



Telecoms Infotech Forum

Briefing paper

# e-Security in the Broadband Age

March 2006

<http://www.trp.hku.hk/tif/home.php>

# Telecoms InfoTechnology Forum

TIF is an industrial and policy forum run by the Telecommunications Research Project (TRP) at the University of Hong Kong, director Dr John Ure. The TRP provides background briefing papers for each TIF and posts these, together with presentations and proceedings papers, on the website [www.trp.hku.hk/tif](http://www.trp.hku.hk/tif). TIF is the source of funding of the TRP and relies upon sponsorship.

The output of the TRP is public domain research into economic, policy and regulatory aspects of telecommunications and related sectors such as IT, new media, Internet and e-commerce.

This TIF conference is supported by:

- Computing Technology Industry Association (CompTIA)
- Hong Kong Association for Information Systems (HKAIS)
- Hong Kong Computer Society (HKCS)
- Hong Kong General Chamber of Commerce (HKGCC)
- Hong Kong Information Technology Federation (HKITF)
- Hong Kong Internet Service Providers Association (HKISPA)
- Hong Kong and Mainland Software Industry Cooperation Association (HMSICA)
- Hong Kong Telecommunications Users Group (HKTUG)
- Hong Kong Wireless Technology Industry Association (WTIA)
- Information Security and Forensics Society (ISFS)
- Information and Software Industry Association (ISIA)
- Information Systems Audit and Control Association (ISACA) Hong Kong Chapter
- Internet Professionals Association (iProA)
- Internet Society – Hong Kong Chapter (ISOC-HK)
- Internet and Telecom Association of Hong Kong (ITAHK)
- Professional Information Security Association (PISA)
- The Office of the Telecommunications Authority in Hong Kong (OFTA)
- World Teleport Association (WTA)

The objective of TIF is to stimulate informed interest in the policy and regulatory aspects of information and communications technologies (ICTs), to foster greater transparency and a better understanding of the economic and technological dynamics of the sector, its impact on social welfare and its policy implications.

For further details of TIF and TIF membership, please contact:

Jenny Wan at the *Telecommunications Research Project*: tel: 2859-1919; fax: 2857-9434 or Email: [Trproj@hkucc.hku.hk](mailto:Trproj@hkucc.hku.hk)

### The Good

'Hong Kong Police Force's Technology Crime Division keeps a record of online and computer security crimes. Only 19 people suffered online theft in 2004, according to the division's data. There were only 11 reported cases of illegal access attempts via telecommunications equipment in 2004, down dramatically from 275 in 2000.' (*The Standard*, 8 August 2005)

### The Bad

In March 2006 it was discovered that for three years the personal contact details of 20,000 complainants to the Hong Kong police could be found by a simple search of the Internet. 'Mr Wong said workers had uploaded the database onto a website while converting it to be used on a more modern computer... While there was a password to protect the information loaded onto the site, there was nothing to stop it being downloaded.' It was then discovered that 600 individual insurance policy holders of ING Life, and the personal records of cellular mobile operator CSL customers had also found their way onto the Web. (*South China Morning Post*, 14 March 2006)

### And the Ugly

'An unprotected computer has a 40 per cent chance of being infected by a malicious worm within 10 minutes of being connected to the Internet. After an hour, the odds rise to 94 per cent.' (Sophos, an e-security company). 'Internet users believe they are more likely to be victims of a cybercrime than a physical one in the coming year.' (IBM survey, January 2006). 'Proceeds (US\$105 billion) from cybercrime exceeded proceeds from the illegal drugs trade in 2004'. (US Treasury Advisor, November 2005)

### e-Security

This TIF Briefing Paper explores the nature and evolution of spam, of different viruses (or malware, inclusive for any type of malevolent software) and the threats they pose, and the environment and social engineering that nurture them. It then considers some of the legal and organizational steps that can be taken to be secure when navigating the information superhighway, and what enterprises can do to maintain the security of their operations.

### Part 1: An Evolving Threat

Today there are more than 120,000 PC computer viruses but the first widespread one was the Brain virus discovered in January 1986. Brain infected 5 ¼ inch 360K floppy disks and spread around the globe without the benefit of the Internet or email. The 1996 Concept virus introduced an element of 'social engineering' where an email plays upon

human curiosity by tempting users to open files with subject lines ‘that ranged from the friendly to [the] salacious’.<sup>1</sup> The 1999 Melissa virus propagated worldwide in 48 hours and generated a large volume of email traffic, forcing many companies to switch off their networks.

Some viruses behave as ‘worms’ which means that they make copies of themselves and spread from computer to computer via email, office network, or removable media. Others act as ‘Trojan horses’ which are pieces of malicious code hidden within a legitimate application that do not actively try to spread but focus on the user’s machine.<sup>2</sup> Table 1 outlines some of the headline-making viruses.

Table 1: A Brief History of Infection

Date	Name	Description	Effect
1986	Brain	Named after Brain Computer Services, a store in Lahore, Pakistan; written for a doctor who suspected a colleague of stealing his research papers; meant to shut down the colleague’s computer as punishment	Innocuous: renamed floppy disk on which it found itself
1992	Michelangelo	Predicted to hit 5 million machines	Turned out to be far smaller than anticipated
1996	Concept	1 <sup>st</sup> cross-platform virus; macro virus to exploit security weaknesses in Microsoft applications	Infected Word documents on PC and Mac
1999	Melissa	‘Zero day vulnerability’ coined to describe this virus’s release and rapid infection	Caused US\$80 million in damage; clogged up email
2000	Love Letter, Love Bug	Disguised as message saying ‘I love you’; affected one in 28 emails at its peak; changed homepages and copied itself to emails.	Estimated to have caused more than US\$10 billion in damage; ‘one of the most destructive pieces of crimeware ever written’
2000	Klez-H	Hidden inside picture files	775,000 copies spotted
2001	CodeRed	Took advantage of security vulnerability in MS Internet Information Server (IIS)	About gaining notoriety for the virus writer trying to spread the virus as fast as possible
2001	NewPic CoolNow (2002) Choke (2006)	Special viruses for Instant Messaging (IM) networks	Some are capable of sending short messages to infected contact lists and ‘analyze’ the replies
2001	Nimda	Worm Sends itself by email.	The first worm to modify existing web sites and to use normal end user machines to scan for vulnerable web sites.
2003	Slammer	Virus	SQL Slammer infected 100,000 database servers within first 10 minutes of launch
2003	Blaster	Worm	Led IT departments to reimpose control, ending the ‘computing free-for-all’
2003	Sobig-F	Accounted for one in 17 of all emails sent, one million copies found in 24 hours	Led to massive global slowdown in email
2004	MyDoom	Accounted for one in 12 of all emails sent with 1.2 million copies found in 24 hours when virus was at its peak	Infected a quarter of a million computers in a day
2004	Cabir	First virus to hit mobile phones and transmit via Bluetooth	Mobile phone viruses are on the increase but there have only been 60 in the past two to 3 years compared to over 100,000 PC viruses
2005	Netsky.P	Worm; entices recipient to open a false failure notification of a returned email	Capable of disabling commercial anti-virus software
2005	Zafi.D	Spreads as an attachment to infected messages	Copies its file to the Windows system directory and runs on every system startup.
2005	Sober	Worm; has produced more than 30 strains; an example of ‘hactivism’, the combining of	Masquerades as an email from federal investigators (like the FBI, CIA, UK National

