Book Review of How to avoid becoming a victim

James Bowers, Jr.[1]
Indiana University of Pennsylvania, USA

H. Thomas Milhorn, MD, PhD, Cybercrime: How to avoid becoming a victim, 2007, Boca Raton, FL: Universal Publishers, 309 pages. ISBN:1-58112-954-8

The book, Cybercrime: How to avoid becoming a victim, written by H. Thomas Milhorn, MD, Ph.D. sets out to educate its readers about the many different types of cyber crimes and ways in which internet users can protect themselves from becoming victims. According to the author, cyber crime is identified as "any type of activity that uses the Internet to commit a crime (p.1)". A broad area of cyber crime is covered throughout the book with special emphasis given to defining what constitutes each type of crime, poignant examples of actual crimes, and finally, useful tips for protecting yourself from each type of crime. Indeed, there are 36 chapters in the book, covering almost every conceivable area of cyber crime, areas such cyber bullying and immigration fraud, as well as the more popular predator and credit card fraud. Appendix A provides the readers with information on how to report cyber crimes, specifically which office they should contact. Appendix B provides an essential glossary for cyber terminology. The purpose of this review is to provide readers with an overview as to what to expect from it.

Milhorn is a retired professor who has penned over 150 papers (both research and education) as well as four books (three nonfiction and one fiction). He taught for the University of Mississippi Medical Center, where he was a professor of Physiology and Biophysics, as well as an associate professor of Psychiatry and Human Behavior. He holds several certifications and is educated in other areas above and beyond his medical training including: mental health counselor, addictions counseling coursework, and theology. Milhorn's interests include web design and teaching computer classes for adult students. Although is areas of expertise are not cyber crimes, he does provide a thorough examination of the particular areas. Milhorn's Curriculum Vitae can be found on his own webpage: http://www.milhorn1.netfirms.com/.

Computers are now in every country, and are accessible by a vast majority of persons in industrialized countries. Internet-connected people must know how to protect themselves from the online dangers. Milhorn's goal with this book is to provide a vast repository of protective measures, both for the novice and the veteran in computer use.

[1] Department of Criminology – Doctoral Program, Indiana University of Pennsylvania, PO Box 13, Ernest, PA 15739 724-992-1453 Email: zxmm@iup.edu

He wants the internet to be as safe as it can be for its users. Milhorn sets out to educate the world after his own personal attacks from hackers. His modem was hijacked by an anti-spyware company, as well as a number of viruses. False charges were added to his credit card after he purchased items online. This book was written in response to those attacks. Again, the prevention aspect is out of the area of his expertise, but any reader will find his personal crusade to be well researched.

Milhorn explains that the categories of cyber crime involve persons, property, or organizations. These crimes can be a single event, presented from the perspective of the victim, or a series of event, which are explained by the multiple incidents with the victims. The chapters cover a broad range of topics. Auction fraud, job scams, charity scams, child pornography, copyright violation, cramming and slamming, credit card fraud, credit repair scams, cyber bullying, and cyber extortion begin the earlier chapters. The next chapters cover cyber extortion, cyber-harassment and cyber stalking, cyber hijacking, cyber snake oil, cyber terrorism, dating scams, education scams, gambling scams, hacking, and identity theft. Also, immigration fraud, investment fraud, laptop theft, loan scams, lottery scams, Nigerian fraud, overpayment scams, predatory scams, predatory behavior, pyramid schemes, prostitution, sales fraud, and spam. Lastly, travel scam, viruses, and hoaxes are discussed.

Most people are aware of the obvious aspects of cyber security, such as having an appropriate firewall, up to date anti-spyware, and anti-virus software. But, there are areas that even experienced computer users may fall prey to traps. The story of Jake Bisenius tells of one such trap that anyone could be a victim of. Jake lived in Washington and wanted to buy a Sony Play Station II for Christmas. He thought he was receiving a deal with the total cost being $275. He was told "We guarantee the item to be exactly as shown below" (p. 26). Mr. Bisenius had no idea that the ad was a picture of the Play Station, and nothing more. The seller had been correct, albeit dishonest as Mephistopheles in a Faustian story. Milhorn warns buyers to search for delivery information, return policies, and warranties before making online purchases. Milhorn also recommends using legitimate escrow accounts (accounts set up by a third party to handle the money). It remains unclear how to do so. This is a weakness of the book that could be turned into a strength in future editions. Many sites can be made to look like the original, but in fact could not be further from the truth. The book does provide many other tips in addition to the one above.

Another story of online fraud involves travel scams. Many people search the internet for deals when wanting to travel. Milhorn asserts that when a deal seems too good to be true, it probably is. Donna Copeland of Colorado desired to travel to Maui. The trip she booked through the online company included airfare and hotel rentals. She emailed Sunscapes to ask questions, only to find there was no return email. A quick internet search revealed that the company went out of business. She was still charged the $2,100 bill. Milhorn advises buyers to research the company. At the risk of sounding like blaming the victims, Copeland should have researched Sunscapes, since it was not a 'popular' or well-known site. Also, Milhorn recommends that all packages be confirmed. A problem with this recommendation is that the scam artist could still be answering the phones, confirming a flight that will not happen.

