Did you know that in 2012, seventy-five percent of Americans’ computers were hacked, one trillion dollars worth of intellectual property was stolen through cyber crime, and seven Facebook accounts were hacked every second? In fact, the United States government spends over four billion dollars on cyber security efforts to try and one-up China in the cyber war, where thirty percent of cyber attacks originate.

Hacking has become more common because it has become a more efficient method to steal information. Of course, common targets are successful companies and individuals are always at risk because they hold valuable data. However, other targets may surprise you. Just as successful are many renowned universities receiving hundreds of cyber attacks per day because of their list of famous faculty members, student databases that include children of prominent adults, and access to expensive online catalogs. Furthermore, your computer is not the only machine susceptible to hacking. Anything connected to a network or the Internet, like your car’s computer system or even a pacemaker, is vulnerable.

How can you protect yourself? To keep your computer safer, make sure to continually install updates and security tools and patches. Also, this may sound redundant, but choosing a smart password can ensure that your sensitive information is secure. In fact, a hacker’s computer can guess a password containing six lowercase letters in ten minutes. However, it would take four hundred sixty-three years for the hacker to guess a password of eight lowercase and uppercase letters, numbers, and symbols. In addition, while surfing the web, it is common to be prompted for personal information, such as a username and password, birthdate, credit card number, etc. Make sure to verify that the site’s URL starts with https, not just http. The extra “s” stands for secure and means you can trust this site with personal information because it will
encrypt your input. But, there is a false sense of security because even if the URL starts with https, there are extensive documents on the website’s privacy policy, and your sensitive information is being encrypted, a hacker can still get into your web browser and scroll through your history to predict your interests before sending you a spam e-mail with links to malware. Last, but not least, do not click on any links or popups that seem suspicious. As hackers become more sophisticated and deceptive everyday, they are able to create convincing software that look almost identical to the applications you use on your computer. With just one click on one of these popups, you could download various computer viruses and malicious software. Now, more than ever, we rely on and have confidence in technology to communicate, store confidential information, and many other useful tools. These electronic benefits come with responsibilities for the users, namely cyber security.