Executive Summary

Identity theft is an old misdeed, but the growth of Internet and e-commerce has taken it to a whole new level. Using widely available Internet tools, thieves go "phishing" and "pharming" to trick unsuspecting computer users into providing personal data, which they then use for illicit purposes. All of this is possible because face-to-face client relationships do not exist on the Internet. Establishing one's real identity for online transactions is complicated, thereby making fraud easier.

The potential for fraud is a major hurdle in the evolution and growth of online commerce. E-payment and e-banking services – the focus of this book – suffer substantially from public mistrust. In the United Kingdom, for example, a recent study estimated that 3.4 million people were unwilling to shop online owing to concerns about online security.

Given the growth of online ID theft, many OECD member countries have taken steps to ensure that consumers and Internet users are adequately protected. These steps encompass various measures: consumer and user-awareness campaigns, new legislative frameworks, private-public partnerships, and industry-led initiatives focused on technical responses.

Despite these initiatives, most countries have not sufficiently addressed the problem of ID theft, and online ID theft in particular. Thus, the scope, magnitude and impact of ID theft vary from one country to another, or even from one source to another within the same country. These differences reflect the need for a more co-ordinated response at both the domestic and international levels.

The purpose of this book is threefold: (1) to define ID theft, both online and off-line, and to study how it is perpetrated, (2) to outline what is being done to combat the major types of ID theft, and (3) to recommend specific ways that ID theft can be addressed in an effective, global manner.

The tools of the trade

As explained in Part I of this book, there are three main methods thieves use to obtain personal information via the Internet and/or individual computers:

- Malicious software (malware) is surreptitiously installed into a computer or device – fixed or mobile – to collect the user's personal information over time.
- Computers or mobile devices are hacked into, or otherwise exploited, to obtain the user's personal data.
- "Phishing," whereby thieves use deceptive e-mails to get users to divulge personal information, includes luring them to fake bank and credit-cards websites. These phishing messages, commonly distributed by e-mail spam, are also used to install malware on the computers of unsuspecting recipients.

Phishing techniques are becoming more sophisticated and harder to detect. Some aptly named principal forms are:

- "Pharming": using deceptive e-mail messages to redirect users from an authentic website to a fraudulent one, which replicates the original in appearance.
- "SMiShing": sending text messages ("SMS") to cell phone users that trick them into going to a website operated by the thieves. Messages typically say that unless users go to the website and cancel, they will be charged for services they never actually ordered.
- "Spear-phishing": impersonating a company employee/employer via e-mail in order to steal colleagues' passwords/usernames and gain access the company's computer system.

ID thieves misuse victims' personal information for a plethora of unlawful schemes. Typically, these involve: misuse of existing accounts; opening new accounts; fraudulently obtaining government benefits, services, or documents; health care fraud; and the unauthorised brokering of personal data.

Challenges in addressing online ID theft

Part II of this book outlines what is currently being done to address online ID theft at the domestic and international levels. There are ongoing efforts, but they are stymied by two major issues:

1. *Lack of a common definition.* ID theft is defined differently in OECD member countries: some view it as a specific crime, while others regard it as a preparatory step in the commission of other wrongs or crimes. Lack of a common definition for ID theft may complicate efforts to combat the problem in a comprehensive, cross-border fashion.
2. *Lack of comparable data.* ID theft (whether offline or online) has largely failed to attract the attention of statisticians. Most data are from the United States; statistics for Europe are sparse, except for the United Kingdom. When data are available, they often do not cover ID theft as an independent wrongdoing. The United States is one of the few countries with data that analyse ID theft as a separate offense.

In addition, statistics are collected differently by countries, complicating cross-border comparisons. Moreover, findings of public and private entities vary greatly: some sources conclude that the scale of ID theft has declined in recent years, resulting in growing consumer confidence. Other sources show ID theft is on the rise.

Prevention and enforcement strategies

Domestic level: As discussed in Part II, the public and private sectors in most OECD member countries rely on a range of consumer and user-education tools to combat ID theft. In some countries, information is shared among various public and private entities in order to investigate and prosecute ID theft. Resources for policing are limited, however, in many countries.

Companies in some countries understand the need to deploy human resources and security strategies to prevent data leakage. Nevertheless, there is a recognition that more needs to be done to ensure they adequately prevent those data security breaches.

