Book Review of Net crimes & misdemeanors: Outmaneuvering webspammers, stalkers and con artists

Mari B. Pierce[1]
Indiana University of Pennsylvania, USA

J.A. Hitchcock, Net crimes & misdemeanors: Outmaneuvering webspammers, stalkers and con artists, 2nd edition, 2006, Information Today, Inc., 459 pages. ISBN: 0-910965-72-2

When asking for an example of a criminal, it is fair to assume that few will describe those who commit unlawful acts using the computer. Rather, most will give an instance of violent crimes committed against individuals or crimes involving personal invasion of property. If someone actually used an example of a crime focusing around technology, it is likely they will use an Internet pedophile or a hacker for their illustration. Although an increase of media attention and community awareness has been brought to a few types of Internet crimes, the reality is that the magnitude of this problem is not known to the general public nor how we, computer users, should protect ourselves from potential victimization or obtain help if we become a target of these crimes. "Net crimes and misdemeanors are committed against more than 200,000 a year and the numbers are growing every day" (Hitchcock 2006, 2). With this quantity of victims, computer users need to know how to protect themselves. However, the average computer user is not technologically savvy.

J.A. Hitchcock understands the limitations of technical knowledge of the average computer user. Her revised edition of "Net Crimes and Misdemeanors: Outmaneuvering Webspammers, Stalkers and Con Artists" (2006) explains various types of Internet and computer based crimes, and provides definitions and tips applicable to the novice and experienced computer user. One of the nation's leading authority on cybercrime, Hitchcock has years of experience working with computers and technology. She has taught various college level courses, written for magazines and newspapers, gives lectures, appears

[1] Doctoral Candidate, Department of Criminology – Doctoral Program, and Assistant Director Criminology Advising Center Indiana University of Pennsylvania 1117, Chestnut Street, Indiana, PA 15701, USA. Email: m.b.pierce@iup.edu

on television and radio and trains law enforcement on how to track cyber criminals and provide assistance to victims. Currently, she is president of WHOA, Working to Halt Online Abuse, and also their Kids/Teens Division. Hitchcock's expertise is not based solely on her educational and professional resume; she herself is a victim of online harassment. Hitchcock shows that not only children and novice computer users, but also the most advanced online users, can fall prey to these criminals and their tricks. It appears that her goal is to educate computer users of the dangers of cyber world and how to be an informed user in order to safely navigate through the Internet. She also provides resources for those who find themselves the victim of a cybercrime.

Hitchcock's book is full of technical phrases and terms; however, she does not assume these terms are universally understood. Each chapter begins with a category of cybercrime and a thorough explanation. Her book does not speak only to those with an incredible amount of technological knowledge. Rather, this book contains definitions to all terms, provides real life illustrations of scams and other crimes, examples of those who have been victimized and provides tools to help all online users. This information is presented in such a way that it is easy to follow, interesting to read and also extremely informative.

The premise of this book is not for online users to be afraid to use the Internet or to cease their online activities altogether. Rather, it demonstrates that the cyber-world mirrors real life. Hitchcock states time and again that online users should never provide information online that they would not tell a stranger standing on the corner. Too often, naïve or trusting computer users fall prey to the idea that the Internet is safe and that what they say is anonymous. Hitchcock illustrates that this is not true. She begins by telling the story of her online victimization. This increases her credibility as she is not simply talking at computer users; rather, she understands where many of her readers may be coming from. Her desire to help the general public is apparent which adds credence to the information provided within the text.

Hitchcock was the victim of cyber-stalking. It began when she responded to an online post from a publication agency, Woodside Literary Agency's, call for manuscripts. Upon her reply, the agency requested that she submit her writing along with a reading fee. As an

already published author, she questioned this request and subsequently warned other writers seeking publication about this agency's credibility through her own various online postings. This seemingly helpful warning to fellow writers was seen by Woodward as a "call to war" (7).

Nearly immediately after her postings, her personal computer was hit with hundreds of emails, called email bombs. Her employer was also bombed by emails from "her" stating derogatory comments and antagonistic messages in her name began appearing on various website postings. Although Hitchcock contacted the Internet Service Provider (ISP) and changed her email address, the stalking did not cease. Her home address and phone number were also provided online and multiple men responded to these ads.

Although it would seem that Hitchcock or any other victim in this situation could receive immediate legal assistance for this harassment, actually victims face multiple challenges in obtaining help from law enforcement. At the time of her victimization, fighting cyber-stalking and harassment was foreign to most law enforcement agencies. Hitchcock was persistent, requesting assistance from local, state and federal agencies and still little to nothing was done. In fairness to these agencies, it was simply that they did not know how to help.

With the aid of her computer savvy friends, however, they were able to acquire information needed to file a civil lawsuit. Her frustration with the system, how difficult it was to find help to stop this harassment and her inability to obtain swift justice resulted in her increased determination. Hitchcock began to investigate the agency that was stalking her, testified before legislative sessions and helped to pass a bill making email harassment a crime in her state. Since then, other states have followed suite, often aided by her testimony. At the time of this publication, forty-five states had some type of cyber-stalking or harassment law. Hitchcock's stalkers eventually were convicted and sentenced for their crimes.