<sup>1</sup> ‘The virus world is kept alive by very human traits – a desire to communicate and share information, the overwhelming urge to look at pictures of comely young women.’ (‘The computer virus comes of age’, *Financial Times*, 30 January 2006)

<sup>2</sup> When viewed on an unpatched Windows machine, the Banker Trojan copies itself to the Windows system directories then, using a keylogger program, Banker monitors all of a user’s Internet transactions. When users log into an online banking site, Banker records all of the information they enter in an attempt to steal passwords and financial transaction data. A copy of the collected data is then surreptitiously e-mailed to the criminal who is controlling the Trojan. Brazilian newspapers reported that in the fall of 2005 53 people in Brazil had been arrested for using Trojans to steal a reported US\$30 million from online banking customers. (‘Trojans Can Trap Even The Wary’, *Financial IT Security*, March 1, 2006)

		malicious code with political causes	High-Tech Crime Unit, etc.)
2005	Zotob	Worm aimed at media organizations	Hit CNN live on air and stopped the show
2006	Karma Sutra, also known as Nyxem	Transmitted by email promising racy pictures (i.e. 'Miss Lebanon 2006'); deletes all Word, Excel, PowerPoint, and PDF files on PC; hijacks users' email address book and sends replicas of itself to the contacts listed	Primitive, i.e. meant to destroy files rather than seek financial gain or take control of a computer; didn't happen on corporate networks but home users could still be vulnerable

### *Cyber Crime*

Besides the lure of illicit financial gain, what are some of the factors driving the surge in viruses? The Internet, by interconnecting the world, has facilitated virus propagation and increased risk and interdependence. As more people get high-speed broadband Internet connections, they tend to spend more time and money online. An 'always on' PC heightens the risk that malware may invade. And there are a lot of naïve users out there. Free Webmail services like Yahoo! mail and Hotmail were prone to infection until the virus filtering which takes place at the Webmail server-end was improved. People click on links embedded in seemingly reputable email messages and are whisked to sites infested with viruses. Websites that offer pornography, gambling, or free MP3s are more likely to install malware on computers that visit.

Who are these cyber muggers? Once a form of 'electronic vandalism' (i.e. 'cyber graffiti') malware has become a profit-making venture ('crimeware'), from amateurs causing mischief to professional hackers, many working for organized crime. As a result, the 'threat landscape' has changed, from global outbreaks ('pandemics') to smaller, stealthier attacks. It is more about data gathering (or *phishing* for data) using keylogger and spyware programs in surreptitious ways, about an 'underground economy that is trading fraudulent credit card information and extorting money from Web sites'. Online groups and communities, file servers, Web servers, Internet relay chat, email, Instant Messaging, multiplayer games, collaboration tools (like blogging), peer to peer, networks (even networked printers and copiers have enough processing power and storage to launch an attack), Websites, desktop software, database programs, media players, ATM machines, medical devices, wireless devices, and even anti-virus software are all targets. Complicating matters, the threat is not just external but also internal, coming from employees who steal customer databases, pricing lists, discount lists, blueprints, strategy documents, designs, and money.<sup>3</sup>

Interestingly, some believe that Hong Kong has been spared the spread of identity thefts because the use of smart ID cards, that carry encrypted personal information in an embedded chip, makes it harder for identity thieves to pose as their victims. However there are those who believe 'that it may only be a matter of time before hackers catch up with the technology. "Before too long, identity fraud will be too tempting for local smart card hackers not to target."' (SCMP, 17 July 2005). Table 2 below lays out the new threat landscape in greater detail.

<sup>3</sup> Either to sell them to a competitor or use them to start their own business. 'As software and networks become more secure, IBM analysts said many criminals may target the most vulnerable access point within an organization: Its employees. This means insider attacks could surge. The frightening thing about this is that no amount of anti-virus, firewall or anti-spyware software can guard against internal hackers. Instead, sophisticated software that spots unusual network behaviour is required, coupled with increased vigilance on the part of company employees, particularly IT managers and administrators. Content monitoring systems can also be employed that check what employees are sending and receiving in emails and other communications.' ('Security', *Warren's Washington Internet Daily*, 24 January 2006)

