Digital Literacy Classes Start with Cybersecurity

By Joan Holliday

As the Southern Chester County Digital Literacy Coalition begins the pilot project with Train the Trainer classes, we are learning the importance of cybersecurity. The lessons learned are worth sharing.

Have you ever been a victim of hacking?
Hacking is the unauthorized access to or control over computer network security systems for some illicit purpose.

Have you ever been a victim of phishing?
Phishing is a type of social engineering where an attacker sends a fraudulent ("spoofed") message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.

Ways to prevent hacking and phishing are being discussed in the digital literacy classes that have started In October with employees from MCHC/The Family Center; Mighty Writers and the Kennett Area Senior Center. RSVP Volunteers non-profit is providing the training.

We are told that the most important education that we will receive is learning how to safely use our digital devices. Losing one's personal identity and privacy can literally destroy a person's secure life.

Downloading antivirus software is the first step. Fortunately, there are free programs, which will scan, detect and remove a computer virus before it causes damage. All digital literacy students will be taught how to do this.

As one starts creating passwords, there are several things to consider. Hackers continue to get smarter so more complicated passwords are required. Using names of family members or memorable dates can always be looked up by a hacker, so words need to be spelled differently with a variety of symbols and random numbers with up to 8-12 characters.

Changing one's password frequently is recommended. It also is important to have different passwords for every device.

Always be sure you know the sender of an email. If you are being asked to send a password or personal information, you are a victim of phishing. Banks will never ask for this information. In fact, banks will use 2-Factor Authentication, by sending you a new code on a phone to use before opening an account.

Email messages in which you do not know the person asking for any kind of personal information needs to be suspect. And, if you don't know the company of an advertisement, just delete and don't "unsubscribe" as this is another entry for a hacker. Just delete the message!

Emails that have unusual email addresses; generic salutations, words that have poor grammar or are stating an urgent deadline that a response is needed are all signs of a hacker or phisher.

When searching information on a web site, it is important to stay with the mainstream reputable sites. Downloading information from an untrustworthy web site is another way a digital device can become infected.

Receiving a pop-up message that says your antivirus software is expiring and you need to click on a link to find out more, is another example of how your computer can be opened up to a hacker. Directly contacting the provider of your security system to learn if this is true is the right approach.

The instructor tells us that all of this information is "common sense" but in a moment of haste and concern, one can put one's cybersecurity at risk, as well as lose all the information stored on one's computer, including one's identity and privacy.

The Story of Kennett by Joan Holiday and Bob George may be purchased on Amazon and at the Mushroom Cap or Resale Book Shoppe in Kennett. You may contact Joan Holliday at dochollisv@aol.com