The book is divided into twenty-one chapters, which can appear overwhelming to those unfamiliar with computer technology. However, once the reader begins, the quantity of information is not as daunting as initially perceived. It is reader friendly in the sense that one can find specifically the topics for which they are seeking assistance. Topics range from decreasing SPAM, an online form of junk mail, to tips for online shopping and auctions, avoiding identity theft, safely chatting in chat rooms and online dating. Although, Hitchcock does

explain all terms and types of crimes in lay terms, as a non-technical computer user, the chapters discussing web encryption, viruses and other types of intrusions, and filtering software, although described in rudimentary detail are still intricate and challenging to comprehend.

Hitchcock not only addresses the common forms of Internet nuisances such as SPAM and innocent urban legends and hoaxes passed via email, she also speaks to more dangerous types of online manipulation which even the savviest individuals have fallen prey. Her rule of thumb to Internet users is that if it sounds too good to be true, it probably is. Although this seems apparently obvious, for some reason, individuals who would never participate in such activities in the real world, will willingly pass out personal information, hand over money or send on chain letters when red flags are waving furiously. She gives examples of a number of scams which many haven fallen prey.

The Nigerian scam is just one of the multiple schemes commonly seen online. The email which arrives in one's inbox usually involves a story about an unclaimed inheritance. The writer is seeking assistance and in exchange the recipient of the email message will receive a percentage of the money. This is just one scam that has developed with technology, as this one has been around for decades, long before the existence of the Internet. Although this is not a new trick, a number of individuals have fallen victim to this, losing great amounts of money. Hitchcock is again reinforcing her point that people are inherently trusting online. Not all scams are as seemingly outlandish as the one just described. Many appear genuine.

Cyber-criminals have the ability to create emails and links from what appears to be a credible account or business. These emails often state that account information needs to be updated in order to verify the user's identity. A mirrored official logo or slogan of a legitimate company is often posted in the email. This is how these scammers steal identities. For those who do not know what to look for, it is easy to fall victim. Hitchcock provides a number of examples, including visual images of website pages in order to help the reader clearly identify the differences between the valid and false WebPages.

There are websites for nearly anything that a consumer can possibly want. Many are legitimate, actually most probably are; however, amongst these are always websites with fraudulent intentions. Consumers seeking children to adopt, friends or romantic partners must be especially attentive. Scams and frauds committed

through these types of sites are often the most heartbreaking as the victims typically have true intentions, are optimistic and seeking genuine companionship or other types of relationships. Hitchcock tells the stories of multiple victims and provides useful tools to any computer user who searches and participates in these sites.

Protecting children is also addressed in this text. The majority of the book speaks to how adults can keep themselves safe while online. Parents cannot adequately protect their children if they do not know how to defend themselves. Public attention and law enforcement emphasis on those who target children online has recently exploded due to the multiple instances of children falling prey to pedophiles through chat rooms and other types of online communication. This awareness has led to many parents taking a proactive stance about their children's online use. Hitchcock discusses the importance of monitoring children's online activities through filtering or monitoring software, keeping the computer in a high traffic room in the home, talking with children about the dangers of online use and providing them information about what to do if they are approached by a stranger online. Hitchcock's suggestions regarding software, although seemingly difficult to understand to a non-technical parent, are thoroughly explained, visual examples are given and websites are provided to find more information.

The most basic tool to prevent computer intrusion is often overlooked. Although nearly every computer comes with anti-virus software, unless it is updated timely and used properly the computer is not fully protected. This is the first step in avoiding the many problems and issues that computer and Internet users can face. Without this software, seemingly innocent emails with attachments from friends could result in invasion. Hitchcock again provides multiple examples, basic guidelines, visual depictions and other suggestions in order to keep the computer and its user safe.

This book is a must have addition to the personal library of every computer user. Beginners to cyber-world could benefit from learning the many scams and tricks present online and could possibly avoid problems which many newcomers to the online world face. Computer Science students or Criminal Justice/Criminology students in an introductory cybercrime class would benefit from this text as it thoroughly speaks to issues in both disciplines. As a inexperienced computer user it is difficult to speak to those who are, however,

Hitchcock claims that "it is not written so simply that experienced Internet users will find it too basic" (2). With that said, it appears that this text is geared toward the education of those naïve and unfamiliar with the newest technologies and the dangers that lurk online.

This text teaches Internet users the tools needed to attempt to stay ahead of those preying on the innocent and how to feel secure online. Although the reality is, this is nearly impossible. This is where this book could benefit all users; those who are currently being victimized can find plenty of resources to aid them. Hitchcock does not claim that her book is all inclusive, however, with the information provided a novice computer user, a computer science student with limited knowledge in the field of criminal justice and criminal justice/criminology students with a narrow awareness in the field of computer technology will walk away with an incredible about of useful knowledge for their education as well as information needed to keep themselves and their families informed and safe.