

Keeping Safe on the Internet

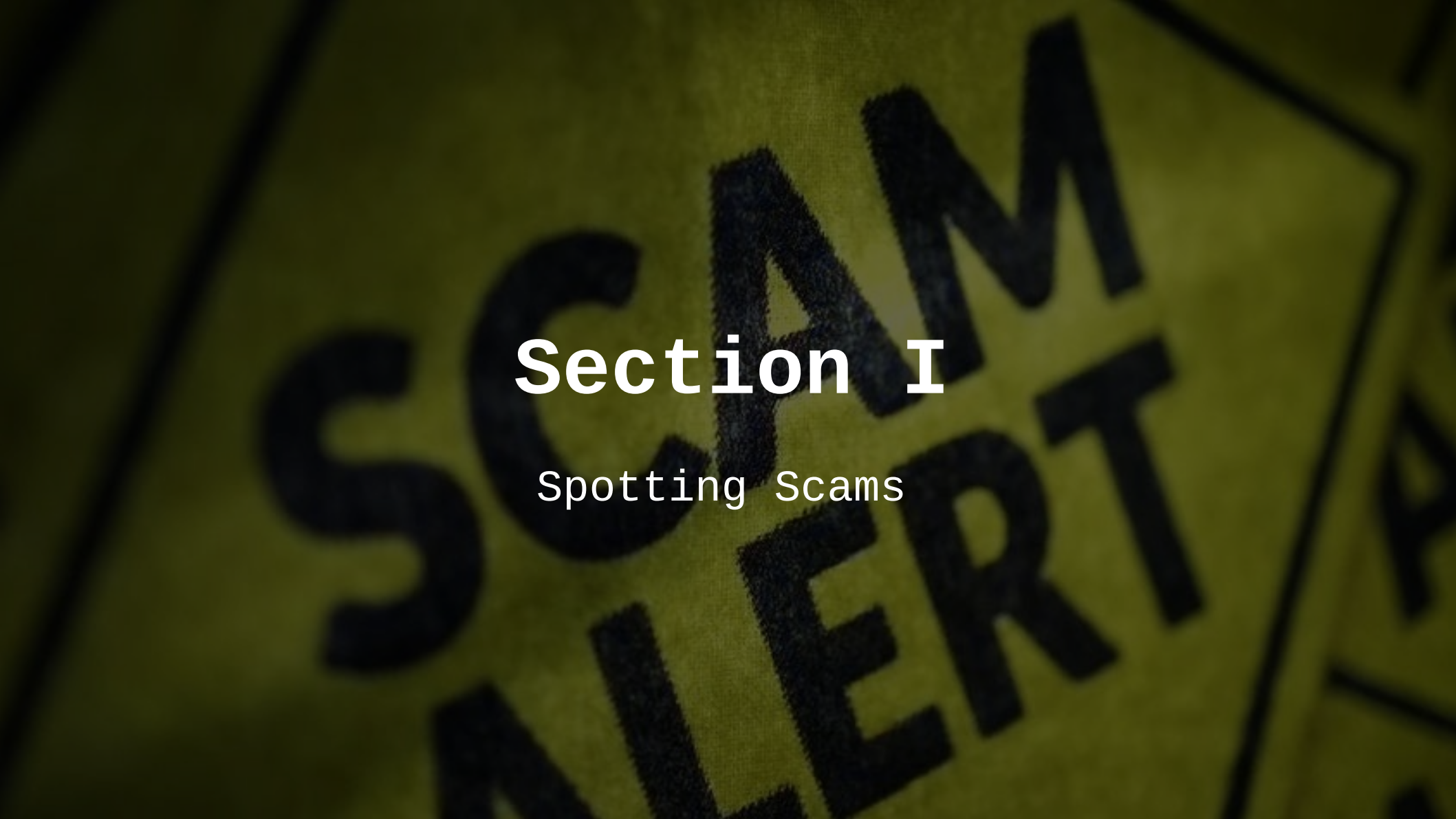
Presentation by: Blake Mackay

Introduction



The Internet has never truly been a safe place, and it won't get any safer for a while.

