Human-Computer Interaction and Cybersecurity Handbook

Abbas Moallem

Smart home network and devices

Publication details
Abbas Moallem
Published online on: 24 Oct 2018

How to cite :- Abbas Moallem. 24 Oct 2018, Smart home network and devices from: Human-Computer Interaction and Cybersecurity Handbook CRC Press
Accessed on: 15 Aug 2023

PLEASE SCROLL DOWN FOR DOCUMENT

Full terms and conditions of use: https://www.routledgehandbooks.com/legal-notices/terms

This Document PDF may be used for research, teaching and private study purposes. Any substantial or systematic reproductions, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The publisher shall not be liable for an loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.
chapter nine

Smart home network and devices

Abbas Moallem

Contents

9.1 Introduction ........................................................................................................................ 177
9.1.1 Passwords ............................................................................................................... 178
9.1.2 Beyond passwords .................................................................................................178
9.1.3 Network usability problems ................................................................................. 178
9.1.3.1 No professional administrators .................................................................... 178
9.2 Home networking routes and feature management ....................................................179
9.2.1 Acquiring a router .................................................................................................180
9.2.2 Connecting router to network ..............................................................................180
9.2.3 Managing home network ..................................................................................... 181
9.2.3.1 Setting user name and password .................................................................... 181
9.2.3.2 Home networking configuration .................................................................... 183
9.2.3.3 Home networking and user mental image .................................................... 184
9.2.3.4 Home networking devices and firmware ..................................................... 185
9.2.3.5 Internet of things ............................................................................................ 186
9.3 Solutions and challenges ............................................................................................. 186
9.3.1 Home networking and privacy ............................................................................ 186
9.4 Conclusion ..................................................................................................................... 188
References............................................................................................................................ 188

9.1 Introduction

With the speedy expansion of the Internet and Internet-based technologies in homes, the connection of a household to an Internet service provider has become as common as connecting to the basic utility providers for electricity and gas. According to Internet Live Stats (2016), 88.5% of the United States, and 40% of the world population, are Internet users. Users, moreover, are not typically satisfied with having just their computer connected to the Internet. They need wireless connections at home for their computer devices, and cross access connections that allow them to view, modify, and control their computer devices. Users also need to control and monitor security and problem-solve to maintain an uninterrupted Internet connection and a secure network.

Not long ago, home Internet connections were limited to computers. Now, gradually, within a “smart home” (Cheng and Kunz 2009), a wide range of computers and computerized devices can be connected and interact globally and with each other. However, after initial configuration, users are advised to conduct frequent monitoring of the interactions of each device and to frequently check security settings of each device (updating firmware, viewing the connected devices, changing passwords, and so on). Frequent monitoring provides a method of examining the router to ensure that it has not been hacked. For instance,
monitoring can display all the devices connected to the user’s network, so any unauthorized devices can be easily identified.

Today, roughly 9 in 10 American adults use the Internet (Pew Research Center 2017). It is estimated that households have 10 connected devices now, projected to rise to 50 connected devices per home by 2020 (Phadnis 2016). More devices mean a wider number of systems and accounts that require user management. For example, managing a switch box that turns one Ethernet connection into several, allowing multiple wired devices to connect to the Internet without overloading the router, or eliminating bottlenecks to make sure that the modem/router can handle the broadband speeds.

Despite the increasing value of the information stored on devices connected to a home wireless network, users are also presented with the threat of network privacy and security breaches. User habits, and knowledge of network features and safety, are thought to have a great impact on risk rates.

9.1.1 Passwords

Most users are under the impression that a complex password will keep them safe from breaches. However, reports indicate that even a complex password is not necessarily a secure password (McMillan 2014). In addition, in October 2017, new research from security researcher Mathy Vanhoef of KU Leuven, in Belgium, found that a flaw in the cryptographic protocols of Wi-Fi protected access II (WPA2) could be exploited to read and steal data that would otherwise be protected. In some situations, this vulnerability even leaves room for an attacker to manipulate data on a Wi-Fi network, or inject new data into it. In practice, that means hackers could steal users’ passwords, intercept their financial data, or even manipulate commands to, say, send their money to hackers (Newman 2017).

