User accounts and passwords can be great security risks. The way that we handle them has a direct effect on the security of your personal data and all data that you have access to. You should look at your username and password as your first line of defense. The use of strong passwords helps defend against the possibility of a hacked account. In terms of handling your username and accounts, always be certain to log off of all sessions and devices when you have completed your task. Never leave yourself logged in. Log out of public computers, portals and web sessions. When considering what is and is not a strong password, please use the guidelines noted here.

- Use a password with a mix of at least eight mixed-case alphabetic characters, numerals and special characters
- Use a password that is difficult to guess but easy for you to remember, so you do not have to write it down.
- Don’t use your own name as a login
- Don’t use the name of your spouse or child
- Don’t use other information that might be easily obtained about you.
- Don’t use a word that can be found in an English or foreign language dictionary.
- Avoid using the “remember your password” feature associated with some websites, and disable this feature in your browser software.
In our world today, we rely so much on technology. From social media to keeping up with today’s news, or even access our personal resources such as banking, it can all be done anywhere and at any time. Unfortunately this need for convenience and instant accessibility puts our data at risk. Risks such as identity theft and credit card fraud are real and happening more and more each day. The best way to protect us from these types of threats is through education and awareness.

Here are a few top cyber security threats and tips on how to protect against them.

**SPAM**

Spam is the act of flooding the Internet with many copies of the same message in an attempt to force the message on people who would not otherwise choose to receive it. Some of these emails may contain links or attachments prompting you to download a file. While the most widely recognized form of spam is email spam, the term is applied to other social media such as instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam and file sharing spam.

**Malware**

Malware, be it spyware, key loggers, true viruses, worms or any type of malicious code is specifically designed to gain access or damage a computer without the knowledge of the owner. Malware is a piece of software (computer program) written by someone with mischievous or, more usually, malicious and/or criminal intent. Its function is to spread itself by some means, and to do some sort of damage or theft. This may vary from the trivial (e.g. displaying a silly message on start-up) to logging the usernames and passwords you use for other sites such as online banking.

**Phishing**

Phishing are typically email messages appearing to come from legitimate enterprise. Phishing email will typically direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and will capture and steal any information.

How do I phry the phish?

Be cautious when opening email and attachments

**How do I protect my system?**

Beware of suspicious links and websites

Be careful when opening email attachments

Ensure that you have up-to-date protection software

**How to reduce unwanted email?**

Keep your email address private

Review privacy policies before you submit your personal information to any website

Delete email from unknown senders

ASU Center for Applied Cyber Education web page can be downloaded here:

helpdesk@armstrong.edu | 912.344.2518

Armstrong Center, Suite 16