1. What main points did we talk about?
   Internet security

2. What do we want to be the subject of our blog post?
   - Tips for parents to keep themselves and their kids safe?
   - What is a VPN and why it would be important to have?
   - Being aware of user agreement?
   - Good password management?
   - Not opening suspicious emails?
   - Know who you are communicating with when you call a help desk/customer service?
   - Examples of fraudulent websites
   - Setting up antivirus

3. Who is our audience?
   Parents with basic computer skills

   Outline:

   - Why should you be concerned about internet security? What do you have to lose? What can you do to protect yourself?....One way is VPN. (Wade)
   - What is a VPN? (Zuri)
   - Pros (Anvy)
   - Cons (Angel)
   - Tips (Brian)
     1. Ad Blocker (Brian)
     2. Password Management (Anvy)
     3. Be vigilant of who you are communicating with--help desk/customer service (Brian)
     4. Setting up antivirus (Brian)
     5. Example of fraudulent websites with screenshots/photos (Angel)
     6. User agreement (Zuri)
- Conclusion (Wade)

Protecting yourself with a VPN

The internet has taken over the world. As of 2018, more than four billion people have access to the internet and use it in one way or another. It is an amazing resource and allows people to connect more than ever before. Parents, kids, professionals, nearly everyone has a reason to use the internet. Unfortunately, with all of the positivity and connectedness that the internet has provided for us, it also carries with it some heavy downsides. The internet is a tool, and like every tool, it needs to be treated with caution and must be used with care and the proper education. Do you ever search for a product on google and then find that product being shown to you across all of your devices? Or maybe you've noticed that the majority of ads that you see are somehow personally targeted to you. This is an example of data tracking. Did you know that the majority of the information that you put out there on the internet is not only stored and sold to companies for profit, but can also be tracked directly back to you. For many users on the net security and privacy has never been of importance, not necessarily because they don't care but simply because this important and vital information has not been provided to them. There is so much that you can learn to do to protect yourself, but one of the easiest and simplest ways to keep yourself secured is through a VPN.

What is a VPN?

VPN stands for Virtual Private Network, meaning that your connection to another network over the internet is secure. A VPN is a great way to protect you and your kids from becoming a target by sites trying to sell your data. This data can not only be used to send you annoying pop up ads, but companies that have your data also have access to your: location, browsing history, ip address, even your card information depending on the site.

Choosing your VPN

Choosing a VPN isn't as simple as downloading the first one you see in your google search. There are many false VPN services that are not trustworthy, and could also be selling your data. It all comes down to research on which VPN is best for you.

Do Not download a free VPN. Yes, free apps are always awesome, but when it comes to protecting your information, in a free VPN there is no value in protecting your data, and it is more likely that your data will be sold through that VPN provider. In addition to that, as it is with many free applications, the main source of revenue is through ads. This means even if your data isn't being sold, adverts get trafficking priority, which means a slower page loading time and a less fluid online experience.

Although a VPN can be a great way to protect your information, like every application, there are pros and cons:

Pros of VPN

1. You can protect your family's online privacy and safety by shielding both your physical location and IP address. When you connect to a VPN, the VPN's addresses will be used instead of your own.
2. You can protect yourself from hackers because a VPN will encrypt your data (what you have been browsing on the web, credit card information that you used, passwords you have entered, etc.) which prevents the hackers from reading it.
3. You can protect yourself from snoopers when you connect to public WiFi in an area like at the coffee shop, restaurant, or mall.
4. You can help prevent internet service providers (Comcast, Verizon, RCN, etc) from collecting data, tracking your patterns, and selling this information for profit.

Cons of VPNs

1. Slower web surfing speeds. You're adding an extra layer when surfing the web and gaming. Tightly encrypting your information takes time.

2. Not 100% Anonymity. Some VPNs log user data. You're deciding to trust your VPN provider with your information. It's important to do your research before deciding on a provider. Refer to the section above on "Choosing your VPN".

3. Added cost. Quality VPNs will cost a monthly fee. PLEASE be aware of free VPNs. They will come at the expense of your privacy.

4. VPN restricted websites. VPNs cannot access every website. Examples being Netflix, Amazon and Hulu.

Tips for Internet safety

1. Blocking ads: In every website you visit there are ads just waiting to be clicked on and direct you to some random unsafe sites that will lead you to accidentally download malware. Sometimes parents don't know better because they see a better deal on items you're looking for or might be interested in from the ad. A free and simple way to prevent most ads and popups that occur when those ads are clicked is by using ad blocker. An ad blocker is designed to block out these unwanted ads when visiting your favorite

