TACD

TRANS ATLANTIC CONSUMER DIALOGUE
DIALOGUE TRANSATLANTIQUE DES CONSOMMATEURS

DOC NO. INFOSOC-34-07 DATE ISSUED: FEBRUARY 2007

Resolution on Internet Security

Introduction
This resolution is part of a broader set of resolutions issued by TACD dealing with security in digital environments. TACD has already issued a resolution on spam[i] and has recently issued a resolution on ID Theft, Phishing and Consumer Confidence[ii]. This resolution discusses the problem of Internet security in general terms, and the recommendations in this resolution should be taken in conjunction with the other recommendations. The resolution on ID Theft, Phishing and Consumer Confidence and the resolution on spam deal with specific aspects of digital security.

The issue
The Internet has become part of our daily lives. Shops, banks, insurance companies and governments expect consumers to contact them online for services, advice, information, online payment and online banking. In the United States 69.3% of the population is connected to the Internet and in the EU 25, 51.9 %[iii]. The United States has the largest total number of broadband subscribers in the OECD at 57 million representing 31% of all broadband connections in the OECD. In short, the Internet has become an important medium for many in society today.

This has many advantages for consumers: efficiency, ease and more choice between different products and services than ever before. However, a major problem of the Internet is its lack of security. This can have severe consequences for consumers, such as damage to their computers and their contents, theft of their data for fraudulent purposes and intrusive marketing.

Many early network protocols that are now part of the Internet were not designed with security features. This makes the essential infrastructure of the Internet fundamentally insecure. This insecurity makes defence more difficult, especially for consumers, who are not professionally trained to deal with this problem. As a result, many digital products and services are not sufficiently safe. Examples include: websites, wireless modems, personal computers that are sold to consumers without any security features, payment systems that do not use a secure connection and online banking. For consumers who are confronted with this insecurity, it is very hard to keep protection properly up to date, because the Internet is a very dynamic environment. Because of the inherent openness of the Internet and the original design of the protocols, criminal attacks in general are relatively easy, quickly-executed, inexpensive, and difficult to detect or trace[iv]. A cyber criminal does not have to be actually present or online to carry out the attack, and the location of the attacker can be hidden.

The problem for consumers
A recent Consumer Reports survey on the damage caused by viruses and spyware showed that consumers in the United States paid as much as $7.8 billion over two years to repair or replace computers that got infected with viruses and spyware. Consumers are more vulnerable than they think. Consumers Union found that in six months time, spyware infections prompted nearly a million U.S. households to replace their computer. One in four consumers had a major, often costly problem caused by viruses[v]. This research suggests that people are paying large sums to cope with the flood of malicious viruses and other programs that can slow down computers or render them inoperable.

In the Netherlands, a country with a high broadband penetration grade (82% of the population has a broadband connection)[vi], a survey by the Dutch consumer organisation Consumentenbond shows that most consumers do not have adequate knowledge about the relevant threats on the Internet. For example, most consumers could not recognise the right definition of *phishing*[vii] (54%), *pharming* (70%)[viii], *sniffing* (71%)[ix] or *spoofing* (73%)[x]. Although 66% claim to be sufficiently informed about all these threats, the survey results show that they are not[xi]. So consumers really are more vulnerable then they think.

Furthermore, 62% of Dutch PC-users were confronted with problems like spam, spyware or viruses in the last year. Additionally, almost two-thirds of average users find it hard to install security software on their own. They know that there are threats on the Internet, but they do not have the expertise to defend themselves against these threats. In the United States, a survey conducted by AOL and the National Cyber Security Alliance confirms this observation[xii]. This survey was conducted through interviews and technical scans and shows again how vulnerable consumers are. The survey demonstrates among others that 69% of the respondents had known spyware on their computer, while a large majority of this group (92%) did not know that any spyware was installed. Of these respondents, 91% did not know what these programs were or what they were doing on their computer.

Other research shows that security suites do not live up to consumer expectations. Some of these security suites detect digital threats, but do not eliminate them all. Another problematic aspect of the security suites is quality, which shifts over years. Microsoft antivirus software scored really well in 2005, while in 2006 it came in only fourth place (it failed to detect 30% of the viruses and other malware)[xiii]. Consumers run all the risks if they do not switch in a timely manner to a provider who scores well at a certain moment in time. It is hard for consumers to know which one is the best one at a certain moment in time. Other problems occur when consumers want to install wireless modems. They are not sufficiently guided to secure their wireless connections, though this is often the most difficult aspect of the installation process. In short, providers of software and hardware do not take adequate responsibility for digital security.

Due to the fundamental security flaws of the Internet and the lack of sufficient security measures taken by industry, consumers are not able to act effectively to protect themselves. An additional factor is the fast deployment of services and applications on the Internet that involve complex applications, many of which are not designed with security in mind.

The competition-driven model under which telecommunications and technology are developed has not produced products and services with adequate security. For consumers, security is not really a purchase criterion and they expect their products and services to be safe and secure even when they are not. The European directive on privacy and electronic communications[xiv] already obliges providers to deliver safe and secure services and networks. Sales are driven by consumer demand for performance, price, ease of use, maintenance, and support. As a result, hardware and software are sold in an easy-to-use but insecure configuration. This makes them vulnerable, especially when we consider that

consumers lack the structural information, skills and basic knowledge that only professionals have.