Table 2: A Hostile Environment

Name	Description	Effect/Example
<b>Undesirables</b>		
Adware	Festoons screen with endless stream of pop-up ads, slowing down computer to crawl; involves agreements between 3 <sup>rd</sup> -party advertising networks, sometimes spanning 1000s of partners	Advertising is often associated with free applications, but can also raise ethical issues. Decline in online gambling ads after the FBI threatened arrests for sites carrying those ads.
SMTP session hijacking	Gain access to a list of email addresses and send unsolicited junk email to thousands of users	Spam
Spyware	General term for software that does advertising, collecting info, or changing the configuration of your computer – all without obtaining your express consent	Keystroke loggers; password traps; becoming more stealthy
Caller ID Spoofing	Technology that enables callers to disguise their true name and number with false ones.	Marketed to private investigators and debt collectors
False Domains	Estimated 2.31 million Internet domain names, or 5.14% of total, registered with 'patently false' data (US Government Accountability Office)	To avoid detection by the police
<b>Unacceptables</b>		
Botnet (robot network) by Remote login	Network of compromised or zombie computers (bots) that, unknown to their owners, are under the control of hackers (bot masters) and up for hire to perform nefarious tasks	Able to view or access your files to actually running programs on your computer and enables a robot network to use your computer to launch Denial of Service (DoS); cyberextortion
Carder Web sites	Web site built to sell just that one 'hot' item, 'Give us your credit card number and we'll sell you the goods'; take credit card numbers and expiration dates and sell them	Sell cards in 5-10,000 number bundles at \$1-2 a piece, a lucrative business
Children and inappropriate content and contact with strangers (pornography, sexual predators) <sup>4</sup>	Few parents use parental controls and tools to shield children	MySpace; 'whitehouse.com'; ICANN and '.xxx' concept; Utah and Michigan passed laws in 2005 for registries for parents to declare children's contact points, such as emails and cell phone numbers, off limits to receiving content or links to content that is illegal for minors to view or buy
Cyberextortion schemes	Companies heavily reliant on the Internet, such as online gambling firms (can't take bets if their service is interrupted), targeted by criminals inflicting so-called distributed denial of service (DDOS) attacks (see Botnet entry)	Moving on to electronic retailers, online payment services, and the financial industries, 'anyone for whom time offline costs money'; quite a few companies pay <sup>5</sup>
Denial of Service (DoS) attack	Bring computer networks to grinding halt by flooding them with traffic	Used as threat in a number of business extortion attempts
Identity Theft <sup>6</sup>	Hack into someone's PC to obtain banking and other personal information (like name, Social Security number, and birthdate) to assume someone else's identity and take their money or run up credit	The fastest-growing crime in America; affects 10 million Americans (FTC) <sup>7</sup> ; cost UK economy 1.3 billion pounds in 2004 (BBC); Americans have had medical records stolen and then been targeted by spam emails for new drugs
Low tech hacking and con artistry  Human error	About 30 per cent of employees will unwittingly give up their company passwords to someone they think is 'official'; the often neglected 'human side of security' (i.e. human ignorance and laziness)	Use phone and fool someone into giving you the info, much easier than cracking into a computer system
Keystroke loggers	'Drive-by downloads'; planted on desktops from infected Web sites; copies user keystrokes, even snapshots of a user's screen; can steal passwords	Over 6,000 different keylogger variants, 65% increase over 2004; sold commercially as tool for keeping eye on what children are doing

<sup>4</sup> The number of pornography-related Internet sites increased from 14 million to 260 million between 1998 and 2003.

<sup>5</sup> 'Demands are "typically between US Dollars 8,000 and Dollars 10,000 to stop the attack and allow the website to operate for 12 months". In fact, ransom demands have typically gone down with time, simply because companies are far more likely to pay smaller amounts.' ('The whiz-kids and wiseguys of cyber crime', *Financial Times*, 9 December 2005)

<sup>6</sup> It is still worthy to note that 'the most frequently reported source of information used in fraud was from a lost or stolen wallet or checkbook... "Internet fraud is a sexy thing, but dumpster diving also happens."' ('Banks stress vigilance as online fraud scams increase', *Alaska Journal of Commerce*, 15 January 2006)

<sup>7</sup> Roughly 4.6% of the US adult population. Victims spend an average of US\$500 and 30 hours to clear their records.

	and other account information	online
Phishing/Spear Phishing <sup>8</sup>	Relies on tricking or scaring consumer into revealing credit card or bank account details or pin numbers on an official-looking but phony Webpage by sending emails from what looks like a legitimate business or reputable financial institution or even from inside your company (from the IT or HR department)	Top 10 organizations that culprits pretended to be in such ruses were eBay and its PayPal unit, Bank First, Amazon.com, Chase Bank, Wells Fargo, Bank of Oklahoma, Barclays Bank, Bank of America and People's Bank (CipherTrust); 13,562 different kinds of phishing ruses in Sept. 2005 (Anti-Phishing Working Group)
Puddle Phishing	Moving downstream and targeting customers of smaller regional banks and credit unions	Because crooks are targeting smaller group, their pitches can seem more credible; hotels and frequent flier programs
SPIT (Spam over Internet Telephony)  A new variety of hack attack?	Voice-based spam, automatic disconnects, being flooded by phantom calls that cause incessant ringing; call hijacking in which electronic sniffers are employed to determine unique IP phone details in attempts to intercept, listen in on, or record calls <sup>9</sup>	Does CALEA (Communications Assistance for Law Enforcement Act, 1994) allow for VoIP calls to be wiretapped? Could VoIP applications such as eBay's Skype and Vonage give cyber criminals a better way of controlling their zombies and covering their tracks?
Spoofing	When email addresses and page content appear to be from a valid source	To get users to bite to phishing schemes
SQL Injection	Hackers attach increasingly complex suffixes to search terms to target retail website search facilities and databases	Inadequately protected database may reveal confidential customer and purchase information
Zombie	Computers that are remotely hijacked to send spam to millions of email addresses; spammers abusing poorly configured email servers	Around 250,000 new zombies send mail every day (CipherTrust)
<b>Environment</b>		
Failed or insufficient data backup systems	IT systems often lack a remote backup service that automatically backs-up files on a nightly or more frequent basis	Offsite System Redundancy
Growth in outsourcing	More and more business transactions and associations involve third-party technology firms (like outsourced call centers) that have little interest in protecting personal privacy	Call center workers making cash selling customer bank details
Home networking	Networked media devices at home, such as Windows Media Player, RealPlayer, Xbox, PS2, iTunes online; even printer and copier processors can be used to launch attacks.	More vulnerability to be exploited; iPodPorn; an additional reason to be wary of file sharing?
Mac or Linux is safer?	Security by obscurity	But not entirely. In 2006 Leap-A is a virus that spreads through iChat software inside the Mac OS X operating system
Removable and easily-hidden media	USB drives; MP3 players	Enable staff to download sensitive and potentially damaging corporate data
Rootkits or 'click-and-hack' programmes	Rootkits automate the process of infiltration: a set of modified and recompiled Unix tools designed to hide any trace of the intruder and may include programs to monitor traffic, create a back door into the system, alter log files and attack other machines on the network	Wannabe hackers can choose from tens of thousands of hacker-oriented websites for guidance
Unreported Incidents & Complacency & IT Spending Levels	Some 40% of the world's large companies had their IT infrastructure compromised by computer viruses and worms during the first six months of 2004 (Symantec); estimate that just 10-15% of incidents are reported because it makes for bad press	Studies show that a typical company spends barely 5% of its IT budget on security, depending on the nature of the business, the appropriate figure should be up to three times as much (EIU, 19 December 2005)
Vulnerable sectors – some	Largest volume of data breach incidents	HK school system hacked up to 15,000 times a

<sup>8</sup> According to a research report issued in June by Gartner Inc. about 2.4 million Americans reported losing about US\$929 million to phishing schemes during 2004.' ('For a New Breed of Hackers, This Time It's Personal', *New York Times*, 4 December 2005)

