help to monitor and protect against potentially harmful data (Zencc). Wide area networks will benefit from the previous suggested practices as well, and in addition the utilization of virtual private networks may be optimal. This will help to further heighten the overall security of network communications and operations. Managing devices connected to the network and only allowing those that need to be connected will help avoid unnecessary connectivity issues. In all network environments devices, accounts and policies should be regularly monitored and updated to ensure that security is up to date.

**Future Trends**

Technology is an ever-growing field, which makes it important to implement newer technologies and practices to ensure that security is at its best. Utilizing newer encryption methods as they are released will help ensure that the network and the data it contains are secured from newer types of network attacks. In professional environments it is important to educate users on strong security practices while also providing them devices that offer strong security. Additional components that will continue to be strengthened such as VPN and firewall technology should be implemented where possible to heighten overall security of the network. These will continue to receive updates and patches to protect against newer types of attacks and viruses that may be a threat to the network. In all environments it is best practice to ensure that devices, systems and services remain up to date to protect from potential threats and vulnerabilities.

**Global Implications**

With most of the world relying on networks and their connections, the security of networks and their resources should be a primary focus in homes and businesses alike. As all users learn and implement best practices they will contribute to their home and business environments and the security therein. Around the world newer technologies are being developed, both for good and for bad. Implementing the newer security technologies and practices into networks will allow individual homes and businesses to strengthen their network’s security and protect against threats. Establishing strong, secure networks aids in the prevention of successful network attacks.

**Conclusion**

In review, establishing and implementing strong security practices in both home and business environments is essential for the security of networks. Networks that store or transmit confidential information will be at risk of attacks, making it vital that homeowners and administrators understand what may be targeted on their network and how they can secure those components. Learning about and teaching these best practices to others that may use the network will also increase overall levels of security as users work together to ensure that the network remains secured.

Strong security practices pertaining to account and device security may be viable in any location where user accounts and devices are in use, and users can benefit from applying such practices in every area of their digital life. With the potential for attacks to grow in number and intensity, establishing a strong network now will provide users and administrators a secure and trusted environment in which they can store and transmit data, connect to the internet, and perform daily personal and work tasks.

Resources

Anders, D. (2023, September 16). 10 Expert Recommended Tips for a Secure Home Wi-Fi. *Cnet*. https://www.cnet.com/home/internet/stop-home-network-hackers-top-10-tips-to-protect-your-wi-fi-security/

Barney, N., & Lutkevich, B. (2022). Network Security. *Tech Target*. https://www.techtarget.com/searchnetworking/definition/network-security

English, J. (2022, April). An Introduction to 8 Types of Network Devices. *Tech Target*. https://www.techtarget.com/searchnetworking/tip/An-introduction-to-8-types-of-network-devices

Freedman, M. (2023, June 22). 18 Ways to Secure Your Devices from Hackers. *Business News Daily*. https://www.businessnewsdaily.com/11213-secure-computer-from-hackers.html

Naz, Z. (2023, July 13). What is Network Security? Importance, Types of Protection. *Knowledge Hut*. https://www.knowledgehut.com/blog/security/network-security

Seattle University. (n.d.). User Account Best Security Practices. *Seattle University*. https://www.seattleu.edu/its/support/guides/user-account-security/

Staino, P. (2022, May 18). Best Practices for Network Security. *The Ascent*. https://www.fool.com/the-ascent/small-business/endpoint-security/articles/best-practices-for-network-security/

Swanagan, M. (2023, February 7). What is Network Security? (Benefits & Types Explained). *Purplesec*. https://purplesec.us/network-security-types/

*What Is A LAN? Why Secure Local Area Network? - Zencc.net*. (n.d.). zencc.net. https://zencc.net/blog/what-is-a-lan-why-secure-local-area-network

Winkelman, R. (2013). An Educator’s Guide to School Networks. *Florida Center for Instructional Technology*. https://fcit.usf.edu/network/