Reece Zunino

CMIS 111 Final Project

Due: 10 October 2021

**Case Study 1**

So we just purchased a brand new PC. Now it is time to set it up with all the security and applications needed to ensure that our system is safe and secure from outside intruders or even from inside in case we have mischievous kids as I do. So let's start with the basics. First, we will want to make sure that when we set up our PC that we create a profile, this profile will act not only as our profile but also as our administration profile. We can, of course, make the main administration profile if we want to keep all profiles separate, but since this is a home computer, we won't dive too deeply into that. When creating our profile, we are going to want to make a strong password. When creating this password, we will, at minimum, be using two upper case letters, two lower case letters, and two symbols. The password will also need to be a minimum of 12 characters; we will use this password policy for all passwords on this computer and for all programs that don't already specify a password policy. Having a strong password is the first line of defense against any intruders not only into your PC but also on any website or application that requires a password.

When it comes to our computer security, the first thing we think about is the firewall. We aren't going to be worrying about this too much because we are going to be using Norton 360, which will control all settings of the firewall via the interface of the program, and from there, we can set whatever security settings we need to be based on what we are using the computer for. So as we said, we will be using Norton 360 as our antivirus and Nortons google chrome toolbar extension for internet security. After downloading Norton, we will set up our account on the website to access and activate the interface on our desktop. After downloading the program, it already has the basic settings setup that most average users need for everyday tasks, and we are going to leave it at that for the most part. There are many settings in Norton, and here are all the different settings you have access to in the program.

![Graphical user interface, application

Description automatically generated]()

When it comes to the different settings, there are also sub-settings within the settings, so it can get very personalized based on your experience and preference on how you want things to be set up. I find that what it is already set at is pretty adequate for my needs and don't usually change anything unless I am having issues with a specific program that can get blocked due to how the firewall is configured. Here is how the sub-settings of the firewall looks like to give you an example of what you could do with Norton:

![Graphical user interface, table

Description automatically generated]()

Norton is a very versatile program and even has a toolbar to help keep you safe even browsing the internet. As you can see, it can be very customizable to fit what we need to do for the security of our systems, and it's all you need and is all I have ever used for my home PC security. For this, we will download google chrome as our primary web browser along with the Norton Chrome toolbar extension. When it comes to the browser settings, we will keep it basic because the Norton toolbar will also help keep us safe by letting us know what sites are secure and which ones are not, along with scanning all downloads we get off the internet. We will keep the clear browser data default and allow all cookies but make sure to activate the "send a do not track request" setting for peace of mind. We will use the standard security setting because it will be sufficient for what we use our computer for. Under your computers internet options settings page in the control panel, we will also make sure that Medium-high is set as well; even though these settings mostly pertain to internet explorer, it is always good to have them set up in case you need to use it for older sites that may not work well with google chrome. We will not tough the advanced options because this should not be required for what we are using our computer for at home.

When it comes to my online banking at home, I will start with following the password policy that I have and that the bank suggests using to ensure that my account is initially secure. This will ensure that my password is unique and doesn't contain any personally identifying information that a hacker can find through any social media website or by looking up any of my profiles across the internet. When using my bank's website, I will also ensure that the URL website address is the same as the banks and that the proper SSL certificate is verified and authenticated. I will also check my bank's transactions regularly to ensure there are no out-of-the-ordinary purchases from places or sites I have not made purchases.

My operating systems patches and application updates should be automatic and checked for updates when it comes to my operating systems. These updates are usually security patches for bug fixes that the manufacturer does to ensure that any flaws in the operating system are found and fixed so that your system isn't vulnerable to attack. Hackers love vulnerabilities and weaknesses in software and exploit them if they can find them in your system and use it to their advantage to access anything on your system. This is why making sure that your system is always up to date with the latest security patches and virus definitions that Norton updates regularly when there is a new threat that emerges on the web and thy try and implements a definition that will look for this malicious code that can affect your system and cause havoc and even lock up your system via ransomware. Always follow the recommendations of the manufacture of your operating system and any application, even if it's not a security application. These recommendations are there for a reason to help protect your data from outside intrusions.