<sup>9</sup> VoIP messages are communicated using Real-Time Protocol and the new encryption standard being developed is called Secure-RTP. There are some concerns about the first stage of the signaling process, which uses Session Initiation Protocol (SIP) to set up, ring and terminate calls between 'call' or 'signaling' servers. Hackers are already developing ways to attack SIP, allowing them to redirect phone calls to devices they control or to launch denial of service assaults like call flooding. (One solution, SIP firewalls.) ('Voice Over IP: How to Handle the Hazards', *Financial IT Security*, March 1, 2006)

more prone than others	occurred in the education sector	day (SCMP 12 January 2006)
Wireless/WiFi/Bluetooth <sup>10</sup>	Easy to collect packets of data sent across unsecured wireless networks by using publicly available decryption keys; original encryption standard, Wired Equivalent Privacy (WEP), can be broken easily; PDAs and smartphones create new back doors into corporate networks; mobile phone tracking technology	Allows piggybacking: usually unauthorized tapping into someone else's wireless Internet connection; Many airports partition public traffic from the airport's operational LAN and keep that traffic outside the airport's firewall. New IEEE 802.11i standards support up-to-date authentication and encryption

## Part 2: Spam

The Hong Kong ISP Association recently reported that the amount of spam in Hong Kong has risen to more than 30 million emails a day, and warned that spam could account for 90 per cent of all Hong Kong email by the middle of 2006. The Hong Kong Anti-Spam Coalition came out with an estimate that the cost of screening and cleaning Hong Kong electronic mailboxes is HK\$300 per employee per month, or HK\$6 billion a year in lost productivity. Considering the level of vexation and grief spam causes to Hong Kong Internet users, it deserves its own special mention.<sup>11</sup>

The first thing to note is that there are divergent views on whether spam is a growing or diminishing menace. For example, contrast the entries for Pew and Jupiter with the others in Table 3.

Table 3: What's in Your Mailbox?

Date	Survey	Results
2004	National Technology Readiness Survey	Workers spent 2.8 minutes per day deleting spam, at a total cost to US businesses of \$21.58 billion annually in lost productivity
2004	Symantec	Spam increased from 800 million a week to more than 1.2 billion
2005	Outblaze	Calculated a ratio of more than 14 spam messages to each genuine message when the company took a snapshot of more than 1.4 million messages received during a single minute
2005	Pew Internet Project	Found an increasing tolerance for spam among online users, but 52 per cent of Internet users still considered spam 'a big problem'
2005	Jupiter Research	Found that 31 per cent of email in consumer in-boxes was spam, down from 44 per cent two years
2005	Radicati	In 2005, spam traffic totaled 91 billion messages per day, by 2009, spam is expected to reach 228 billion messages per day
2006	Ferris Research	One Day's Emails... Legitimate Emails: 2.5 billion sent to consumers, 7.5 billion sent to corporate users; Spam Emails: 15 billion messages sent

Even voices of authority don't quite agree. In 2004 the end of spam was in sight: 'Two years from now, spam will be solved.' (Bill Gates, January 2004, World Economic Forum, Davos, Switzerland). Two years later ... 'I won't say spam is dead, but we can say spam is contained. If you use the latest anti-spam technologies and educate yourself on how to use them, you should not have a problem.' (Ryan Hamlin, GM for

<sup>10</sup> 'A survey conducted annually by the Hong Kong Wireless Technology Industry Association and published in April 2005 found that of the 1,723 wireless access points found along the tram route from Kennedy Town to Shau Kei Wan, 61 per cent had their encryption disabled, while 46 per cent used an insecure service set identifier, essentially allowing any passer-by to log on to the network to browse the internet, receive emails or worse.' ('Wi-fi wide open to wardriver attacks', *SCMP*, August 9, 2005)

<sup>11</sup> For the history buffs, it is generally agreed the very first spam message was sent by a marketing representative of the DEC computer company on May 3, 1978, over the Arpanet, a computer network that preceded the Internet. The message, urging Arpanet users on the West Coast of the United States to attend a DEC product presentation, prompted a predictably angry response, with one user even hinting at legal action or sanctions. ('Spam's noir side invades the Net', *International Herald Tribune*, Jan. 25, 2006)

Technology, Care and Safety, Head of Anti-Spam for Microsoft, *International Herald Tribune*, 25 January 2006).

At first glance there is a lot of spam, or junk email, out there, regardless of what survey you read. AOL reckons its spam filters block 1.5 billion emails a day while 300 million get through, many of them scams - see Table 4. There are even spam blogs or 'splogs'.<sup>12</sup> Cellphone spam is becoming a concern as well, especially when overseas spam incurs expensive roaming charges. And of course, many legitimate emails, including legitimate mass mailings such as newsletters, are caught in spam filters and not delivered.

Table 4: AOL's 2005 Top 10 Global Spam Subject Lines

1. Donald Trump Wants You - Please Respond	Popular recognition
2. Double Standards New Product - Penis Patch	Sexually oriented spam
3. Body Wrap: Lose 6-20 inches in one hour	Body improvement products
4. Get an Apple iPod Nano, PS3 or Xbox 360 for Free	Technology offers
5. It's Lisa, I must have sent you to the wrong site	'Personalized' correspondence
6. Breaking Stock News***Small Cap Issue Poised to Triple	'Pump-and-dump' stock scams
7. Thank you for your business. Shipment notification (77FD87)	Bogus transactional spam
8. (IMPORTANT) Your Mortgage Application is Ready	Mortgage-related scams
9. Thank you: Your \$199 Rolex Special Included	High-end 'deals'
10. Online Prescriptions Made Easy	Cheap pharmaceuticals

Spam imposes costs on all Internet users.<sup>13</sup> Spam uses scarce resources of users and service providers without compensation or approval. Spam consumes network and computing resources, email administrator and helpdesk personnel time, and reduces worker productivity. In the aftermath of Hurricane Katrina, thousands of fraudulent emails went out from people posing as collectors for the American Red Cross.

### *Blocking Spam*

What can be done, besides immediately deleting any spam email received? There are technological and legislative remedies, with varying degrees of effectiveness. One can decrease spam through the use of better filtering devices. Filters use various types of content analysis techniques to uncover suspicious characteristics, words, or phrases within an inbound email that spammers try to hide.

<sup>12</sup> While 80,000 blogs may be created every day, about one in five is spam. Google's blog-creation tool Blogger has an open API (applications protocol interface) which has made it easier for computer programs to create splogs. During one weekend in October 2005, some unknown persons used Blogger to generate more than 13,000 fake blogs. Because search engines base their rankings in part on how many other sites link to a particular site, splogs can propel the sites to which they are linked to the top of search-engine results. ('Splogs', *New York Times*, 11 December 2005) This is an example of 'link spam'.

