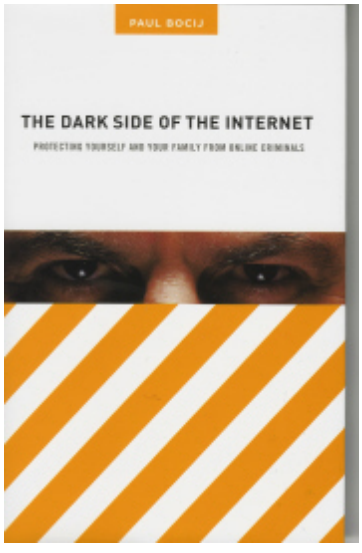

The Dark Side of the Internet

Edition: 1st

Author: Paul Bocij

ISBN 027598575X

Publishers: Praeger

Price £25.99

Publication Date: 30th Oct 2006

Publisher's Title Description:

In less than a decade, personal computers have become part of our daily lives. Many of us come into contact with computers every day, whether at work, school or home. As useful as the new technologies are, they also have a darker side. By making computers part of our daily lives, we run the risk of allowing thieves, swindlers, and all kinds of deviants directly into our homes. Armed with a personal computer, a modem and just a little knowledge, a thief can easily access confidential information, such as details of bank accounts and credit cards. This book is intended to help people avoid harm at the hands of Internet criminals. It offers a tour of the more dangerous parts of the Internet, as the author explains who the predators are, their motivations, how they operate and how to protect against them. Behind the doors of our own homes, we assume we are safe from predators, con artists, and other criminals wishing us harm. But the proliferation of personal computers and the growth of the Internet have invited these unsavory types right into our family rooms. With a little psychological knowledge a con man can start to manipulate us in different ways. A terrorist can recruit new members and raise money over the Internet. Identity thieves can gather personal information and exploit it for criminal purposes. Spammers can wreak havoc on businesses and individuals. Here, an expert helps readers recognize the signs of a would-be criminal in their midst. Focusing on the perpetrators, the author provides information about how they operate, why they do it, what they hope to do, and how to protect yourself from becoming a victim.

The Author

PAUL BOCIJ is a published writer of numerous computer training titles and has published articles on various cybercrimes in journals such as The Criminal Lawyer and Prison Service Journal. He is the author of Cyberstalking (Praeger, 2004).

Reviews

Anyone who owns a computer must have encountered that moment when they feel like tearing their hair out or picking up the computer and throwing it out of the window.

There is every chance the moment may have been brought about by those unpleasant people who for some reason known only to themselves, spend their lives hell-bent on destroying other people's work or pleasure, viz the writers of viruses, trojans and worms.

As well as fully covering the subject of on-line criminals, this book actually goes on to examine who writes viruses and why. Apparently it is curiosity, educational, enjoyment, status and social benefits, political, financial gain, or revenge, which covers just about everything except a sick mind!

We are reminded on Page 59 of the importance of back-up in the section on 'Dealing With Viruses'. I learnt very many years ago the three most important words in computing, 'Back-up, back-up, back-up' or the Grandfather, Father, Son routine', which of course I fail to adhere to.

This same section deals with the importance of Anti-Virus software, which I have used for many years. I still do not rely on Windows and run Norton, which I personally have found very effective.

This is an excellent book, which covers everything you need to know and I will certainly recommend it to all my family and friends. My copy will not be far from my desk.

We are told on the cover that, 'We assume that behind the doors of our homes, we are safe from predators, con-artists and other criminals wishing us harm'. The truth is as the Sergeant always told the patrols in 'Hill Street Blues' "Be careful out there people".

In addition to matters already mentioned, the book also covers Spy and Adwear, Identity theft, Fraud, Junk E-Mail and much more. If these words mean nothing to you, then this book would be a very good place to start.

Rob Jerrard

REVIEW OF “THE DARK SIDE OF THE INTERNET”

REVIEW WRITTEN BY

SALLY RAMAGE®

JULY 2007

“This book is a crime prevention book on internet crime, not a law book. The book appears to be written with a view to crime prevention and with the perspective of a crime prevention practitioner. Paul Bocij relates the methods used and opportunities sought by the internet criminal. This book arms the reader with information and crime prevention techniques that can be used to avoid victimisation. In this respect Paul Bocij’s "Dark Side of the Internet" is an educational book. Just as you would protect your physical self and belongings with property protection devices such as burglar alarms, locks, CCTV and other security devices, you should protect your physical and mental self and our finances on the internet with access control strategies, virus protections, passwords and keeping to the rules for information security.

Its 253 pages contain 12 chapters, namely-

Cyberterror.

Cyberattacks.

Viruses, Trojans and Worms.

Spyware and Adware.

Identity Theft.

E-mail fraud.

Auctions and other forms of Fraud.

Junk e-mail.

Intellectual Property theft.

Cyberstalking.

Online relationships.

Deviant subculture.

Each chapter of the book ends with useful website addresses and details of books for further information on that particular topic. At the end of each chapter are brief guidelines drawn from the FBI, the National Consumer League, the National Centre for the Victims of Crime, the US Department of Justice and others. There is included a glossary which is to be found at pages 205 to 218. The books also has an extensive bibliography.

After reading through this book, I did not want to go to my computer for some time, but for most people that alternative is not viable in this information age. When considering internet crime, we must remember that it is not the internet that commits crime but people who lie, cheat and steal. Offenders are to blame for the bad reputation of the internet. The internet is just the system in which cybercrimes are committed. Some such offenders are those who constructed the system itself. For example, with regard to cyberattacks, Paul Bocij says (on page 27) that "Research has shown that most security incidents originate from within the organisation".

The most disconcerting thing I have read in this book on cybercrime is the attack on the public at large in ways such as chain e-mails, petitions and charity and disaster-fund relief fraud. Bocij says that, "whenever a major disaster takes place, it is only a matter of hours before criminals try to take advantage. Online frauds relating to disaster relief have appeared after major incidents around the world, including 9/11 and Hurricane Katrina. Typically, millions of e-mails are sent out asking for donations. Following the link given in the e-mail message takes the Internet users to a web site that appears to belong to a genuine charity. The site asks people to make a donation by credit card and anyone who does so risks becoming a victim of identity theft".

Identity theft is a financial crime. In identity theft on the internet, the suspect assumes the identity of the victim through use of personal information and uses the new identity to commit fraud. The primary element for the success of identity theft is obtaining the personal information of the victim.

Chapter 6 deals with e-mail fraud such as phishing and 419 "scams". Email frauds are usually frauds against the individual.

Chapter 12 discusses the ways that sexual deviants target children and vulnerable adults. A paedophile on the internet simply develops a relationship and seduces children over a period of time, all the while parents being oblivious of this relationship. Oftentimes parents have not installed parental controls or filtering software on their children's computers. Children's computers are usually positioned in the privacy of bedrooms where illicit secrecy is fed. The book educates the adult reader who can then educate children about not giving out their names, telephone number, address or parent's information to anyone on the internet.

My comment on internet crime is that the internet does not have territorial boundaries like our physical environment. As human beings, we passionately confirm to ownership of our territory and this invokes our protective care. The internet does not give the same perception of territoriality or protectiveness that people have for their homes, streets, parks and countries. The internet facilitates anonymity and secrecy and herein lies the roots of the crime. "The Dark Side of the Internet" is an informative crime prevention book".

Sally Ramage