The last area to be mentioned is on viruses, worms, Trojans, and spyware, which are arguably the most dangerous parts in regards to the security of your computer. Whenever a person visits a website, there are cookies that are posted to the person's

computer. Later, trawlers can determine which websites a person visited and gather information on that person. Visiting websites, such as porn sites greatly increases the risk to a person's computer security. Milhorn vehemently advises to steer clear of these sites. Pop-ups are also dangerous. Some of them are set up to look like a regular window, so when a user goes to close the window, it is actually a button to download spyware. Milhorn recommends using the Alt + F4 function to close the popup window. This way, the window is actually closed, without putting your computer in peril. Examples of such perils include what is referred to as 'keystroke loggers'. Keystroke loggers are programs that can capture information about a person when they use their computer. Imagine having this spyware on your computer. When ordering products online, someone can view your credit card number, your name, and expiration date. This can wreak havoc on your credit history, because disputes must be filed within 60 days, and few people read their credit history that frequently. Even when proper police forms are filled out, the victim may still incur the credit charges that do not belong to them.

The intended audience range from children to senior citizens, both the novice and lay person to the experienced computer users and those in academia. In the section on cyber bullying and stalking, Milhorn advises children to tell their parents of the situation to resolve it. Also, Milhorn warns parents to be cautious of their child's online activities, and not to allow children to have webcams in their bedrooms. This may seem commonsense to more experienced users, but parents must talk to their children about the dangers of internet predators. The section on online dating advises senior citizens that a 20's something younger man may not really be after their hearts, but their wallets instead. Indeed, a wide range of ages for the target population allows for practically anyone to benefit from reading the book. This book can easily be utilized by the persons in academia as a textbook, both at the undergraduate and graduate levels for such classes as cyber criminology and computer science classes. The setup allows for professors to pick and choose what sections to cover.

Strengths of the book include the fact that it is well organized by chapters. The chapters are in alphabetical order by crime, and as mentioned before cover 36 chapters. This allows the reader to go exactly where they want to read on a particular topic. There is a convenient reference section at the end of each chapter. This would allow any reader who wants to examine the original source the opportunity to do so. Another strength of the book is the glossary at the end, as well as the definition of key vocabulary words throughout the chapters. For example, the word cramming is "the illegal and unexpected adding of charges to a person's telephone service" (p. 64). As the reader navigates the book, there will be numerous new words that will be added to their vocabulary. At the end of the book, there is a list of agencies and their applicable contact information per cyber crime. This is for both specific and general crimes. The text is not difficult to read, so anyone could follow the advice Milhorn puts forth. Milhorn's book is well thought out and practical, with real world examples in each topic section. The major strength of the book is the proactive tips for preventing cyber crimes from happening to you. Finally, a well written and general overview of the crimes is presented in each chapter.

As mentioned before, the author is not an expert in the field of cyber security. He has written prior books, some on cyber crime, but his work on computers involves teaching an adult class on computers and that he like's web design. Some would argue he should not be writing this book because of a lack of expertise. He is medical doctor (MD), and PhD in physiology and biophysics. Another weakness of the book is

numerous typos. Milhorn writes "but in reality is a link to a criminal website whose goal is to still [sic] your credit card number" (p. 3). Also, he writes, "and all HTTPS (web traffic) uses [sic] ports 80 and 1080" (p. 4). The typos go on and on throughout the book, on page 6, 12, 17, etc. This author does not base his work on empirical peer-reviewed references. Instead, it seems he did a Google search for each chapter. It is possible that some of the websites will have changes or moved if someone tries to access them. In addition, some of the definitions are over simplistic. This may annoy some of the more advanced computer users. At times, Milhorn is not specific enough regarding topics and ways to spot a cyber crime happening to you. For example, for Milhorn, avoiding high-risk websites is offered as a way to protect yourself against cyber crime, however no mention is given that details how one would classify a website as "high risk". The author simply says to avoid them. He gives two examples of high risk websites: porn sites and gaming sites, but there are plenty of other high risk websites and he makes no mention of how to spot them. One last weakness is that Milhorn spends a lot of time on "scams/schemes" section of the book when they all pretty much carry the same message—"if it's too good to be true, it probably is." It could therefore be recommended to cut out a lot of this and replace it with more depth on already covered topics.

Overall, Milhorn's book delivers exactly what the title states it will deliver—a prevention of cyber crimes. It is debatable as to the quality of the recommendations though. This book should be read by all who use a computer. This book covers many topics in the area of cyber crimes. As time goes on, Milhorn will be adding to the variety of the chapters, as criminals find new ways to exploit computer users. This book is a handy reference tool, especially because of the format. Due to heavy reliance on the internet and the new breed of criminals it spawned, this book is a helpful tool that one can use to become educated about what may happen to them if they are not protected while online. Protection can be achieved through the reading and understanding of the chapters.