<sup>13</sup> 'In a vain attempt to filter the "four letter word" on the Internet, local internet service providers [in Hong Kong] spend HK\$80 million annually - with consumers ultimately footing the bill.' ('Legislation to restrict unwelcome spam is expected next year, but legitimate e-marketers are wary of becoming accidental victims', *SCMP*, August 20, 2005)

Table 5: Filtering Techniques

Keyword analysis	Scrutinizes for specific words and phrases within the text of an email message.
Lexical analysis	Examines the context of words and phrases and suspicious words or phrases are assigned 'weights,' depending on the context in which they are found.
Bayesian analysis	Uses knowledge of previous events as a predictive tool by examining email known to be legitimate, in addition to known spam, and comparing the content to develop a database of words may help identify future spam.
Heuristic analysis	Scrutinizes message's spamlike characteristics, with each getting a probability score. If a probability threshold is reached, the message is deemed to be spam.
Header analysis	Examines message headers to determine the sender's validity. URL analysis compares embedded links in email messages to a list of URL rules or known spam addresses.

Source: 'Open your eyes to anti-spam options', *Newsbytes News Network*, 8<sup>th</sup> December 2005

However, used alone, content analysis can generate many false positives (i.e. identifying valid emails as spam). Reputation-based filters allow for a broad range of responses, including blocking, rate-limiting, or quarantining messages for further review, without having to do intensive content analysis. Large email providers such as AOL and Yahoo!, who together represent more than half of the email addresses on many US consumer email lists, have worked with legitimate marketers by employing a whitelist that enables email sent from pre-identified addresses to arrive unhindered at no additional cost. A blacklist would contain IP addresses of known spammers and those PCs and mail servers would be blocked, although spammers move on quickly and preventive measures are often too late. An ISP could close holes in their end-user broadband systems and block certain numbered ports through which a server machine makes its services available to the Internet but a few networks, out of greed or mismanagement, do not.<sup>14</sup> Other anti-spam techniques include sender authentication, challenge and response, and reverse Domain Name System lookups.<sup>15</sup> Honey pots are decoy email mailboxes that act as spam traps.<sup>16</sup> Smaller enterprises can purchase server-based anti-spam appliances that feature a hardened, secure hardware and software combination.

Other remedies, mostly non-technological ones, have seen concerns raised over their merits. AOL and Yahoo! are planning to start a 'stamp' scheme – 'certified email' – to charge companies for sending legitimate bulk email – US\$2.50 per thousand emails but the price could go up or down depending on the market. The plan is seen by some critics as an excuse for AOL and Yahoo! not to put the extra effort in improving active filtering. They also see it as the thin end of a wedge to introduce a two-tier Internet, one for the rich and one for the rest. Qwest had a terms-of-service policy for its high-speed Internet subscribers which included a provision that would allow Qwest to charge them

<sup>14</sup> 'The real problem is that Internet Service Providers can make money by allowing spam through "SMTP port 25" [ see [http://www.postcastserver.com/help/Port\\_25\\_Blocking.aspx](http://www.postcastserver.com/help/Port_25_Blocking.aspx) ] a port routed through Hong Kong that allows anonymous users to send spam through an ISP while only having to list their IP address, a general category that makes it impossible to locate the culprit.' ('Spam blacklist unworkable', *The Standard*, April 29, 2005) A coalition of some 40 Japanese service providers, including IJ, has mooted port 25 blocking as an effective spam countermeasure. Several Japanese residential ISPs are blocking outbound data on port 25, which is used to send mail from a server. ('Japan leads the way in spam relay prevention', *VNUNet United Kingdom*, Feb. 10, 2006)

<sup>15</sup> Microsoft advocates a technology known as Sender ID, which checks a registered list to determine whether a message came from the same domain as the email address indicates. Yahoo! and Cisco lead a group that advocates a cryptographic method of email authentication, DomainKeys, to address the problem, known as domain spoofing.

<sup>16</sup> Microsoft has gathered evidence by collecting spam in special trap email accounts to file more than 100 lawsuits against alleged spammers and reached settlements worth about US\$10 million. ('Is Gates' Prediction on Spam A Bust?', *Seattle Post-Intelligencer*, Jan. 23, 2006)

US\$5 for every spam email sent through their computers whether they knew about it or not.

### *Anti-Spam Legislation*

But the remedy whose success has been most debated has been the use of legislation in curbing the spam problem. There are two issues currently being debated in Hong Kong. The first is how to control spam phone calls, especially as they affect mobile cellular phone users who have to pay high roaming charges when they receive these nuisance calls when traveling outside Hong Kong. The second is email spam. Hong Kong's Unsolicited Electronic Messages Bill addresses both issues. In regard to spam phone calls Hong Kong is planning to follow the example of the USA. In 2003 the Federal Trade Commission introduced the opt-out National Do Not Call Registry in accordance with the Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994. According to *Primedia Insight*, 17 January 2006, by 2006, 76 per cent of all US adults say that they have signed up for the do-not-call list, a significant increase from 57 per cent in January 2004 and 32 per cent in September 2003. But unlike the US approach in which very substantial fines for abuse are enshrined in law, the Hong Kong approach, which covers spam via fax, email, SMS, MMS, and recorded phone messages by interactive voice response systems (IVRS), proposes to leave the implementation to the telecommunications regulator, OFTA.<sup>17</sup> Freedom of speech and expression would be protected as non-commercial organizations would not be affected by the bill's provisions. Fines would range from HK\$100,000 for spammers to HK\$1 million and five-year prison sentences for the offenses of address harvesting and automatic throwaway accounts. Some critics have called the bill anti-business.

To combat email spam the US CAN SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing) went into effect February 2004. CAN SPAM requires senders to follow certain rules, such as not disguising their identities and giving recipients the opportunity to opt out of future messages, but it did not ban unsolicited commercial email. However, the law does allow federal and state authorities, as well as Internet providers, to go after anyone breaking the rules.<sup>18</sup> CAN SPAM critics said it superseded stronger state laws, made it impossible for individual lawsuits, and provided inadequate penalties ('lacking teeth') when applied in the court of law. In addition, CAN SPAM needs to be updated to meet new spam challenges, such as spam sent by botnets. But, most importantly, it never addressed spam sent from abroad or the issue of going after renegade email marketers who move overseas.<sup>19</sup> The FTC lobbied Congress to enact the 2005 US SAFE WEB bill (Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers Beyond Borders) which allows the FTC to pass intelligence on suspected spammers to foreign intelligence agencies.

