Dangers of the Digital Age

The Digital age is a place of great wonder. We have a near infinite number of

resources at our hands. We can see what's going on around the world in real time,

communicate with anyone from anywhere, we can even order food from the comfort

of our armchair with the click of a mouse or the flourish of a keystroke. The digital

age has brought much good to the world in every sector of society and we are able

to do things today that would have been deemed impossible even just fifty years

ago. It is indeed a marvelous age we live in, but as in every age, progress has its

dark side. As long as there are people working to use technology to better mankind

there will also be people who seek to better themselves by taking advantage of

others.

How is this done in the digital age? It is done through malware. Malware is a

broad term for any type of computer program, method, code or any device used by

cyber criminals in order to bring harm to your computer in order to bring profit to

themselves. One type of malware is the virus. A digital virus has much of the same

qualities as a physical virus. Once introduced into a system a virus can replicate

itself and carry out preset commands that will slow down a computer's processing

capabilities and harm the system as a whole. Viruses spread, most commonly,

through emails. They often appear as a graphic or link or attachment. They appear

harmless at first, but once they are activated by the click of the mouse, they will

instantly download ("What Is a Computer Virus?" 2015). This often happens

without the user even realizing it because it often takes only a fraction of a second (Four Ways Hackers Can Install Malware on Your Mobile Device, 2015). Once installed the virus can erase information, record keystrokes and send them back to the cyber criminal or even reformate your hard disc, all of these would be devastating to your computer and very dangerous to the security of your life in general. Viruses can even use your computer as a launching pad, hijacking your email in order to spread itself to other systems ("What Is a Computer Virus?" 2015).

Phishing is another form of malware. Phishing occurs when a cyber criminal creates a convincing message, that is sent most often through email, to your computer. The message usually impersonates a business and asks that you fill out information in order to rectify a problem with your status in the business. The messages often contain threats to terminate your account in the business if you do not send the information. Through this method cyber criminal trick people into giving up their private information such as credit card numbers, names, addresses, social security numbers. They gain these pieces of information and then commit crimes in the name of the person whose information they stole. This is commonly referred to as identity theft (Phishing, 2015). The digital age can be a dangerous place for the unwary, with cyber criminals lurking behind every false email and phony web page, but honest users are not helpless in the fight to prevent cyber criminals from accessing their personal information.

The greatest way to fight against malware and cyber crimes is to prevent them from happening in the first place (How to remove virus from PC or laptop, 2015). Most forms of malware are stopped before they can even do any damage to

the computer (What is a Computer Virus?, 2015). This is made possible by

programs such as firewalls, antivirus and antispyware programs, all of which

prevent malware from infecting your computer. Apart from anti-malware programs

there are several practical steps that people can take to prevent infection. Users

should not read suspicious emails, click on links whose title does not match its URL,

they should never act on impulse because of a threat of account termination in an

email (How to recognize phishing email messages, links, or phone calls, 2015).

Finally, if a virus or other form of malware does get onto a computer, then the user

should immediately shut down their device and enter Safe Mode which is a program

that allows a computer to run without doing further damage to the system (How to

remove virus from PC or laptop, 2015). Then the user should download or plug in

(via USB) a program that scans the system, collects corrupted material, stores them

and erases the virus.

The digital age is a dangerous time for the unwary user. Cyber criminals

have taken advantage of the fact that most any device, computer, tablet, or phone,

can connect to the internet and can often contain sensitive information. But if the

user is carful and seeks to become "tech-savvy" they can avoid the traps set by most

cyber criminals. We must be knowledgeable about our devices, because even in the

digital age we cannot leave our security solely in our computer's hands.

WORKS CITED

"Four Ways Hackers Can Install Malware on Your Mobile Device." - *How to Protect Yourself from Identity Theft*. N.p., n.d. Web. 02 Nov. 2015.

"How to Recognize Phishing Email Messages, Links, or Phone Calls." *What Is Phishing*. N.p., n.d. Web. 02 Nov. 2015.

"How to Remove a Virus, and Other Malware Blasting Tips." *PC Advisor*. N.p., n.d. Web. 02 Nov. 2015.

"Phishing | OnGuard Online." *Phishing | OnGuard Online*. N.p., n.d. Web. 02 Nov. 2015.

"What Is a Computer Virus?" *Computer Virus: What It Is and What It Does*. N.p., n.d. Web. 02 Nov. 2015.