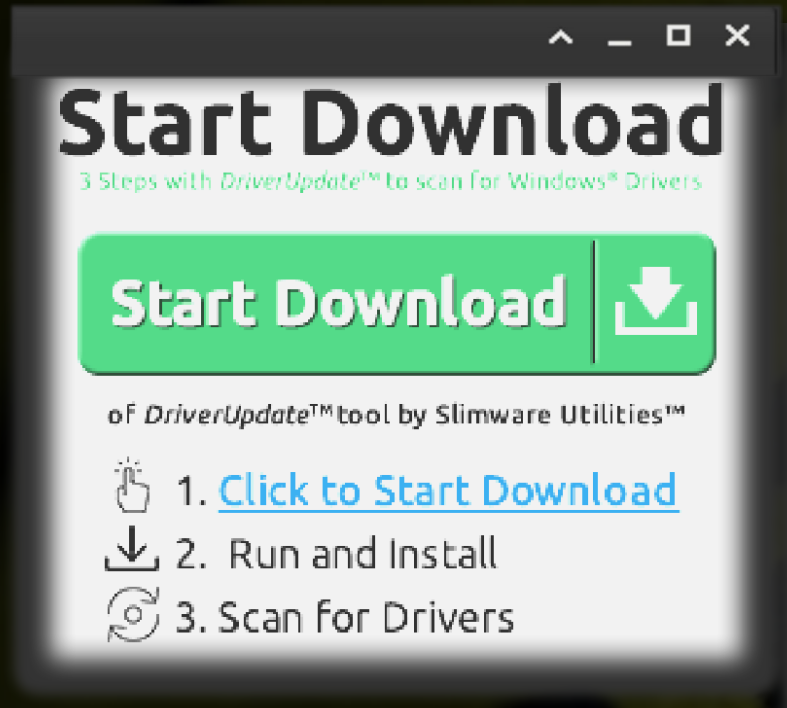
No matter the circumstance, an indecent human being will find a way around the rules, and because there are not many law officers or other authorities to stop crime on the Internet, here are some ways to protect yourself and others.



Section I

Spotting Scams

Download Scams



There are many reliable, legit, and useful free software available to be downloaded. Majority of people use Windows/MacOS/ChromeOS, which require the downloading of executable files or similar to install most of the programs.

But where do you download these things? ALWAYS make sure you download from the official website, cloud, or repository. Other non-official sites can be infested with malware.

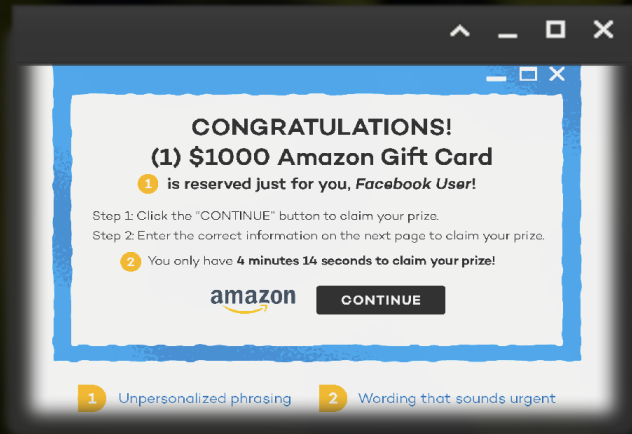
Be sure to not click fake download links as well. On trusted sites, they almost always show up as advertisements. You can tell if they have a certain URL or certain UI that only ads have. Some official download links may also lead to suspicious sites through DNS sabotage, so be careful where you download.

Phishing



The most important thing you need to know about browsing the web, is the fact that you should NEVER share information with anyone.

Phishing commonly happens through email and can send you to a fake website to sign in, and keylog your password. Don't trust anyone on the Internet, and at sometimes, not even yourself. Never take any "free rewards" or anything similar.



Antivirus



To further prevent viruses, consider an antivirus. For Windows, I typically use WebRoot: Secure Anywhere. It's not free, but paid antiviruses are more trustworthy.

Using Windows's built-in Antivirus isn't as fast-acting. One last thing to keep in mind. Antiviruses are known to hog up RAM.

Summary of Section I

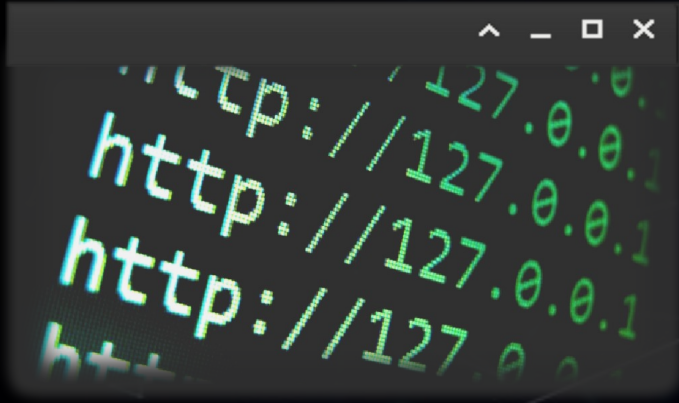
- Only download .exe (or similar) files from the official source of the software. Also beware of redirects.
- Never click a fake download button. They are usually ads or redirects to sites if they do appear.
- Never share personal information on the Internet with others.
- Don't fall for "You won a free ____" or other scams.
- Consider purchasing third-party antivirus software.