**Case Study 2**

My 13-year-old family member wishes to join in on the social media platforms that millions of others are on, along with regularly texting her friends and others. Even child predators look for these kids that they deem easy targets because they don't have any security settings that help prevent these incidents. However, there will be precautions and restrictions put in place for their safety and even made aware of the possible issues and outcomes that can happen if they are not followed for whatever reason because child kidnapping is a real threat and unfortunately occurs regularly around the world.

Let's start with Facebook since it is the most utilized platform and is most popular with everyone around the world these days. There are many predators, cyberbullies, and criminals on Facebook. They will all try to either access your information or try and hurt you by commenting hateful and demeaning things depending on how your account's security and privacy settings are set up. With all this in mind, the child needs to understand the restrictions that need to be in place to ensure their safety. ![Table

Description automatically generated]()

Since the family member is so young, they might want to forgo putting anything on their about me profile that would allow a stranger to find out what school they attend or where they live. The child should also set up their privacy settings on their account so that only friends can view their profile. This way, it is not available to the public to see. This is a way to safeguard the profile against anyone trying to view their information and pictures. Along with the basic settings, they should also make sure that geotagging is off if they post on their phone to their profile. I would also explain to the family member that when making a post, to ensure the post is not set to public but to only be viewd by friends.

Twitter is well known for cyberbullying, even more so than Facebook. It is just like all other social media websites but has its own spin on things regarding Twitter. Twitter allows users to send blurbs out and share other tweets from different users from either the public space or their follower's lists. The user must understand that they are responsible for the material that they tweet and that it can be used against them in many ways. One way the user can avoid this from happening to them is through the privacy settings in Twitter. The setting that users and opt into is "protect my tweets." This will allow the user's account only to be available to persons on their follower's list. They can also set their account to where everyone can tag them in pictures, or only those who follow them can tag them. They can slow not to tag them in tweets or photos, which is the safer option given the user's age. Text

Description automatically generated

Another highly recommended setting to make sure it is turned off is geotagging, like with Facebook. This will ensure that no one can see where that person is tweeting from and try and use that information to try and kidnap that kid, which often happens more than is in the news media.

A screenshot of a computer

Description automatically generated with medium confidence

When it comes to texting, it is not as dangerous as being on social media platforms because you are more isolated to your contacts list than when you are on a public domain like Facebook and Twitter. However, by no means does that mean you are not subjective to those who are trying to phish for your information that they might have gotten off that website you happened to put your phone number into to try and win that dream house or that chance to win that large sum of money. They still need to be careful even on their phones and always be vigilant when an unknown number calls them. We need to make sure they understand that if the number is not plugged into their phone, don't answer it. If the call is essential, they will leave a message or text them if possible. The family member also needs to be aware that they are responsible for the content they text. Like with social media, cyberbullying through textmessgaes is serious, and in some states, if not all, it is a severe crime. They can end up in Juvenal hall if they are arrested for it. Sexting is also a very serious crime these days, and if convicted, they may have to register as a sex offender even though they are a minor themselves. This has happened many times over the years recently and is not to be tolerated nor taken lightly by any means.

Now that we have covered most of the major platforms that the family member wishes to use, they need to realize that while this may be guidance, they are responsible for what they do in cyberspace and on their phone. They must also make sure that they keep an eye out for suspicious messages or texts and let an adult know immediately if this happens to them so that the issue can be reported and resolved promptly. Also, when it comes to reporting cyberbullying, they need to let an adult know what is going on so that they know there is help and that they are not alone in this and that it can be reported so that it is stopped immediately. One primary website is this <https://cyberbullying.org/report>, which is always the best place to start to notify cyberbullying.

References

Facebook. (n.d.). Facebook. Facebook - Log In or Sign Up. <https://www.facebook.com/help/238318146535333/?helpref=popular_topics>

Report Cyberbullying. (2021, October 5). Report cyberbullying. Cyberbullying Research Center. <https://cyberbullying.org/report>

Twitter. (2021, March 30). Protecting your personal information | Twitter help. Help Center. <https://help.twitter.com/en/safety-and-security/twitter-privacy-settings>

Twitter. (2021, March 30). Who can see your tweets – Twitter privacy and protection settings. Help Center. <https://help.twitter.com/en/safety-and-security/public-and-protected-tweets>