9.1.2 Beyond passwords

Users who follow the basic device setup guides, but who want to further configure the security of their devices, are struck with two deficiencies: the lack of the knowledge of what proper preventative measures are and the lack of the skill to implement preventive actions [how to do it using device user interface (UI)]. Users with limited networking experience generally claim that managing a home network beyond the basic setup protocols of the devices is a tedious, difficult task.

People who have a home networking device have more than likely experienced a variety of home networking UI issues. They might have even asked someone with technical knowledge to help with installing, connecting, and configuring the device that they acquired or had problems with. No matter the type of device—a wireless router or an interactive TV can very quickly become complicated.

9.1.3 Network usability problems

Edwards et al. (2011) concludes that “network usability problems run deep because the technology was initially developed for research labs and enterprise networks and does not account for three unique characteristics of the home: 1) lack of professional administrators, 2) deep heterogeneity, and 3) expectations of privacy.”

9.1.3.1 No professional administrators

The issues that seem to be related to user difficulties with network security technology are that UIs are built for advanced users with information technology (IT) backgrounds,
heterogeneity in users and home networking configurations, and the complexity of problem-solving home network issues. For example, Grinter et al. (2005) noted that home users are often unable to verbally articulate accurate information about their networks or even a mental model of their network, which has been shown to be related to their level of expertise. In addition, most people have neither the time nor the inclination to be continually vigilant for new threats on their home network; they are focused on getting their work done (Dourish et al. 2004).

There is a need to understand some of the network vulnerabilities in an average household and how to thwart a hacker’s future attempts to attack. Households will have to improve their ability to detect and correlate attack activity to respond to increasingly sophisticated threats that accompany these high-growth technologies. With that said, security experts state that no single product or vendor can cover every possible threat angle. Home network users must understand our worldview of cybersecurity should be a systematic framework. With this perspective, homeowners can understand how to prevent access to digital spaces such as bank accounts as well as physical devices such as smart TVs. However, with today’s technologies, this level of security is harder to obtain when the user does not have an advanced level of cybersecurity knowledge and skill.

One of the main demographic groups of Internet users in most developed countries is older adults. Older adults benefit from the expansion of the smart home. They seem to have an overall positive attitude toward this technology (Demiris et al. 2004). The usage of health monitoring sensors or security devices in the home to enhance their lives is a good example of how these users benefit from this technology. However, the ease of use for these applications is crucial for secure usage by older adults especially if they are using medical monitoring devices. Consequently, this population can be even more vulnerable to cyberattacks, identity theft, and social engineering.

Home network devices should make it easy to add computers, or any other smart appliances to the home network, and establish interactions by offering users easy-to-use secure settings. In the following section, we will provide a summary of common issues and discuss potential solutions.

9.2 Home networking routes and feature management

The modern home generally uses a router connected to an external network (Internet service provider or ISP) as the centerpiece of home networking. The router provides wired and wireless Internet connection to all devices in the home. Despite the extent of home networking, the large number of users, and the potential impact on home users’ security by nefarious actors and schemes, the number of investigations into home security vulnerabilities and breeches is relatively very small.

In general, home security needs to be managed at each of three layers: by the ISP, by the home networking device (router), and by each connected device.

According to Cisco Systems, Inc. (2017), security breaches at the ISP provider level include the following:

- Denial-of-service and distributed denial-of-service (DDoS) attacks, which are aimed at disabling access to various Internet services for legitimate users
- Excessive traffic and resource depletion caused by infected machines, which can generate problems for service providers
- Attacking the border gateway protocol (BGP) routing and injecting faulty BGP routes for traffic redirection, one of several techniques attackers use to obtain “interesting” traffic
• Stealing of domain name system (DNS) information and using this to redirect Internet traffic to serve the needs of people with criminal intent
• Device compromise, including breaking into vital components of the infrastructure and modifying their configuration

These security issues are handled by ISP companies and will thus not be reviewed in this chapter.

The second level of security is the responsibility of end users in each home, or small businesses, through the UIs of the router.