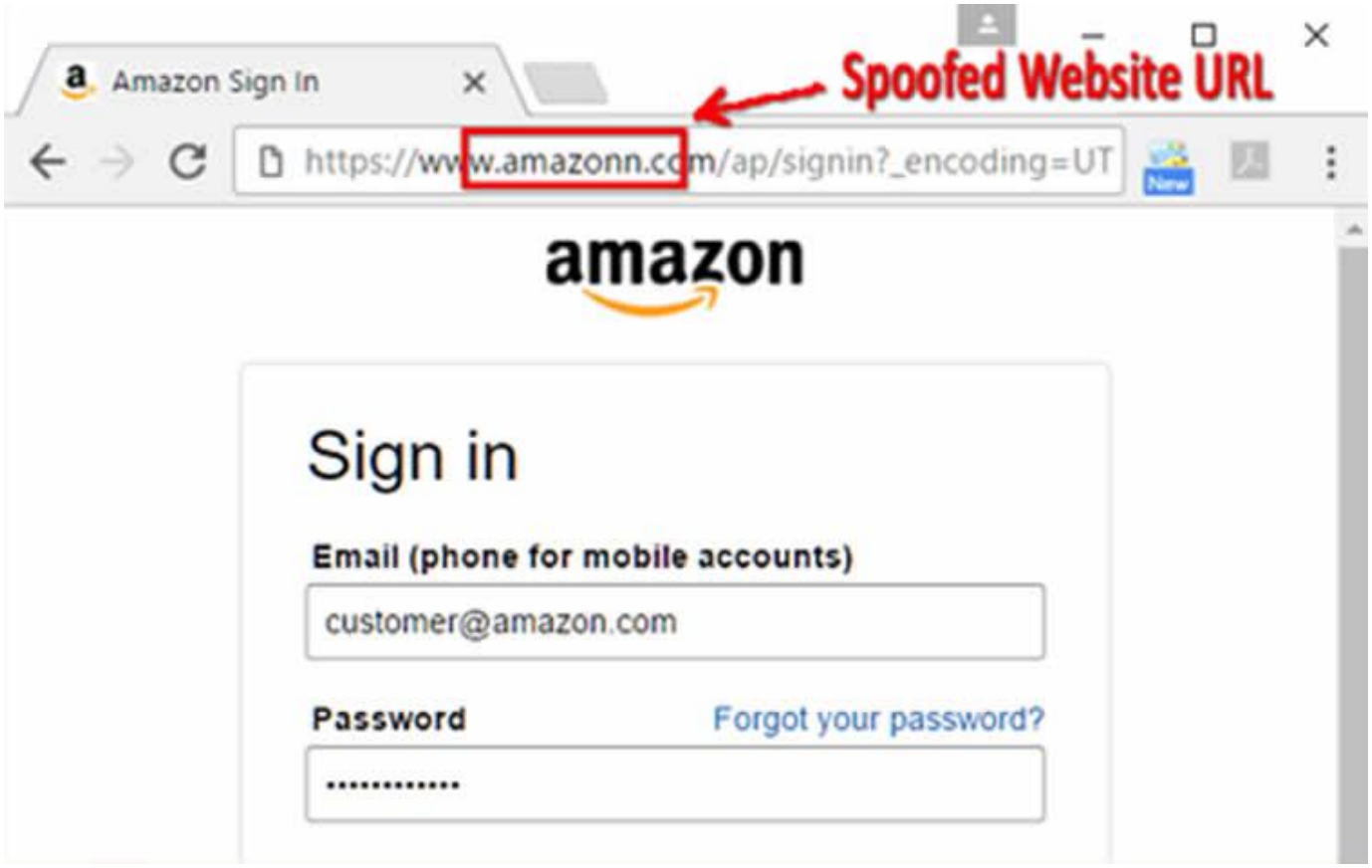
websites. Without these ads you are much more safe to surf the web by eliminating the chance of misclicking on these ads to bring you to an unsafe site.

2. Password strength: Set a strong password to protect yourself from hackers who may try to steal money or your identity. You can increase your security by creating a password that is difficult to guess. Make your password long using both upper and lowercase letters as well as numbers and special characters. Do not create a password that is easily guessable or that contains personal information. Change your passwords regularly.