A few countries have taken steps in this direction, imposing an obligation on data collectors, such as requiring companies and Internet Service Providers (ISPs) to disclose data breaches affecting customers and the public. Other countries are still considering whether such disclosure should be mandated by law. In some European Union member states, ISPs are requesting the right to act on behalf of their customers if personal information is misused and results in direct or indirect losses.

International level: Various international organisations and groups are involved in fighting cyber fraud. The OECD, for example, has developed policy responses in the areas of fraud against consumers, spam, security and privacy, including the *2006 Anti-Spam Toolkit* and the *2003 Cross-border Fraud Guidelines*. In addition, there have been a number of bilateral, multilateral and regional initiatives in which law enforcement, police and government entities have joined forces to prevent and prosecute online ID theft.

Public-private international initiatives: Some efforts are data-sharing fora for gathering statistics on phishing, malware and other online threats. Other efforts are enforcement-oriented, in which the private sector assists governments with investigations, implementing technology, and developing customised legislation and best practices for stemming online ID theft.

Conclusions and recommendations

The analysis in this book suggests that policy makers should address a number of issues in order to advance the fight against ID theft:

- ***Definition*** – The lack of a common definition of what constitutes identity theft may stymie efforts to address the problem in a comprehensive fashion, across borders.
- ***Legal status*** – ID theft/fraud is not an offence per se under most OECD member country laws. It is a crime in a few. Whether ID theft should be treated as a stand-alone offence, and criminalised, needs to be considered.
- ***Co-operation with the private sector*** – The private sector should actively participate in fighting ID theft. OECD member countries could consider more restrictive laws that increase the penalties imposed on ID thieves and could engage in outreach to the private sector to encourage entities to: i) launch awareness campaigns; ii) develop industry best practices; and iii) develop and implement technological solutions to reduce the incidence of ID theft.
- ***Standards*** – Member countries should examine establishing national standards for private sector data-protection requirements. They should consider requiring the disclosure of data-security breaches at companies and other organisations that store data about their customers.
- ***Statistics*** – The production of more tailored and accurate statistical data, covering all OECD member countries, could help determine the impact of ID theft on the digital marketplace.

- ***Victim assistance*** – OECD member countries could consider developing assistance programs to help victims of ID theft recover/minimise their injury.
- ***Remedies*** – Member countries could consider whether to enact legislation to provide more effective legal remedies for victims of ID theft.
- ***Deterrence and enforcement*** – The lack of criminal laws prohibiting ID theft and the limited resources of law enforcement authorities indicate there is insufficient deterrence. Member countries could explore the value of increasing resources for law enforcement, ID theft investigations and training. More generally, given the rapid evolution of ID theft techniques and methods, more resources and training could be granted to all OECD authorities involved in the battle.
- ***Education*** – Consideration could be given to broadening education on ID theft so as to cover all interested stakeholders including consumers, end users, governments, businesses and industry.
- ***Co-ordination and co-operation*** – Agencies involved in the enforcement of ID theft rules and practices are numerous at both domestic and international levels. Their respective roles and framework for co-operation could be clarified to help enhance their effectiveness.

Consideration could be given to improving domestic law enforcement co-ordination by developing national centres dedicated to the investigation of ID theft crimes. With regard to co-ordination and co-operation with foreign law enforcement authorities, member countries could explore areas of mutual interest, such as: i) enhancing deterrence; ii) expanding participation in key international instruments (e.g. the Council of Europe Convention on Cybercrime); iii) and improving response to requests for investigative assistance; and iv) otherwise strengthening co-operation with foreign partners (e.g. in training law enforcement).

This book addresses issues and concepts of a technical nature which might evolve rapidly. The laws may have changed since first publication, and the reader is cautioned accordingly.

Glossary

Backdoors: A malicious software program that allows an attacker to access a system by listening to commands on a certain User Diagram Protocol ("UDP") or Transmission Control Protocol (TCP) port. Backdoors facilitate the attacker's acquisition of information such as passwords and allows the attacker to execute remote commands.

Bots and botnets: Some malware is distributed using botnets, a group of "zombies" or bots infected computers compromised though malware and turned into malware that can be used to carry out attacks against other computer systems. These computers become compromised when a bot program, a type of malware, is installed on the system.

Dumpster diving: Generally refers to the act whereby fraudsters go through bins to collect "trash" or discarded items. It is the means that identity thieves employ to obtain copies of individuals' cheques, credit card or bank statements, or other records that hold their personal information.