9.2.1 Acquiring a router

An ISP provides a router or users acquire one from the multitude of brands available on the market. The selection of a router is always a tedious task since most of the time, people might not know exactly what the meaning of the information provided on the packaging of the device is. Figure 9.1 shows the information on three major brands of routers. Phrases such as “dual-band gigabit,” “up to 340 bps,” “300 + 300 Mbps,” and “tri-band 2.2 Gbps combined speeds” used on the packaging are not likely to be understandable to an average user. A survey of home networking users conducted in 2011 by TMC News might still be relevant. This survey showed that only 1% of the respondents bought their particular router because of its reported ease of use, while 22% of respondents bought based on the speed of the router and 17% bought based on its price. When participants were asked about purchasing a new wireless router, speed remained the top factor and increased in importance to 37%, while ease of use moved up to the second priority at 17% (TMC News 2011). One might think that this still would be the case.

9.2.2 Connecting router to network

Over the years, most brands have improved the installation process, through simple wizard and smartphone and tablet apps that users can use for first-time and subsequent installations. Smartphone and tablets did not necessarily simplify the task. Having said that, the user following the instructions can be quickly connected to the Internet and with a password that is offered during the installation or a self-specified password. Once users are connected to the Internet, they consider that their task is completed and write the password for further use. However, from the security point of view, the issues...
start from the moment that the user is connected to Internet. Despite continuous progress in hardware, improvements to managing the security settings of these devices are still complex.

9.2.3 Managing home network

Today, most people can easily connect their newly purchased home routers to the Internet using the Quick Guides and helpful Tech Support line that vendors provide. However, users commonly agree that managing home networks is still a difficult task that is out of reach for most users with limited networking experience.

It is probably unrealistic for router manufacturers to require such knowledge on the part of their customers. Some of the issues in the way of securing users’ networks are (1) an extremely personal device and attack vector-filled environment where there is (2) no professional administrator to maintain a (3) heterogeneous collection of consumer technologies that (4) are increasingly cyberphysical and sensor rich. The combination of these factors leads to an array of attacks and complicates the design of defenses for home devices (Denning 2013).

Some research suggests that instead of having individuals manage their networks, they should “outsource the management and operation of these networks to a third party that has both operations expertise and a broader view of network activity” (Feamster 2010). Yang et al. (2010) suggest that it could be better to provide the home user with a conceptual model that can help them understand key aspects of networking and with visual tools to do a range of common tasks. Another approach has been to try and improve router UI usability, enabling users to perform complex system management tasks independently for their home network (Moallem 2014).

Let us look at a number issues when managing a home networking router. A user must access the UI of a router in order to set and manage a network. The UI always acts as the point of access, regardless of the brand, range, remote access, and other provided functionalities of the router such as universal serial bus (USB) ports or guest networks. To do so, in addition to username and password settings, users must deal with a variety of other router security settings for device management.

9.2.3.1 Setting user name and password

After initial password setting at installation, using the default router password or user-selected password, the user should be able to change their password. In a study conducted by the author with 104 undergraduate students (63 males and 41 females with 72% between the ages of 18 and 25), it was found that 91 (88%) owned a router. This group was asked if they knew how to change their network password. If they answered “yes” to knowing how to change their network password (50 participants or 48%), they were asked how they would go about making such a change. The explanations of how to change their password by those 51 who responded “yes” showed that 23 (43%) would do it by entering the IP address of the router and 8 (16%) would go to the provider site. The remaining 20 (41%) students did not provide a clear or accurate response, with answers such as “asking my brother” or “Google search.” Considering that the people who responded with “IP address” and “service provider” as those who actually knew how to change the router password (23 participants—22% of all participants), even if we consider that the survey was a self-reporting one and participants’ responses may have been completely wrong either way, we can conclude that among the group, approximately one-third might be able to change their router password. However, we can also extrapolate the level of
understanding of this group of people about how to manage a router. If young college students do not have the understanding that they can log in their router user interface to change the password, then we can assume that the understanding will be even less among the general population that owns a router for home networking. According to PEW Research Center (2017), “undergraduate and graduate students differentiate themselves more clearly when it comes to home broadband access, as more than nine in ten undergraduates (95%) and graduate students (93%) are home broadband users—well above the national adult average of 66%.”

Today’s user is asked to set a more personalized password, keep the default settings, or switch to a desired name and password (surprisingly many users might not even remove the password or choose a very simple one). It is reported by Barker (2014) that more than half of all home routers are poorly protected using default or easily hacked password combinations such as admin/admin or admin/password.

The password setting has two layers. One sets a password for the Wi-Fi requiring, all devices to enter the password. The second layer sets a password to manage the router, access the admin UI of the device, and manage network security including the network password.