Section II

Your IP Address and Accounts

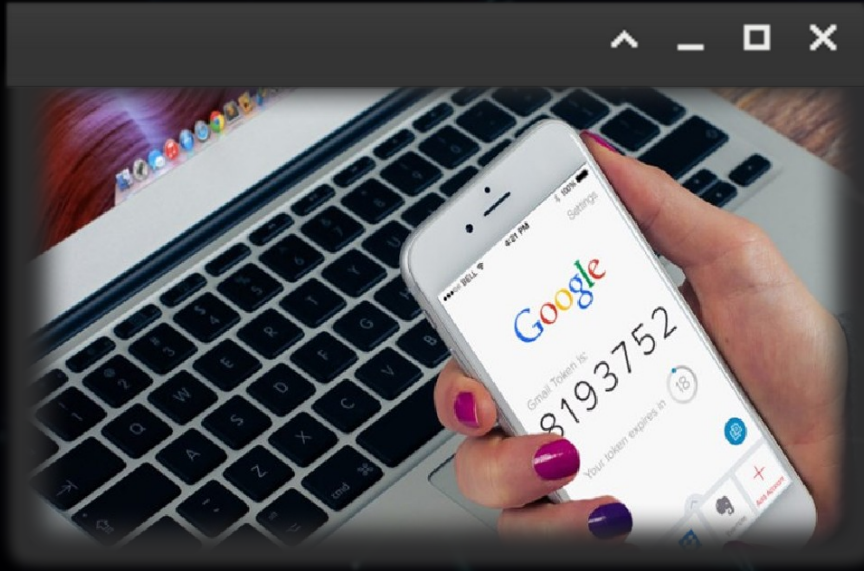


Protecting Your IP



Much like your name and home address, your Private IP is personal information. If you click on certain links or go on certain pages, someone will obtain your IP, and can be used to track your location from your state, or even close to your exact address. To prevent your IP from being violated, you can get a VPN (Virtual Private Network), which hides your Private IP when browsing the web. Some are free, and some are paid for.

Protecting Your Accounts



Obviously, your password, token, and other forms of authentication are important to keep private and away from other users to ensure no one can hack into your account. If you have a cell phone, you're in luck. Many services offer Multi-Factor Authentication, which involve you using your phone as a new step to signing in, thus protecting your account from hackers. Some companies will directly text you, or use an app like Google Authenticator or Authy. But keep in mind, beware if you install malware on your phone (chances are it allows for MFA access to unwanted people) and never share your backup/MFA codes.

Summary of Section II

- Your Private IP Address can track you as far as your town, not exact location.
 - To prevent unwanted access to your IP, use a VPN.
- Don't click random links or go on random websites, without a VPN at least.
- Multi-Factor Authentication can help your account become more secure. A phone is necessary.
 - Hacking a MFA account isn't impossible, but can be avoided easily by avoiding download scams on your phone or your computer.
 - Never give anyone your IP or MFA Codes.



Section III

Avoiding Toxicity and Disturbing Media

Avoiding the Bad



If you've been on the Internet for long enough, you've probably ended up seeing something disturbing. It's the scary truth of the world that these bad things are everywhere, and the Internet is just the place to spread the danger. Unfortunately, none of this stuff is 100% fully acted upon by law, so we have to be "street smart".

A blocking extension for Chrome and Firefox called uBlacklist has the ability to not only make websites disappear, but images from said websites, too. It does a much better job than Google SafeSearch does blocking disturbing sites that aren't even labeled as pornographic, such as FurAffinity, Twitter, and sometimes even DeviantArt. Some sites although not 100% pornographic can sometimes have hosted pornographic or fetish art pop up without Google ever batting an eye. So block those websites, and if you ever come across something, you can also block that on the fly!

Hostility

Some people on the Internet can be very untrustworthy, so make sure you don't end up on the wrong side of the tracks. Some users can expose you, lure you, harass you, and disturb you. If you want to be super-safe, don't even speak to people you don't know, but that's just being paranoid. If you want to be even MORE paranoid, you can just avoid social media all together. The most beneficial way would be avoiding these people and being careful.



Summary of Section III

- Use an extension like uBlacklist to block bad websites, and to avoid disturbing imagery on Image Search sites.
- Stay away from websites that might get you in a bad spot.
 - Be very careful who you interact with.
 - To be super-safe, only talk with those you know.
 - To be ultra-safe, don't even go on social media.
- Best way is to just be careful, because the other two can be a very paranoid choice of action.

Conclusion



I hope this has gave you the information you need to safely surf the web. It's not an easy world out there, so might as well browse prepared! The knowledge you have just received is all based off of experiences, and have come from no sources. Please do not take any of this as bias.