Keystroke loggers: A program that records and "logs" how a keyboard is used. There are two types of keystroke loggers. The first type of keystroke logger requires the attacker to retrieve the logged data from the compromised system. The second type of keystroke logger actively transmits the logged data.

Man-in-the-middle attack: The process by which the phisher collects personal data through the interception of an Internet user's message that was intended to be sent to a legitimate site.

Pharming: The use of deceptive e-mail messages to redirect users from an authentic website to a fraudulent one, which replicates the original in appearance.

Phishing: The use deceptive e-mails to get users to divulge personal information, includes luring them to fake bank and credit-cards websites.

Pretexting: A form of social engineering used to obtain sensitive information. In many instances, pretexters contact a financial institution or telephone company, impersonating a legitimate customer, and request that customer's account information. In other cases, the pretext is accomplished

by an insider at the financial institution, or by fraudulently opening an online account in the customer's name.

Rootkit: A set of programs designed to conceal the compromise of a computer at the most privileged base or 'root' level. As with most malware, rootkits require administrative access to run effectively, and once achieved can be virtually impossible to detect.

Shoulder surfing: In relation to ID theft, refers to the act of looking over someone's shoulder or from a nearby location as the victim enters her Personal Identification Number ("PIN") at an ATM machine.

Skimming: The recording of personal data from the magnetic stripes on the backs of a credit cards; data is then transmitted to another location where it is re-encoded onto fraudulently made credit cards.

SMiShing: The sending of text messages ("SMS") to cell phone users that trick them into going to a website operated by the thieves.

Spam: Commonly understood to mean unsolicited, unwanted and harmful electronic messages. here appears to be a growing correlation between malware and spam.

Spyware: A form of malware that sends information from a computer to a third party without the user's permission or knowledge. Different types of Spyware may collect different types of information. Some Spyware tracks the websites a user visits and then sends this information to an advertising agency while malicious variants attempt to intercept passwords or credit card numbers as a user enters them into a web form or other applications.

Trojan horse: A computer program that appears legitimate but which actually has hidden functionality used to circumvent security measures and carry out attacks. Typically a Trojan enters a user's computer by exploiting a browser vulnerability or feature.

Virus: A hidden software program that spreads by infecting another program and inserting a copy of itself into that program. A virus requires a host program to run before the virus can become active. The term "virus" is increasingly used more generically to refer to both viruses and worms.

Vishing: Phishing via Voice over Internet Protocol ("VoIP").

VoIP: A new technique using phones to steal individuals' personal information.

Worm: A type of malware that self replicates without the need for a host program. Worms can exploit weaknesses in a computer's operating system or other installed software and spread rapidly via the Internet. A mass-mailing worm is a worm that is spread out through bulk e-mail.

Bibliography

ACCC (Australian Competition and Consumer Commission) (2003), Court declares imitation Sydney Opera House website illegal, press release, 28 August 2003: *www.accc.gov.au/content/index.phtml/itemId/360431/fromItemId/378016*.

ACPR (Australian Centre for Policing Research) (2006), Review of the legal status and rights of victims of identity theft in Australasia, Report Series No. 145.2, Commonwealth of Australia: *www.acpr.gov.au/pdf/ACPR145_2.pdf*.

ANSI (American National Standards Institute) and BBB (Better Business Bureau) (2008) ANSI-BBB Identity Theft Prevention and Identity Management Standards Panel Final Report, 31 January 2008, *www.ansi.org/standards_activities/standards_boards_panels/idsp/report_webinar08.aspx?menuid=3*.

APEC (2006), Letter of Support from the Chair of the Telecommunications and Information Working Group, 20 March 2006, Strasbourg: *www.coe.int/T/E/Legal_affairs/Legal_cooperation/Combating_economic_crime/6_Cybercrime/T-CY/*.

APEC (Asian-Pacific Economic Co-operation) (2005), Strategy to Ensure a Trusted, Secure and Sustainable Online Environment, November 2005: *www.apec.org/apec/apec_groups/working_groups/telecommunications_and_information.html*.

APWG (Anti-Phishing Working Group) (2006a), Phishing Activity Trends, report for November 2006: *www.antiphishing.org/reports/apwg_report_november_2006.pdf*.

