Cyber Security: How to Protect Yourself Online

March 2018

Awareness

Over the last twenty years or so, the Internet has become an absolute staple of our everyday lives. It is incredibly valuable in terms of communication, education, etc. but it can also be dangerous for those who are not properly trained.

Unfortunately, with over an estimated 3 billion people having access to the Internet, there are bound to be users looking to take advantage of others. Luckily, with some minor adjustments and preparation, you can be secure and safe to explore the Internet without the fear of being susceptible to an attack.

Of course, no one is truly "unhackable," as anyone can clearly find news articles about various large corporations being attacked, but as technology advances, society as a whole needs to adapt in order for the Internet to remain safe for the common user.

To increase the average user's security, I believe some of the very basic topics should be further emphasized because even though someone who has a strong technological background considers the basics obvious, many others may find the same information enlightening. These topics include the use of strong passwords, keeping your system and virus protection up-to-date, being more aware of suspicious emails, and increased knowledge of what is and isn't safe to post on social media.

The keys to Internet Safety:

- Strong, unique passwords
- Up-to-date systems and virus protection
- Be careful of untrustworthy emails and websites
- Be more selective with the information that you share online.

Have any questions about the article or something that was not addressed?

Feel free to contact me via email at rj@lansingpl.org

RJ Reynolds, IT Assistant at the Lansing Public Library and Information Technology student at Governors State University.

Passwords

As someone who has to remember upwards of 30 passwords for everyday use, I understand the desire for something simple and memorable to be used, but the importance of a strong, unique password cannot be stressed enough.

When creating a password, never use anything that can be easily guessed (date of birth, family or pet names, etc.). Also, make sure to add capital letters, and special characters (!, @, $, etc.). Using unique passwords for each individual account is recommended as well.

Nothing is impossible to crack with the use of hacking tools, but the trick is to make it difficult for hackers to get into your accounts and ultimately not worth their time to continue targeting you.

Keep Your Software Up-To-Date

Updates can occasionally be long and somewhat tedious, but their importance is something that cannot be understated. For PC users, Windows frequently has updates that increase system security as well as address issues from previous versions of the operating system. The same thing can be said for users of Apple and Android products: update your operating system, it is the most basic line of defense but is also a powerful one.

On top of OS updates, it is recommended to have some form of virus protection on your device. Virus protections are not perfect, but they add yet another layer of defense and catch various forms of malware (viruses, spyware, adware, and so on). Ensure that your virus protection is always up-to-date and run scans on a regular basis to keep your system constantly free of these sorts of threats.

Many of these tools are available for subscription or even for free. Personally, I recommend using a

combination of a virus protection with live system monitoring (such as Avast, Kaspersky, or Norton) and a powerful free software called Malwarebytes to run scans for malicious software.

Beware of Phishing Emails

Phishing is one of the oldest, but most common and effective ways cyber criminals get information from the average internet user. Phishing emails are generally emails that are disguised to look like they are coming from a trustworthy source such as Microsoft or Amazon. These emails may look professional, but some red flags should be raised immediately when opening them:

- Check the email address, if it is something along the lines of "Amazon.Support@gmail.com" then it IS NOT coming from the company. They have distinct email addresses and will NEVER contact you unless you request assistance.
- The email will ask for personal information (usernames, passwords, credit card numbers, etc.).
- Phishing emails will generally have some sort of way of "forcing" you to give the information; it is common for them to say that your account will be closed or some similar consequence.
- Beware of odd links and attachments as these are generally infected.

Know the signs of common phishing attempts and identifying them will become simple and easy to avoid.

Social Media: What is Safe to Share?

Many users (especially those using Facebook) are prone to sharing a bit too much information. Facebook users often fill their bio with all kinds of information so that it is easier for people that may (or may not) know them to connect with them. This includes date of birth, email address, phone number, etc. All of this information is widely available to the public, even if your profile is private. All it takes is for a contact of yours to have their account compromised for someone malicious to find your information.

Much of the information that is frequently shared is directly linked to your identity. For example, if you do mobile or online banking, your bank account more than likely uses your phone number or email address as a form of identification to either log in or reset your password in the event that you forgot it or have been locked out of your account.

Only share what you are comfortable with a stranger knowing and social media will remain a useful resource.