All the router brands have a preset username and password for the device and an IP address to access the device. For example, the Comcast Xfinity router generally uses the IP address http:/10.0.0.1 and “admin” as the username, with the default password “password.” According to a study (Moallem 2012), 9% of participants did not know what an IP address is, while 39% claimed that they thought they knew what it meant but were not sure (Figure 9.2).

![Figure 9.2 Understandability of the terminology used on home networking device UIs. The graph shows the percentage of participants who were not sure at all what the meaning of each term was (84 participants: 54% male, 46% female, 54% under 25 years).](image-url)
9.2.3.2 Home networking configuration

There is a variety of parameters that make it hard for users to configure and manage their networking devices efficiently. These parameters include channel selection, remote access to routers and devices, and IP selection. The growing number of devices that will connect to home networking systems increases the difficulties presented by each parameter. Apart from regulatory concerns, users must also be aware of standard practices undertaken when managing a wide variety of systems and accounts (Phadnis 2016). Even for a relatively small home network, managing the security of network each time that a new device is added can be a substantial challenge, and each device can introduce a new, substantial challenge.

As we have previously mentioned, to manage a home networking device, user must log in to the router UI to change or set configuration.

Let us take a look at a router UI that is provided by a major Internet provider to their clients in the United States (Figure 9.3). Looking at the main page of this device requires the user to understand the concept of the password for Wi-Fi and password to manage the device. Even if they are logged in to administer the device, they still need to have a good understanding of the terms. If users do not understand the meaning of the words or concepts used in the UI, how would they be able to manage security aspect of their devices?

Figure 9.3 UI of the router provided by the main ISP in the United States. Most people do not have a clear idea about the security mode and relationship with password and channel selection.
Figure 9.3 shows the UI of the router provided by Comcast, an ISP in the United States. Most people do not have a clear idea about the security mode and relationship between password, mode, and channel selection. All routers provide WPA2-phase-shift keying (PSK) [temporal key integrity protocol (TKIP)], WPA2-PSK [advanced encryption standard (AES)], and WPA2-PSK (TKIP/AES) as options. These modes or options encrypt a network with an encryption key, and each provides a weaker or stronger encryption. In fact, we have observed that many average users did not even understand the concept of encryption. Even if you search the Internet or read the device documentation, you can hardly see an easy explanation of these options, just an indication of which one is better to use. Therefore, people might randomly use one versus another or even go with an easy option without knowing the consequences.

Here is how Wikipedia defines WPA and WPA2:

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP).

WPA (sometimes referred to as the draft IEEE 802.11i standard) became available in 2003. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2, which became available in 2004 and is common shorthand for the full IEEE 802.11i (or IEEE 802.11i-2004) standard.

As it can be observed from the preceding terminology, the definition or explanations are very complex while it could just have said “strong password” like a simple lock or a more secure lock for better secure system. This would probably be more understandable for people.

All Wi-Fi broadband routers communicate over specific wireless channels. Like channels on a television, a number that represents a specific radio communication frequency designates each Wi-Fi channel. This type of UI is more appropriate for the IT professional than an average home networking user. Although routers allow user to choose the “channel,” the typical default channel setting is generally is set to “Auto,” presuming that most users will be satisfied with the selection of the device. To check this, one might just ask people who have a router about the difference between “5 GHz” and “2.4 GHz,” and it will quickly be noticed that people hardly know their meanings. Many of us have looked through the list of a dozen or so channels that the manual option of the router provides and wondered what they are and which one is faster, to no avail.

One of the fundamental issues in understanding the UI of the router by the users is the fact that they do not have a correct mental image of how the device operates.
Chapter nine: Smart home network and devices

systems or devices are working is essential. However, when the mental image of a system or device is incorrect, it is referred to as a “folk model.” Folk models are mental models that are not sufficiently accurate in the real world, leading people to incorrect decisions when their decisions are based on this type of conceptualized image. It has been observed that in technological contexts, users often operate with folk models rather than with a correct mental model of the system or device. If technology is designed on the assumption of a different mental model from that of the user, the desired behavior will also be different from what is expected when making decisions (Athhavanka 1997).

Wash (2010) conducted a qualitative study to understand users’ mental models of attackers and security technologies. In this study, the researcher investigated the existence of folk models held by home computer users.