Other countries have stronger anti-spam legislation than the US. Japan<sup>20</sup> has adopted an 'opt in' approach, meaning that companies need explicit permission to send an unsolicited commercial message to consumers who, in turn, receive only the marketing

<sup>17</sup> See 'Do-not-call plan needs sharper teeth to make an impression' Yvonne Chia, *SCMP Technology Post*, 28 February 2006.

<sup>18</sup> The Federal Trade Commission (FTC) has taken 20 separate actions against spammers. AOL and Yahoo! have filed 27 other suits. (*Dow Jones*, 5 January 2006)

<sup>19</sup> The US (24.5%) and China (22.3%) led Sophos's list of spam-relaying countries Q4 2005, with South Korea (9.7%) – previously number 2 – France (5%) and Canada (3%) rounding out the top 5. (PR Brief, January 2006).

<sup>20</sup> Japan has more than 11 per cent of the world's broadband connections but only 2 per cent of global spam. The US has 21 per cent of the world's broadband lines, and accounts for 24 per cent of the spam relayed worldwide. ('Japan leads the way in spam relay prevention', *VNUNet United Kingdom*, Feb. 10, 2006)

messages they have requested. Some European countries have done the same. In the UK, individuals have the right to sue.<sup>21</sup> Australia has made all spam illegal, with the exception of messages sent out by charities, political parties, and the government. The penalty for not complying can be as high as A\$1.1 million a day. New Zealand has passed an anti-spam law to prevent it from becoming a safe haven for spammers.<sup>22</sup> China has experienced a problem with SMS spam and will require users of prepaid cellphone accounts to register using their real names in 2006.<sup>23</sup> China plans to release anti-spam rules by March 2006 that will require email providers to register the IP address of their mail servers and email advertisements sent in China to include 'AD' in the subject header to identify them as ads. But prosecuting spammers will require closer international collaboration.<sup>24</sup>

### Part 3: Protecting Enterprises and Consumers

Highly publicized security breaches are leading to increased awareness and investment in IT security. So have new corporate governance rules and compliance obligations such as the 2002 Sarbanes-Oxley Act.<sup>25</sup> So have state laws in America that require companies to notify customers when their personal data has been compromised. But moves to strengthen laws have also led to a lively public debate over the trade-offs and the right balance to strike between security and ease of use, between trust and an 'emerging Web of consumer surveillance', between ensuring that personal freedoms and privacy are protected and the government's ability to use pertinent information to protect against dangers facing the country.<sup>26</sup>

While common sense dictates that consumers and businesses alike take IT security seriously, it often fails more than prevails. Security involves relying on multiple 'barriers'. Ideally, vendor-supplied defaults for system passwords should not be used. Sensitive information should be encrypted. Anti-virus software should be routinely updated. Virus and email and vulnerability scans should be regularly scheduled. Strong passwords should be required.<sup>27</sup> Data access should be restricted to a 'business need-to-

---

<sup>21</sup> But the Information Commissioner's Office (ICO) in the UK has admitted it made no prosecutions against spammers in 2005, even though it received 364 complaints. (*Computing*, 9 February 2006)

<sup>22</sup> This is important because 'many email administrators are already blocking countries indiscriminately in their own anti-spam efforts. I have seen a message advocating blocking of e-mail from Hong Kong because it is "another spammy Asian country"'. ('Will anti-spam laws curb the problem?', *SCMP*, March 1, 2005)

<sup>23</sup> Out of the 200 million pre-paid subscribers, 30 per cent had registered their phones with false personal information – the 'faceless' problem. China's phone companies shut down more than 10,000 accounts in 2005 for sending illegal messages with fraudulent, harassing or erotic text.

<sup>24</sup> In April 2005 the Seoul-Melbourne Multilateral Memorandum of Understanding on Co-operation in Countering Spam was signed to encourage closer cooperation among the signatories in minimizing spam originating in or passing through the Asian region to end users. The signatories will also promote the exchange of information on technical, educational and policy solutions to the problem under the framework. ('HK joins international community against spam', *Xinhua News Agency*, April 27, 2005)

<sup>25</sup> The law was drawn up in the wake of the Enron and MCI Worldcom scandals to protect investors by ensuring the integrity of financial reporting and forcing corporate officials to take full responsibility for public disclosures required under the law. Hong Kong and mainland firms are affected insofar as they must conform to the strict transparency requirements with which their US business partners or clients are subject to. But Sarbanes-Oxley is not very specific about which documents need to be saved and for how long.

<sup>26</sup> The privacy debate has been fueled incidents like the September 2005 arrest of Chinese journalist Shi Tao after Yahoo! gave his personal email account to Beijing; by the warrantless electronic wiretaps and surveillance conducted by the National Security Agency (NSA); by Google's refusal to provide the Justice Department with information in the US government's fight against a Supreme Court ruling that struck down the Child Online Protection Act; etc.

<sup>27</sup> One expert recommends 'a minimum of seven characters with at least one uppercase letter, one lowercase letter, and a digit and/or symbol'. ('Safety in numbers', *Information Today*, Feb. 1, 2006). Numerous vendors are selling the latest generation of laptop computers with built-in fingerprint readers.

know' basis. Access to network resources should be tracked and monitored. Security systems should be tested. Limits should be set to the hyperlinks employees put in emails to customers. Employees should be educated not to download online games or unsolicited email attachments or use file sharing Web sites. Two-factor authentication should be used. Anti-spy ware programs should be installed and a firewall to protect the computer from online attackers. The latest security patches should be downloaded from the Microsoft and other websites which can be done in an automated fashion. Investment in an intrusion detection and protection system can lead to detection of abnormal activity and whether outsiders are looking at network structures, mission-critical machines (hosts: the computers on the network), and points of weak security. Where users have remote connections to the network, a network management system should be used to check that all devices connecting to the system comply with security protocols. Documents no longer needed should be shredded. The blocking of ports (such as those numbered 135, 139, and 445, both ingress and egress) that are used for communication between MS platforms on a LAN can prevent anyone outside the LAN from accessing these ports. Backing up and relocating data to a secure offsite location is a basic precaution for disaster recovery in the case of an emergency. Deploying filters is another protection - see Part 2 above. And so on.

