

*Net Crimes & Misdemeanors*, by J.A. Hitchcock is a book that every attorney should own simply because the Internet affects virtually every facet of life. It is the perfect reference manual for both experienced and inexperienced Internet users. Emphasis is placed on encouraging the reader to understand the severity of cyber crimes and how to prevent them, or in the worst case, what remedies are available to victims of it. The author believes that for every crime that occurs in the real world, a corresponding crime has or will occur over the Internet.

Today, Hitchcock is a cyber crime expert who lectures to and trains law enforcement around the country about cyber crime. She points out how few of her students are up-to-date on cyber crime issues, as indeed she was not before she experienced such crimes firsthand. Hitchcock begins her book by discussing how at the time she became a victim of harassment and stalking over the Internet, she considered herself an experienced Internet user. She then provides the reader with a unique perspective of the impacts of Internet crime by illustrating, through her own life experience, that even the most experienced Internet user can become a victim.

During this roller-coaster ride of email bombs and harassment, Hitchcock highlights the frustration many victims encounter when trying to engage law enforcement to apprehend and punish a perpetrator. In reality, law enforcement is not as educated as it needs to be about the intricacies of Internet crimes. At the time the author was victimized, there were few laws in place to protect victims of Internet crimes. Hitchcock remembers law enforcement's response to her when she requested legal assistance with her Internet harassment claim. Specifically, law enforcement responded, "I don't know what to tell ya lady." This forced Hitchcock to become educated and eventually become

an “expert” in cyber crime. Hitchcock went on to win a lawsuit against her harasser. She later testified in front of the Maryland legislature and submitted written testimony to the California legislature, resulting in those states passing cyber stalking bills. Today, Hitchcock serves as the president of an organization called “Working to Halt Online Abuse, a group that works with one hundred cyber crime victims per week.

In this book, Hitchcock thoughtfully discusses every major type of on-line crime in its own chapter, including identity theft, credit card fraud, cyber stalking and harassment. Each chapter is cleverly structured beginning with the presentation of a cyber crime topic and then illustrating that topic with actual case examples. Hitchcock concludes the chapter with “preventative tips,” remedies for victims and definitions of key terms used within that chapter. Hitchcock’s preventative tips include pictures of computer screen prints, enabling the reader to visualize exactly what the author is discussing. The book concludes with a comprehensive, chapter-by-chapter list of over one hundred websites that victims and prosecutors alike can contact to obtain assistance, report a crime or simply educate themselves. This listing is followed by a comprehensive glossary of terms that not only assists the reader’s understanding, but also serves as a useful reference tool.

Hitchcock warns that the Internet is a great place for identity and credit card theft because most websites that sell merchandise sell consumer’s personal information. Perpetrators can easily commit credit card fraud because unlike in person, there are no witnesses or video cameras, no signed receipts and no requirement to show the sales clerk the credit card. She also warned that cyber stalking, which occurs when the stalker

follows the victim around on-line, is the most prevalent type of on-line harassment because anonymity provides the stalker with a feeling of “invincibility.”

Throughout the book, Hitchcock stresses three main difficulties victims and law enforcement encounter in trying to catch and prosecute cyber criminals. First, the Internet allows users to remain anonymous. Second, information is easily altered or deleted in a split second. Lastly, there are still inadequate cyber-related laws and legislatures are often slow in responding to new technology. First Amendment protections also make it difficult to ban most kinds of speech or prohibit anonymity. In fact, Hitchcock observes that there seems to be more latitude with on-line speech, especially where there is no “direct” physical threat made. Courts are also frequently faced with jurisdictional issues due to the lack of geographical borders in the cyber-world. Currently, some states have Computer Crimes Task Forces that conduct criminal investigations, mostly focusing on crimes against children, stalking and harassment.

The author wraps up by pointing out that hackers are everywhere and are constantly trying to gain illegal access to a victim’s computer. In fact, one small business owner reported that he sees five attempts per hour to hack into his computer. When he is in chat rooms, this number increases to over twenty per hour because hackers have a longer time to attempt to access his computer. Thus, Internet users should be aware of the amount of time they spend at unsecured web sites.

The moral of this story is, get educated.