The fact that most user do not know that their router has a UI that they need to log in to manage the configurations indicate this mismatch from user mental image and how the device operates.

9.2.3.4 Home networking devices and firmware

The increasing number of devices connected to a home network system creates additional endpoints, which adds more complexity to protecting security vulnerabilities. With some embedded systems on the rise, cyberattacks that focus on firmware rather than application or operating system levels are also on the rise. Choi et al. (2016) summarizes several types of firmware attacks as follows and suggests solutions such as firmware validation and update schemes.

- **USB firmware**: A USB memory stick is plugged into the system. The compromised firmware presents itself as a normal mass storage device but shortly installs a Trojan from the web to the compromised firmware, which is able to send system commands to manipulate the system.
- **Network interface card (NIC) firmware**: The firmware of an NIC is modified to control packets.
- **Hard drive firmware**: A hacking tool designed to reflash the hard disk firmware of a system with malicious code. It obtains the malicious code from a command server and then flushes the obtained code to the existing firmware, i.e., replacing the current firmware with a malicious one. The boot process of the system is also able to capture the disk encryption password or other passwords at the operating system level.
- **Battery firmware**: A battery contains an embedded microprocessor just as USB devices, NICs, and hard drives do. By compromising the battery firmware, it is possible to overheat the battery and even cause the battery to catch on fire.
- **Printer firmware**: A firmware modification which attacks a printer. This vulnerability allows the arbitrary injection of a developed malware into the printer firmware. There are multiple ways that the can be used to access the computer connected to home networking or alter and reroute print jobs, open saved copies of documents, or reset the printer to its factory defaults, or wiping out all users’ settings. This can happen by hacking into a network printer without security features. However, if the printer is accessible through the Internet, there is a variety of ways to hack into home networks. If the printer is not password protected, the task of the hacker is even much easier, although even a password-protected one will not stop hackers. One of the most efficient ways to avoid being hacked would be to acquire printers that support encrypted connections to and from personal computers (PCs) on the network and get rid of older printers that do not have security features (Geier 2012).
9.2.3.5 Internet of things

Gartner, Inc. (2015) forecasts that 20.4 billion connected things will be in use worldwide in 2020, and the total spending on endpoints and services (an endpoint device is an Internet-capable computer hardware device on a transmission control protocol/IP network) will reach almost $2 trillion in 2017. This development makes managing home networking even more fragile from a security perspective.

Botnets are a collection of Internet-connected devices, which may include PCs, servers, mobile devices, and Internet of things (IoT) devices that are infected and controlled by a common type of malware. Users are often unaware of a botnet infecting their system. A botnet might run one or more bots. Botnets can be used to perform a DDoS attack, steal data, send spam, and allow the attacker access to the device and its connection.

The Internet bot [a software application that runs automated tasks (scripts) over the Internet], Kelihos, and Asprox botnet, created on connected devices (even appliances such as refrigerators) can, for example, start a spam e-mail attack. TVs with built-in cameras and microphones pose another attractive category of targets, as do other previously innocuous household devices. The possibilities for IoT attacks are truly endless, but ultimately, such attacks are likely to be about money/profit.

There is a need to look into understanding how some of the vulnerabilities present them for the average household should a hacker attempt to attack.

Households will have to improve their ability to detect and correlate attack activity to respond to increasingly sophisticated threats that accompany these high-growth technologies. Security experts state that no single product or vendor can cover every possible threat angle (Huffington Post 2013). We must look into understanding how our worldview of looking into cybersecurity must be in a systematic framework that helps homeowners control access from physical device points such as smart TVs, smart cars, Wi-Fi-connected washing machines to digital spaces such as social media and bank accounts. This requires the user to have a level of technical know-how in networking and security, which would be unrealistic to enforce and maintain, given the rapid changes and advancement of technologies. The combination of this variety of factors can lead to the vulnerability of home networking to an array of attacks such as ransomware (Kaspersky Lab 2016).