In general, security by specialists is not viewed as a series of concentric circles or of layers building upon one another but, as with the Internet, as a string of islands linked by connecting streams. As one IT security consultant put it 'One island is the vendor, another island is you, another island is the customer, etc.' where the VPN 'streams' connecting them are encrypted. (Interview) Table 5 below illustrates some common technological and procedural solutions to IT security – to prevention, detection, and reaction. Those most likely to be helpful to consumers mostly fall under one of four headings: anti-virus, anti-spyware, encryption and firewalls.

Table 5: Protecting the Enterprise and the Consumer

Action	What?	Reaction
<i>Procedures</i>		
Risk and business impact assessment	Examination of business processes; establish clear chain of command; educate employees; decide what data and applications are important, what needs to be protected, levels of protection to apply	Only have finite resources; testing is essential; not about waiting for some technological silver bullet; role of Chief Information Security Officer (CISO) morphing into operational risk management
Company policies: written email and Internet acceptable usage policy (AUP)  See Cyberslacker entry in Issues	Set out quotas for personal email and how much time in working day can be used for personal Web browsing; make clear what is unacceptable surfing; define whether employees have access to instant messaging and hotmail-type accounts	Can be enforced by software which tracks Web/email content such as Surfcontrol and Websense <sup>28</sup>
Non-disclosure agreements and background checks when hiring for sensitive positions such as the people who manage a company's computer systems	2004 survey of 23 incidents of insider misuse of computer systems determined that a quarter of the insiders involved had a criminal record	Emphasize that employees are in a privileged position and that it's their responsibility to protect the sensitive information they work with
<i>Network-based security (i.e. for airport terminals, for switches, hubs, routers, and wires)</i>		
Network Admission Control (NAC) (Cisco)	Set of technologies built into network infrastructure which enforces policy compliance on all devices connecting to the network	Cost issue: requires upgrading switches and routers and deploying software agent on each asset to monitor data, difficult to do in a heterogeneous environment
Secure LAN Controller (ConSentry Networks)	Uses algorithms rather than signatures to detect network anomalies; when detects	No need to install agent on host; modeling behavior, looks at suspicious

<sup>28</sup> A Harris Interactive survey found that, while nearly 75 per cent of users are aware of corporate email policies, only 46 per cent claim to always comply. ('Don't Overlook Internal E-Mail Monitoring', *CMP TechWeb*, Dec. 12, 2005)

	infected device just blocks parts of machine virus is infecting, doesn't completely lock out user	network activity and quarantines it before it hits critical servers; unlike signatures which can only be developed once malware is out in the wild
Deep packet inspection tools	Examine each data packet to block harmful transmissions	Block known virus threats or blacklisted IP addresses known to be used by hackers
Belated introduction of IPv6	Includes check on every single packet sent so that packet's receiver will know its origin and that it wasn't tampered with on the way	Such precision to make life harder for online criminals as scams become more visible and reveal spam's origin, making it easier to track offenders
Self-immunizing networks (Tel Aviv University researchers)	Honeypot scheme that uses a shadow network to transmit immunizing messages	In simulated 200,000 computer network with one honeypot for every 250 computers, virus would infect less than 1 per cent of computers
<b>Perimeter: Gateway to the Network from External World</b>		
Anti-virus software Anti-spyware software	Better anti-spyware solutions use signatures and behavioral tags to identify and block the ability of spyware to install files, they can also recognize the protocols typically used by each spyware program to communicate with an outside computer to transmit collected information or update its own code, and block these transmissions	The software needs updating, but online updating only updates the original software package which may have been superceded by a later version. This is a source of false security.
Encryption	Secure socket layer (SSL) employs constantly changing public key to encrypt data and a private key to decrypt it	US law allows for a highest level of 128-bit algorithm (AOL's Banking Center); unencrypted access in Google's Gmail not an option, forced to use SSL all the time
Firewalls	Suite of software to act as barrier between network and Internet to prevent unauthorized access and keep system safe from malware; fends off direct probes	Electronic gates; BUT most firewalls don't inspect outbound data traffic (like keylogger files)
Virtual Private Network (VPN) tunnel	Done through private or partitioned pipes	SSL VPN for all remote access, enables one to have a single point of control and filtering for all Internet-based applications
Trust Zones	Combination of firewalls and Virtual LAN data pipes distinct from overall corporate network	Create multiple layers so it would be difficult for attacker to penetrate protected assets without being noticed
VoIP call pattern analysis tools	Data is cross-matched against phones, corporate call server, and 'gateways' that bridge VoIP to conventional telco infrastructure	Detect and flag unauthorized 'domains' or call servers that may be attempting to intercept or redirect a company's calls
Filters	Incoming messages pass through 'an assembly line of detection methods, from hash-based spam signatures to rules-based heuristics to Bayesian statistical computation' <i>IT Architect</i> , February 2006	Help ensure high catch rates and low false positives but can eat up computing resources; SpamAssassin, popular open source spam detection software
Internal employee monitoring and email content controls	From network, database, and application access control, tracking and auditing to individual keystroke capture, and video surveillance; archiving messages in event of investigation	To protect security of corporate intellectual property and assets and for performance and productivity purposes; to prevent potential compliance violations; to prevent distribution of offensive content (pornographic material, sexual or racial harassment, etc.); to protect against major corporate liability issues
Biometrics	That is, use fingerprint reader to verify identity	October 2005 Australia introduced biometric e-passports, which make use of 3D facial recognition technology
<b>Online and Offline</b>		
Two-factor online authentication	Requires users to input one password or PIN they create for themselves and one they are assigned randomly through a token device	To better protect online banking customers; June 2005 HKMA required all banks in Hong Kong to use two-factor authentication in order to guard third-party transfers from online snoopers
Token technology	Extremely portable, easy to use, size of car alarm remote	A physical representation of digital security; used by online financial services, health-care providers, automotive dealers, online gamers, and educators to prevent theft of exams
Cyberinsurance	First-party coverage helps companies recover losses owing to network outage,	Written premiums topped US\$200m in 2005, up from US\$100m in 2003 (Aon

	also includes payments to hackers holding your Web site or customer data hostage; third-party liability covers legal expenses if security fails and someone sues	Financial Services Group)
Fraud coverage for online brokerage, banking, and lending customers	For example, E*Trade offers 100% fraud coverage for its retail customers.	Projected the potential financial exposure the company could face may be as much as US\$5 million <i>this year</i> and as high as US\$10 million in 2007
Outsourcing network security 'Security in the Cloud'	Difficult to keep up with monitoring intrusions, have to hire someone 24 hours a day; concern over handing network security to a third party	Turn client into a 'black hole' on the Internet where no one can see them and anything directed to the client goes through the 3 <sup>rd</sup> party security firm
Thin Clients or Fat Clients (PCs)?	Applications and data stored on server, network administrator needs to secure just the server, not every (brain-dead) workstation; 'just as many passwords to reset, broken keyboards and flaky mice to fix, and lost files to restore from tape'	But people like their PCs (fat clients) which let them pick their own software, flexible, innovation-oriented
Police Cybercrime Unit	Jan. 2006 Jenson James Ancheta of California pleads guilty to violating Computer Fraud and Abuse Act <sup>29</sup>	Who would you report an electronic crime to in the Hong Kong police?