APWG (2006b), Phishing Activity Trends, report for December 2006: *www.antiphishing.org/reports/apwg_report_december_2006.pdf*.

APWG (2007), Phishing Activity Trends, report for April 2007: *www.antiphishing.org/reports/apwg_report_april_2007.pdf*.

ASWPRPCC (Australasian and South West Pacific Region Police Commissioners' Conference) (2005), Australasian Identity Crime Policing Strategy 2006-2008, report produced by the ACPR, December: 2005: *www.acpr.gov.au/pdf/ID%20Crime%20Strat%2006-08.pdf*.

British Telecom, CPP, Get Safe Online, Lloyds TSB, Metropolitan Police, Yahoo! (UK) (2006): Security Report, February 2006, *www.btplc.com/onlineidtheft/onlineidtheft.pdf*.

BWGCBMMF (2004), Report on Identity Theft, report to the Ministry of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, October 2004, *www.ps-sp.gc.ca/prg/le/bs/report-en.asp*.

BWGCBMMF (Bi-national Working Group on Cross-Border Mass Marketing Fraud) (US-Canada) (2006), Report on Phishing, October 2006, report to the Ministry of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States: *www.psepcsppcc.gc.ca/prg/le/_fl/Phishing%20for%20CBCF%202006-en.pdf*.

CAO (Cabinet Office) (Japan) (2006), Summary Report on the Enforcement Status of Act on the Protection of Personal Information in Fiscal Year 2005, June 2006: *www5.cao.go.jp/seikatsu/kojin/foreign/enforcement-status2005.pdf*.

CMC (Consumer Measures Committee) (Canada) (2005), Working Together to Prevent Identity Theft, A discussion paper for public consultation, 6 July 2005: *http://cmcweb.ic.gc.ca/epic/site/cmc-cmc.nsf/vwapj/Discussion%20Paper_IDTheft.pdf/$FILE/Discussion%20Paper_IDTheft.pdf*.

Deloitte Touche Tohmatsu, 2006 Global Security Survey: *www.deloitte.com/dtt/cda/doc/content//CA_FSI_2006%20Global%20Security%20Survey_2006-06-13.pdf*.

ENISA (European Network and Information Security Agency) (2006), Survey on Industry Measures taken to comply with National Measures implementing Provisions of the Regulatory Framework for Electronic Communications relating to the Security of Services, 2006: *www.enisa.europa.eu/pages/05_01.htm*.

European Commission (2007), Communication from the Commission to the European Parliament, the Council and the Committee of the Regions, Towards a General Policy on the Fight against Cyber Crime, 22 May 2007, COM(2007) 267 FINAL, *http://eurlex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf*.

European Commission (2006), DG SANCO, Special Eurobarometer, Consumer Protection in the Internal Market, September 2006, Brussels, *http://ec.europa.eu/public_opinion/archives/ebs/ebs252_en.pdf*.

European Commission (2004), Identity Theft: A Discussion Paper, Joint Research Centre, Institute of the Protection and Security of the Citizen, EUR 21098 EN, 2004.

European Commission FPEG (EC Fraud Prevention Expert Group) (2007), Report on Identity Theft/Fraud, FPEG, subgroup on identity theft, 22 October 2007: *http://ec.europa.eu/internal_market/fpeg/docs/id-theft-report_en.pdf*.

Europol (2006), EU 2006 Organised Crime Threat Assessment ("OCTA"): *www.europol.eu.int/publications/OCTA/OCTA2006.pdf*.

GetSafeOnline (UK) (2006), The Get Safe Online Report, October 2006: *www.getsafeonline.org/media/GSO_Cyber_Report_2006.pdf*.

Home Office Identity Fraud Steering Committee (UK) (2006), Identity Crime Definitions: *www.identitytheft.org.uk/definition.html*.

IDTTF (Identity Theft Task Force) (US) (2007), Combating Identity Theft: A Strategic Plan, 23 April 2007: *www.idtheft.gov*.

INTERVICT (International Victimology Institute Tilburg) (2006), The Challenge of Countering Identity Theft, Report Commissioned by the National Infrastructure Cyber Crime program ("NICC"), 6 September 2006, *www.tilburguniversity.nl/intervict/publications/NicolevanderMeulen.pdf*

ITRC (Identity Theft Resource Center) (US) (2004), Identity Theft: the Aftermath 2004, September 2005: *www.idtheftcenter.org/prteen1006.pdf*.

