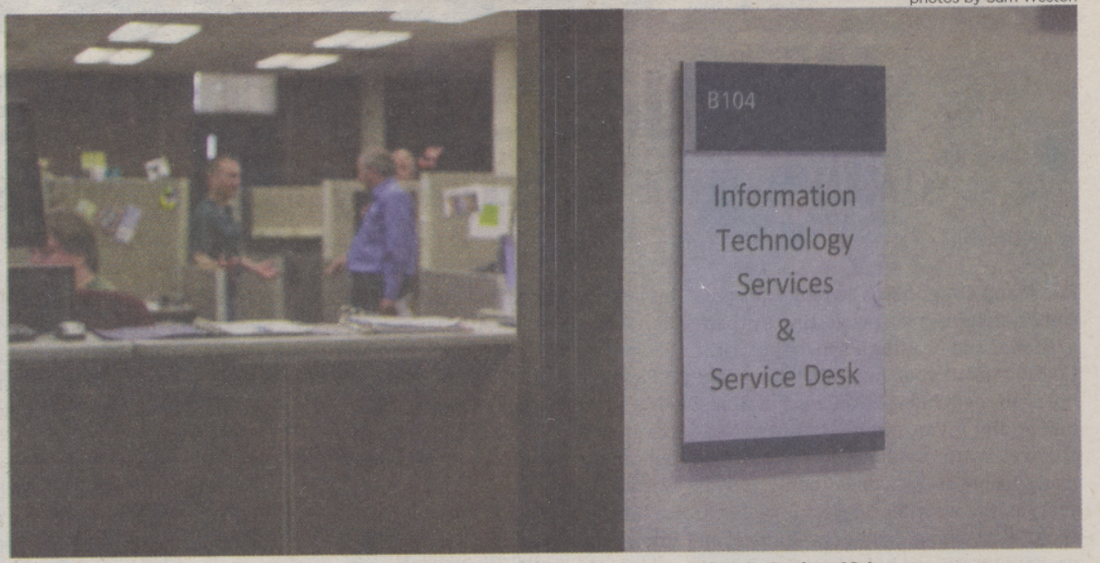
Do the cyber crime, pay the cyber time

photos by Sam Weston

John Hughes works in the ITS department.



The entrance to the Information Technology Services and Service Desk office in Barlow 104.

BY IAN VAN ORDEN

Over the last 50 years, technology has made an unprecedented jump forward. Computer technology alone has changed society itself, especially with the advent of social media. With only a few words, we now have access to near limitless information, and the rate at which new technology is appearing doesn't seem to be slowing. This new technology has improved our lives in so many ways, but it hasn't come without a price.

One of the most prevalent and difficult things to defend against in today's world is cyber-crime. Identity theft is one of the fastest growing crimes due to how much easier it is to procure someone's personal information in a time when everyone posts every miniscule part of their lives on Facebook and Twitter.

An example of a cyber-crime that was recently widely reported by major news networks was the WannaCry ransomware attack. Beginning on Friday, May 12, the worm began its attack, infecting more than 300,000 computers in more than 150 countries around the world. Using an exploit in Windows' Server Message Block protocol, which provides shared access to files, printers, serial ports and other communications on a network, the attack effectively locked down a computer, forcing the user to pay up to $600 in bitcoin or permanently lose access to their files.

These attacks are becoming increasingly prevalent as people rely more heavily on technology and they aren't likely to stop. How do you protect yourself from falling victim to one of these attacks?

One of the most prevalent and difficult things to defend against in today's world is cyber-crime

Though the complete answer is lengthy and complicated, there are a few basic rules you can follow that will prevent most attacks from succeeding.

Always run up-to-date antivirus software on your computer. There are many different options to choose from, and the best option will vary from person to person. If you are running Windows 8 or 10, Windows Defender is included with the operating system and is a good place to start. For something more comprehensive, Avast and AVG are good, free alternatives.

Do not use simple, easy to guess passwords. This is probably the most common reason people fall victim to cyber-crimes. "Password" is not a good password. When crafting a new password, try and use a combination of special characters (!@#$, etc.), uppercase letters and numbers. Do not use popular phrases. It's also not a good idea to use family members' birthdays or anniversaries.

Keep your computer and software updated. The WannaCry ransomware attack took advantage of an old Windows exploit that had been patched out months before. It was only successful because people failed to update to the most recent version of their operating system. Waiting to update makes sense for businesses and schools as they generally require time to update their networks to be compatible with recent updates, but there isn't a real reason for the average consumer to avoid updating their computer. This goes for both your operating system and any software you run daily.

Always know what you are downloading. One of the most common ways that an everyday person's computer becomes infected with a virus is from downloading a suspicious file. Most modern web browsers have methods to protect against the most common malicious files, such as Google's Safe Browsing, but the methods are not foolproof.

Finally, control the amount of personal information that is available online. Social media makes it easy for someone with criminal intent to track down huge amounts of your private information if you are not careful. All major social media sites have methods of limiting what the average user can see. It's a fantastic idea to take advantage of those features. Also, avoid posting something on social media that could get you in trouble in the future. It has become a common practice for companies to look at potential hires' social media accounts after all.

There are other methods, but these are a good place to start. It's also a good idea to take the time to do some research on your own to figure out where your vulnerabilities lie. It may not be the most exciting topic, but its importance cannot be understated.