#### Part 4: Welcome to the Protection Racket

Computer security has become a big business. The February 2006 RSA conference, an industry show, had more than 275 companies exhibiting their security wares and more than 14,000 attendees. Third-party vendors like Symantec, McAfee, Trend Micro, Panda, and ZoneLabs have prospered by developing software, such as Symantec's Norton Utilities (now called Norton Internet Security) and McAfee's anti-virus (AV) and system security products, to protect computers against attacks on Windows vulnerabilities. They have become trusted brand names in a worldwide consumer anti-virus market that reached US\$1.18 billion in 2004 (Gartner) and looks set to keep growing.<sup>30</sup>

The traditional business model has been to sell different stand-alone applications (one for anti-virus, one for firewall, one for anti-spyware, one for anti-spam, etc.)<sup>31</sup>, with users installing the software on their computers and periodically (now almost on a daily basis) downloading the latest updates called 'signatures' that 'fingerprint' a new virus and block it.<sup>32</sup> One analyst borrowed from Gillette's famous business model to describe this approach as 'we'll sell you the razor and then you'll buy the blades'. The drawback is that customers get upset when they realize they have to pay an additional sum of money (or renewal fee) for anti-virus signature updates. For businesses, they pay a multi-year license fee depending on the number of PCs they want to protect and the number of services ('elements'), including maintenance, for which they want to apply.

Vendors are moving towards deeper integration, bundling into security suites the tools that catch viruses and spyware, block spam and pop-up ads and prevent identity theft.<sup>33</sup>

<sup>29</sup> 'A Web site Ancheta maintained included a schedule of prices he charged people who wanted to rent out the machines, along with guidelines on how many bots were required to bring down a particular type of Web site.' ('Botnet Hacker Enters Guilty Plea', *Monterey County Herald*, Jan. 24, 2006)

<sup>30</sup> Microsoft estimates that 70 per cent of PC-owning consumers do not protect their computers with anti-virus software, or have let older software subscriptions lapse, while Symantec thinks the range is 30-40 per cent. According to the Yankee Group, that translates into a potential US\$15 billion market.

<sup>31</sup> Clunky boxes of packaged software sold in a store that sometimes do not work together very well and frequently bog down PCs with higher-than-normal CPU consumption. An additional worry is hackers exposing and selling vulnerabilities in security software, thereby threatening the premium brand names in the market.

<sup>32</sup> 'People think of security as a noun, something you go buy. In reality, it's an abstract concept like happiness.' ('Is It the End of the Security World as We Know It?' Dennis Fisher, *eWeek*, 15 February 2006)

<sup>33</sup> Secude, a Swiss security solutions company, categorizes core products as encryption, identity and access.

The software is getting smarter so that less user intervention is required (automated updates) and threats are being found based on their behavior (using heuristics analysis), not just by searching for a piece of code that is known to be bad.<sup>34</sup> Enterprise security is expanding beyond desktop (the endpoint) and gateway (the network perimeter) protection to data leakage prevention in the form of storage management and database security. Finland's F-Secure is specializing in mobile security software, a market that will grow to US\$1 billion in 2008 (IDC estimate) as more people use smartphones to access their emails and the Internet. New distribution channels are opening up as well. McAfee has partnered with ISPs like AOL and Comcast in the US to offer free anti-virus software. When the consumer installs the free software (VirusScan), they are persuaded to buy incremental pieces of security technology, such as an upgraded firewall for US\$3.95 a month as a premium service offering. Vendors often work with OEMs to bundle their software with new PCs and laptops.<sup>35</sup>

#### *The New Trend: Online Protection*

But the new trend is simplification and selling security software as an online (Web) service, which lives wholly or partly on external servers, and which is offered by subscription, either on a monthly or yearly basis. Because it is an online service, technical support staff will be able to reach into a customer's computer, with the customer's permission, to fix problems. As part of a coming 'services wave' (software for rent) and to address a charge that security in Microsoft's Windows operating system is 'merely bolted on, not built in', Microsoft is unveiling OneCare, offering all-in-one security protection for an annual subscription rate of US\$49.95 (meant to cover up to 3 PCs).<sup>36</sup> Symantec is responding to the challenge with a similar service called Genesis to defend margins.<sup>37</sup>

Through a technology called InfoCard, Microsoft is also trying to tackle the issues of an 'overly complex system' (Bill Gates, Speech at RSA conference, February 2006) of passwords, of an online authentication and identity architecture, and of coming up with an Identity Metasystem that is platform-independent.<sup>38</sup> IBM has responded with the open source Higgins project targeted at corporate technology users. With OneCare and InfoCard, Microsoft hopes to come closer to realizing the pledges of the Trustworthy Computing campaign which it launched back in 2002, to inspire a level of trust in computing similar to the reliance users place on the electricity supply or telephone service.

---

<sup>34</sup> But due to the rapid software development cycle, mistakes sometimes go unchecked in the quality control process. In March 2006, McAfee issued a faulty virus definition update that incorrectly flagged hundreds of legitimate software programs as a virus outbreak.

<sup>35</sup> But many consumers do not update that software once their sixty or ninety-day free trial period ends.

<sup>36</sup> Interestingly enough, anti-trust considerations partly figured in the decision not to bundle anti-virus software with Windows.

<sup>37</sup> Instead of being purchased and installed, Genesis will be available over the Web as a service, so that it can be updated in real time as hackers expose potential threats. It will feature more user-friendly updates and support, offering real time instant-message chats with security experts. Genesis will protect not only PCs but the entire networked home, including DVR boxes, smart phones, and iPods. ('Symantec's New Target: Consumers', Sarah Lacy, *BusinessWeek Online*, 16 February 2006)

<sup>38</sup> To avoid what befell the Passport single sign-on service unveiled in 1999 where people's information was managed by Microsoft instead of by the users themselves and the businesses with which they dealt. This time Microsoft will not host an InfoCard database, instead letting the information reside with other companies on 'virtual cards'.