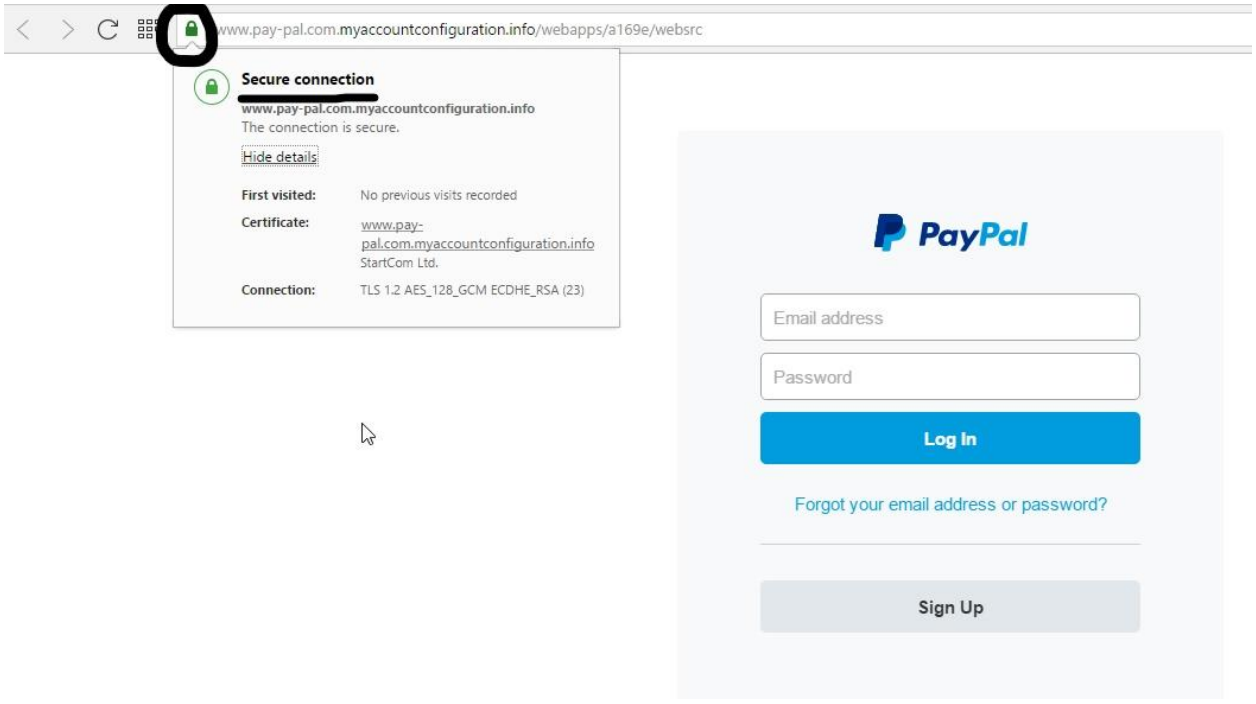
3. Suspicious e-mails: You can get a malware from anywhere online you visit, even your own email. You may see some emails that sound too good to be true and in most cases it is. It is very important to be vigilant on who you are emailing and potential links you may click on. You can be vigilant by reassuring the email is correct because the first thing you pay attention to when you get an email is most likely the main name under that email and it could fall behind a malicious email. This does not only include emails also any other information an email gives such as a phone number that might make you think the email is more legitimate but in reality it is a false number most likely wanting to scam you. But if you do manage to accidently click on a link to download a file that contains malware thats where anti-virus comes into play. Most anti-virus software is able to detect when you are downloading malware and prevents it from further damaging your machine and exposing your personal information to malicious users. It is important to know that an antivirus is not the sole answer for internet security and a big part of internet security is just being informed and staying up to date with internet security because they're are constantly new ways malicious users are trying to get your information.

4. User agreements: Read the fine print: It is very easy to see the words "Terms of Service" and simply scroll down to the bottom of the page and absent mindedly check the "I agree to the Terms of Service" box. We've all done it. Though it may seem like a simple way to skip all the reading and quickly access your app or website, it is the easiest way to breich your internet security. Simply take the time to read or even skim over the terms of service, as many of the terms that you agree to could be taking and selling your data.

5. Below is an example of a fraudulent website:



7. Below is an example of a secure website:



Conclusion:

Let's do a quick recap of what we can do to keep ourselves safe on the internet. We have VPN to make sure no one sees our personal tracking data and location. An adblocker so we can get rid of those pesky annoying advertisements. A password manager to keep our passwords safe, and in control. An antivirus to make sure nothing we download can steal our data. Lastly we know how to identify fraudulent websites and how to be sure that we know what we are agreeing to by understanding user agreements. Now with all of that precious, life changing information at your disposal you are finally ready to browse the internet safely. Always keep an eye out and stay alert about what you are doing, the internet is changing everyday and you can never be too safe.

Sources:

https://www.vpnmentor.com/blog/how-to-really-hide-your-ip-address-with-a-vpn/

https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/

https://www.vpnmentor.com/blog/how-to-really-hide-your-ip-address-with-a-vpn/

https://www.thebalance.com/how-vpn-protects-your-computer-and-privacy-4148267

https://internethealthreport.org/2018/the-good-the-bad-and-the-ugly-sides-of-data-tracking/

https://www.broadbandsearch.net/blog/most-common-uses-internet-daily-life

https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/

https://beebom.com/vpn-pros-cons/

https://www.vpncrew.com/5-disadvantages-of-vpn-that-you-should-know-before-using-it/

https://nordvpn.com/blog/pros-and-cons-of-vpn/

https://www.wordstream.com/blog/ws/2015/10/02/ad-blockers

https://www.makeuseof.com/tag/biggest-risks-using-free-vpns/

https://us.norton.com/internetsecurity-how-to-how-to-secure-your-passwords.html

https://www.nortonsecurityonline.com/security-center/why-antivirus-software.html#:~:text=Antivirus%20%E2%80%93%20Starting%20with%20the%20obvious,mean%20to%20damage%20a%20computer.&text=Antivirus%20software%20can%20prevent%20this%20sort%20of%20attack%20%2D%20stop%20computer%20worms.