9.3 Solutions and challenges

9.3.1 Home networking and privacy

Home and home-based small business networks are used by many users to connect their computers; cell phones; tablets; music storage devices; photo storage devices; and appliances such as games, smart TVs, and IP cameras to the Internet. Obviously, these devices contain the digital heart and life of the household. If a small home business is also being operated within this framework, the digital life includes, but is not limited, to all legal, tax, and property documents, pictures, and videos. Consequently, if a hacker could access these digital assets, it would be a big loss for every single member of that household. With the expansion of ransomware and identity theft, every single unprotected house is a favorable target for criminals. Making the target safer is the job of the home network manager. Sometimes professional services working for different legitimate businesses, such as law offices, private investigators, or even sometimes law enforcement agencies are also intruders (Goldstein 2015).

The only rational solution to make home networking more secure is to provide easy-to-use software that makes the task of managing the network for all level of home users...
accessible. In this way, user will be able to secure their networks easily with an easy-to-use UI. Until this happens, which may be a while away, home users need to learn how to and make themselves responsible for securing their network. There are several main steps that users of the household need to learn and understand. These include viewing and changing the password for wireless connection, turning on and off the guest network or guest network password, and setting parental controls to view a router admin UI; there is no need to have an Internet connection since users log in to the router software. After logging in to the router, the user can make all configurations or needed changes.

The first step is upon arriving at the admin UI login page, one should find a default username and password to log in. The default username and password are presented on the label of the router box or other documentation. Sometimes, even a Google search of the router model and brand can turn up the username of each brand. These days the admin password may not be an easy set password such as “password” but another configuration of letters and numerical characters. Upon successful login, three parameters need to be changed to secure home or small business networking:

- Change IP address to log in to the admin UI from default to user-selected IP address.
- Change admin UI password to a difficult long password to prevent somebody else using the default IP and password to log in.
- If possible, change username.

Following these changes, the user should set a user-friendly wireless network name and configure a reliable security password for connection.

One of the security measures for a small home business networking should be to separate the business user's network and pertinent computers from the Internet connection utilized by guests. Creating a guest network separates guest connection to the Internet from the user’s user home computers.

Educating all family members about possible home network vulnerabilities and cyber-attacks is another good measure to take. This is especially important for families with children who may have friends over. Children these days may be more skilled with computers than their parents or simply have the curiosity to explore other computers in a network, which can consequently lead to the use of the protection of a guest network to access private files on a computer on the network.

Another important measure to protect home networking is regularly changing the Wi-Fi password about every 3–6 months.

It is important that all home networking users shutdown their laptop and desktop computers when not in use. Otherwise, ransomware attacks could encrypt all connected device data including the backup on external hard drives.

Many routers have a USB port that allows users to utilize its internal storage device or simply share pictures or music through the router. It is recommended not to have the storage device be connected at all times to the Internet. The user should disconnect the storage device after back up. This would prevent users from becoming a victim of ransomware.

A virtual private network should always be used when working from home, even if using a “secure” work laptop. Also, a USB drive or any media storage device found from the street should never be used, especially on work computers.

The router should be checked for having a file transfer protocol (FTP) server. If one exists, it should be secured with a password or shut down.

The firmware of the router, the operating system on cellular devices, and the operating system on computers should all be updated from time to time or as soon as these updates...
are available. The firmware updates often include the security patches that would protect the device with the new known issues.

Besides these minimum security settings, the rest of security might be more complicated, particularly in the network with several different devices such as smart TV, gaming devices, smart plugs, and IP cameras.

The other fundamental way of protecting the home network is setting a firewall. A firewall is a barrier that controls data types in and out of your network. It can prevent spam sites from installing unwanted programs on your computer, protect your personal information from theft, and much more. Consequently, setting firewalls to maximum security would be another good security measure.

Managing the access of a specific site can be a particularly beneficial security measure in a home with children. This may include blocking certain specific URLs or sites by setting keywords. This can be achieved by creating a black list and white list.

Lastly, using DNS services such as OpenDNS security services can filter unwanted content and unsafe phishing fraudulence websites.

9.4 Conclusion

The home networking router works as the front door to your digital data. An unlocked door makes everyone quite vulnerable to all levels of intruders. Putting on a reliable lock may not completely protect a family’s digital assets, but at least, it will lock the system to most hackers. All research shows that unfortunately, due to the complexity of protecting systems, most home networks are very vulnerable. Security can be achieved first by making the settings and configurations of the home networking device more user friendly and intuitive to user needs. Secondly, there needs to be an increase in user awareness on security, along with basic trainings to how to properly manage a home network, at the very least to help users protect their system by enabling basic security settings.

References


