**YES/ NO Questions**

* Do you use the same passwords for multiple unrelated accounts?
* Do you let your operating system or browser store your passwords?
* Do you manually store your passwords on your computer? (i.e., notepad, sticky note)
* Do you physically write down your passwords?
* Have you ever received a pop-up, that said something along the lines of “your computer has a virus, please call Microsoft support…”?
  + If yes, did you call?
* Have you ever received an email from a company in which you have an interest in stating that you have won something?
  + If yes, did you click on the link?
* When you walk away from your computer in a public place for any amount of time do you leave it unlocked?
* You receive a pop-up stating that your software (such as java) is out of date, it seems trustworthy and looks legit, do you click “update”?
* Have you ever installed anything from a third party, and upon completion you found that you did not receive what was expected.
* Have you ever installed malicious software on your computer by accident or mistake?

**True/False**

* Anti-virus softwares are an effective way to prevent malicious activity.
* Anything available and/or stored on the internet is attainable by anyone.
* It is possible to change the sender (from) email address to anything.
* Some viruses cannot be detected.
* Your computer can be used by a hacker to hack another target, without you even knowing.
* USB drives that do not belong to you or someone you know should not be plugged into a computer.
* A locked computer is safe and can be breached without your password.
* Free Wi-Fi is secure, paid or Wi-Fi you have to sign in for is very secure.
* Hacking will never go away.
* A new strong defense is developed for a particular attack, that attack is now rendered useless and won’t be able to work with the new defense in place.