Hello Class, One of the first security protocols was Wired Equivalent Privacy (WEP), which was designed in 1997. WEP is no longer used in newer devices, but can still be used in older devices. The reason for WEP becoming obsolete is because hackers developing ways to reverse-engineering and cracking the encryption of the system. There was also WI-FI Protected Access (WPA), WI-FI Protected Access 2 (WPA2), WPA2-PSK, WPA2-Enterprise, WI-FI Protected Access 3 (WPA3), WPA3-PSK, and WPA-Enterprise. Something that is concerning in today’s wireless security are data breaches and malfunctions, which can cost users and companies money. Hackers can crack and decrypt passwords. Hackers can also use packet sniffers, which are computer programs that monitor the traffic on a user’s network and intercept their data and provide then with contents about the user.

Raphaely, E. (2022). Everything You Need To Know About Wireless Security. Retrieved 20 August 2022, from <https://www.securew2.com/blog/complete-guide-wi-fi-security>

Hello Class, some reasons why hackers hack is to steal and leak information and data. Another reason is to take down and disrupt services, and networks of a company. They can do that by overwhelming the server, which makes it crash. Another reason hackers may take down a network is to prove a point. Hackers may also want money. Other hackers may hack to expose and for justice, being hacktivist, idealist, and having political motives. The worst result into hacking my home network would be stealing my card information and stealing my money, and gaining access to my emails.

Agarwal, H. (2022). 5 Key Points Why Do Hackers Hack | Ethical Hacking. Retrieved 21 August 2022, from <https://www.appknox.com/blog/why-do-hackers-hack\>

Hello Katelyn, I agree with you public Wi-Fi is risky to use, because like you said if a hacker gains access to the public network, they can get ahold of not only your information but others that use that public network. I also agree with you that stored information, like passwords and credit card accounts, would be in danger if they get ahold of the network.

Hello Class,

The requirements for Virtual Machines (VMs), are a Processor minimum of 8 core Pentium 4, 2.8 GHz, and a recommended 16 core 2.6 GHz CPU. A RAM minimum of 8 GB and a recommended 16 GB, Hard drive minimum of 50, with a recommended 200 GB. Hyper-V requirements include: a 4 GB RAM. A 64-bit processor

System requirements for Virtual Machine Manager. (2022). Retrieved 21 August 2022, from <https://docs.microsoft.com/en-us/system-center/vmm/system-requirements?view=sc-vmm-2022>

Hello Class, some features in Hyper-V that are common is Networking, Encryption support, Virtualization, Host resource protection, Storage quality of service (QOS), and Shared virtual hard disks. Networking saves time and money and is one of the most helpful features, it also improves the aspect overall. Encryption support, which is helpful for encrypting valuable data. Virtualization is a feature that is used as a line of defense and helps you be protected. Host resource protection helps cloud hosting environment’s function and not worry about resources. QOS helps measure and limits the storage of VMs. Shared virtual hard disks allows you to share a disk with other VMs that are grouped.

Afanasyev, I. (2017). New Hyper-V 2016 features that you should know about. Retrieved 22 August 2022, from https://www.veeam.com/blog/hyperv-2016-important-features.html