ITTC (Identity Theft Technology Council) (US), Online Identity Theft: Phishing Technology, Chokepoints, and Countermeasures, 3 October 2005, *www.antiphishing.org/Phishing-dhs-report.pdf*.

International Telecommunication Union (2006), Cybersecurity Awareness Survey, results as of 17 May 2006, *www.itu.int/newsroom/wtd/2006/survey/charts/q_8.asp*.

Javelin Strategy and Research (2006), 2006 Identity Fraud Survey Report, *www.javelinstrategy.com/products/AD35BA/27/delivery.pdf*.

Javelin Strategy and Research (2007), 2007 Identity Fraud Survey Report - Identity Fraud Is Dropping, Continued Vigilance Necessary, Consumer Version, February 2007, *www.javelinstrategy.com/uploads/701.R_2007IdentityFraudSurveyReport_Brochure.pdf*.

McAfee Avert Labs (2004), Anti-Phishing: Best Practices for Institutions and Consumers, White Paper, September 2004, *www.antiphishing.org/sponsors_technical_papers/AntiPhishing_Best_Practices_for_Institutions_Consumer0904.pdf*.

McAfee Avert Labs (2007), Identity Theft, White Paper, January 2007, *www.mcafee.com/us/threat_center/white_paper.html*.

McAfee (2006), Virtual Criminality Report, December 2006, *www.sigma.com.pl/pliki/albums/userpics/10007/Virtual_Criminology_Report_2006.pdf*.

Microsoft (2006), presentation by Nancy Andersen, Microsoft Vice-President, contribution to the European Commission's conference on "Maintaining the integrity of identities and payments: Two challenges for fraud prevention," The Threat of Cybercrime: The Challenge of Online Identity Theft and Strengthening the Public-Private Partnership in a Changing Threat Environment, 22 November 2006, Brussels, *http://ec.europa.eu/justice_home/news/information_dossiers/conference_integrity/doc/Presentation_Anderson.pdf*

NCL (National Consumer League) (UK) (2006), A Call for Action: Report from the National Consumer League, Anti-Phishing Retreat, Washington D.C., March 2006, *www.nclnet.org/news/2006/Final%20NCL%20Phishing%20Report.pdf*.

OECD (2006c), OECD Anti-Spam Toolkit of Recommended Policies and Measures, OECD, Paris, *www.oecd-antispam.org/*.

OECD (2009) Computer Virues and Other Malicious Software: A Threat to the Internet Economy.

OECD (2007d), The Development of Policies for the Protection of Critical Information Infrastructures, OECD, Paris, [DSTI/ICCP/REG(2007)20/FINAL].

OECD (1999), Guidelines for Consumer Protection in the context of Electronic Commerce, OECD, Paris, *www.oecd.org/document/51/0,2340,en_2649_34267_1824435_1_1_1_1, 00.html*.

OECD (2003), Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders, OECD, Paris: *www.oecd.org/sti/consumer-policy*.

OECD (1980), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, Paris: *www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1, 00.html*.

OECD (2002), Guidelines for the Security of Information Systems and Networks, OECD.

OECD (2006b), Mobile Commerce, DSTI/CP(2006)7/FINAL, Directorate for Science, Technology and Industry, *www.oecd.org/sti/consumer-policy*.

OECD (2006b), OECD Anti-Spam Toolkit of Recommended Policies and Measures, OECD, Paris: *www.oecd-antispam.org/*.

OECD (2006d), Protecting Consumers from Cyberfraud, OECD Policy Brief, Paris, October 2006: www.oecd.org/sti/crossborderfraud.

OECD (2007c), Recommendation and Guidance on Electronic Authentication, OECD, Paris: *www.oecd.org/dataoecd/32/45/38921342.pdf*.

OECD (2007b), Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, OECD, Paris: *www.oecd.org/dataoecd/43/28/38770483.pdf*.

OECD (2007), Recommendation on Consumer Dispute Resolution and Redress, OECD, Paris, *www.oecd.org/dataoecd/43/50/38960101.pdf*.

OECD (2006a), Report on the Implementation of the 2003 OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders, OECD, Paris, www.oecd.org/dataoecd/45/53/37125909.pdf.

OECD (2008), Scoping Paper on Online Identity Theft, DSTI/CP(2007)3/FINAL, Directorate for Science, Technology and Industry.

Table of Contents