Until now, the main responsibility for protection against threats and attacks to digital security has been placed on end users. This is not a logical or effective way to deal with the problem of Internet security, because digital security is, as a result of its dynamics, too complex for the average consumer. Improving security in digital environments is an issue that involves many different parties, including consumers. But the figures mentioned above show that, although raising consumer awareness about Internet security is important, consumers can not be expected to take full responsibility. Managing one's own security is too complex and costly for most consumers.

Recommendations

TACD resolves that the governments of the EU and U.S. should:

1. Enforce and, where necessary, improve or enact laws that oblige providers of electronic products and services to safeguard the security of electronic products and services through appropriate measures. The notion of appropriate measures must be further clarified and specified through the establishment of dynamic and technologically neutral standards.

2. Properly monitor and enforce legal obligations for Internet Service Providers to provide for safe networks and to inform consumers about possible security breaches in their systems.

3. Make providers of electronic products and services legally accountable for losses as a result of damage caused by not taking the appropriate security measures. This works as an incentive for the industry. National regulatory authorities (NRAs), private attorneys and consumers should have the legal instruments to be able to ask for compensation on behalf of individual consumers as well as through class actions.

4. Issue a coherent action plan for Internet security, which includes technology-neutral, dynamic standards for security products and services to comply with, and a certification scheme for privacy and security enhancing technologies developed and monitored by the industry and enforced by National regulatory authorities (NRAs) taking into account recommendation 5 of the TACD resolution on ID Theft, Phishing and Consumer Confidence[xv].

5. Require security to be the default setting. Of course TACD prefers the industry to secure its products, services and networks from its own initiative (as recommended in the TACD resolution on phishing, ID Theft and Consumer Confidence). However, in this regard, TACD is of the opinion that there should be regulation to ensure that the default security setting is part of the level playing field. This regulation provides the means to ensure the weeding out of commercial initiatives that provide and contribute to insecure digital products, services and networks.

6. Establish effective enforcement mechanisms to prevent large-scale economic damages as a result of security breaches.

7. Raise awareness amongst consumers as well as SME's about security measures and existing rights and remedies through information campaigns in partnership with privacy and consumer groups, taking into account recommendation 10 of the TACD resolution on Phishing, ID Theft and Consumer Confidence[xvi].

With regards to industry, TACD resolves that:

1. Internet service providers should provide free information about Internet security and provide for free and adequately working spam filters, virus scanners and firewalls, taking into account recommendation 5 of the TACD resolution on ID Theft, Phishing and Consumer Confidence.

2. Network providers should monitor their network integrity continually and create mechanisms to ensure network integrity.

3. Companies and businesses should agree to not use any malware, spyware and remote manipulation of external computers, and to name and shame companies and businesses that do not comply with this rule.

Endnotes

[i] TACD resolution on Unsolicited Commercial Email: www.tacd.org/docs/?id=224)
[ii] TACD resolution on Identity Theft, Phishing and Consumer Confidence: www.tacd.org/docs/?id=306)
[iii] According to Nielsen/Netratings at www.internetworldstats.com/am/us.htm
[iv] Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World, M. S. Blumenthal, and D.D. Clark, Cambridge MA: MIT Press, page 70-109.
[v] Consumer Reports, *State of the Net*, September 2006
[vi] Centraal Bureau voor de Statistiek, *De digitale economie 2006*, www.cbs.nl.
[vii] Phishing is a specific form of identity theft that employs social engineering and technical subterfuge to obtain consumers' personal information. Typically, the ID thieves, masquerading as legitimate companies, organizations, or agencies, use emails to lead consumers to counterfeit websites designed to trick them into divulging account numbers, passwords, and other data.
[viii] Pharming are attacks on consumers' computers that may be used to either key-log their access to online accounts when they enter passwords or to redirect them to fake websites even if they type in the correct Internet addresses of their banks or other online services.
[ix] Sniffing is the interception and reading of IP-based information packages, e.g. email messages, user names and passwords. Through sniffing, one can '(wire)tap' traffic on the internet.
[x] Spoofing is fraudulent email activity in which the IP address of the original sender is changed to appear as if it originated from a different IP address. Another form of spoofing is the man-in-the-middle attack. In this form of network attack, a hacker will intercept communications between two parties and alter it to convince the recipient to disclose confidential information.
[xi] Survey computer users, *Hoe veilig waant u zich op het Internet*, Consumentengids, November 2006.
[xii] America Online and the National Cyber Security Alliance, *AOL/NCSA online Safety Study*, December 2005.
[xiii] Research Consumentenbond, *Haal een griepprik voor uw pc*, March 2005, de Digitale Consument, and research Consumentenbond, *Houd uw pc privé*, March 2006. de Digitale Consument.
[xiv] Directive 2002/58/EC.
[xv] This recommendation states that governments should provide incentives and regulatory guidance to spur industry to further invest in the security of their systems and their brands.
[xvi] This recommendation states that businesses should help to educate consumers about ID theft, phishing and other forms of internet fraud.