



HOUSE OF LORDS

Science and Technology Committee

---

5th Report of Session 2006–07

# Personal Internet Security

## Volume I: Report

---

Ordered to be printed 24 July 2007 and published 10 August 2007

---

Published by the Authority of the House of Lords

*London* : The Stationery Office Limited  
£16.50 (inc VAT in UK)

HL Paper 165–I

### *Science and Technology Committee*

The Science and Technology Committee is appointed by the House of Lords in each session “to consider science and technology”.

### *Current Membership*

The Members of the Science and Technology Committee are:

Lord Broers (Chairman)  
Lord Colwyn  
Lord Haskel  
Baroness Finlay of Llandaff (co-opted)  
Lord Howie of Troon  
Lord Patel  
Lord Paul  
Baroness Perry of Southwark  
Baroness Platt of Writtle  
Earl of Selborne  
Baroness Sharp of Guildford  
Lord Sutherland of Houndwood  
Lord Taverne

For members and declared interests of the Sub-Committee which conducted the inquiry, see Appendix one.

### *Information about the Committee and Publications*

Information about the Science and Technology Committee, including details of current inquiries, can be found on the internet at <http://www.parliament.uk/hlscience/>. Committee publications, including reports, press notices, transcripts of evidence and government responses to reports, can be found at the same address.

Committee reports are published by The Stationery Office by Order of the House.

### *General Information*

General information about the House of Lords and its Committees, including guidance to witnesses, details of current inquiries and forthcoming meetings is on the internet at: [http://www.parliament.uk/about\\_lords/about\\_lords.cfm](http://www.parliament.uk/about_lords/about_lords.cfm).

### *Contacts for the Science and Technology Committee*

All correspondence should be addressed to:  
The Clerk of the Science and Technology Committee  
Committee Office  
House of Lords  
London  
SW1A 0PW

The telephone number for general enquiries is 020 7219 6075.  
The Committee’s email address is [hlscience@parliament.uk](mailto:hlscience@parliament.uk).

## CONTENTS

---

	<i>Paragraph</i>	<i>Page</i>
<b>Abstract</b>		<b>6</b>
<b>Chapter 1: Introduction</b>		<b>7</b>
Background and acknowledgments	1.11	<b>8</b>
<b>Chapter 2: Overview: the Internet and personal security</b>		<b>10</b>
The Internet: basic definitions	2.1	<b>10</b>
Tracing Internet traffic	2.10	<b>12</b>
Security threats on the Internet today	2.16	<b>13</b>
The scale of the problem	2.27	<b>15</b>
Research and data collection	2.36	<b>17</b>
Conclusions and recommendations	2.42	<b>19</b>
<b>Chapter 3: The network</b>		<b>20</b>
The prospects for fundamental redesign of the Internet	3.1	<b>20</b>
Recommendation	3.8	<b>21</b>
The “end-to-end principle” and content filtering	3.9	<b>21</b>
Who is responsible for Internet security?	3.20	<b>23</b>
Conclusion	3.34	<b>26</b>
Network-level security	3.35	<b>26</b>
Internet service provision	3.41	<b>27</b>
The “mere conduit” defence	3.62	<b>31</b>
Voice over Internet Protocol	3.64	<b>32</b>
Recommendations	3.67	<b>32</b>
<b>Chapter 4: Appliances and applications</b>		<b>34</b>
Usability vs security	4.2	<b>34</b>
Maintaining security—patching and security software	4.13	<b>36</b>
Emerging threats and solutions	4.22	<b>38</b>
Vendor liability	4.25	<b>38</b>
Conclusions and recommendations	4.38	<b>41</b>
<b>Chapter 5: Using the Internet: businesses</b>		<b>43</b>
Overview	5.1	<b>43</b>
Security standards	5.8	<b>44</b>
Incentives	5.23	<b>47</b>
The enforcement regime	5.42	<b>51</b>
Conclusions and Recommendations	5.53	<b>53</b>
<b>Chapter 6: Using the Internet: the individual</b>		<b>54</b>
Overview	6.1	<b>54</b>
Individual skills	6.6	<b>54</b>
Awareness vs knowledge	6.11	<b>55</b>
Sources of information and advice	6.16	<b>56</b>
The role of Ofcom	6.19	<b>57</b>
Education	6.25	<b>58</b>
Personal safety online	6.33	<b>60</b>
Recommendations	6.46	<b>62</b>
<b>Chapter 7: Policing the Internet</b>		<b>64</b>
Overview	7.1	<b>64</b>

The legal framework	7.3	64
High volume, low denomination crime	7.16	67
Reporting procedures	7.20	68
The structure of law enforcement	7.35	71
Police skills and resources	7.44	72
International action	7.57	75
The courts	7.63	76
Sentencing	7.70	77
Conclusions and recommendations	7.74	78
<b>Chapter 8: Summary of Conclusions and Recommendations</b>		<b>80</b>
Overview: The Internet and Personal Security	8.2	80
The network	8.6	80
Appliances and applications	8.12	81
Using the Internet: businesses	8.16	82
Using the Internet: the individual	8.21	83
Policing the Internet	8.25	83
<b>Appendix 1: Members and Declarations of Interest</b>		<b>86</b>
<b>Appendix 2: Witnesses</b>		<b>88</b>
<b>Appendix 3: Call for Evidence</b>		<b>92</b>
<b>Appendix 4: Seminar held at the Institution of Engineering and Technology, Savoy Place, London</b>		<b>94</b>
<b>Appendix 5: Visit to the United States</b>		<b>99</b>
<b>Appendix 6: Visit to Metropolitan Police Service, Cobalt Square</b>		<b>114</b>
<b>Appendix 7: Glossary</b>		<b>115</b>
<b>Appendix 8: List of Acronyms and Abbreviations</b>		<b>120</b>

Note: The Report of the Committee is published in Volume I (HL Paper 165-I); the evidence is published in Volume II (HL Paper 165-II).

References in the text of the Report are as follows:

(Q) refers to a question in the oral evidence

(p) refers to a page of written evidence



## **ABSTRACT**

The Internet is a powerful force for good: within 20 years it has expanded from almost nothing to a key component of critical national infrastructure and a driver of innovation and economic growth. It facilitates the spread of information, news and culture. It underpins communications and social networks across the world. A return to a world without the Internet is now hardly conceivable.

But the Internet is now increasingly the playground of criminals. Where a decade ago the public perception of the e-criminal was of a lonely hacker searching for attention, today's "bad guys" belong to organised crime groups, are highly skilful, specialised, and focused on profit. They want to stay invisible, and so far they have largely succeeded. While the incidence and cost of e-crime are known to be huge, no accurate data exist.

Underpinning the success of the Internet is the confidence of hundreds of millions of individual users across the globe. But there is a growing perception, fuelled by media reports, that the Internet is insecure and unsafe. When this is set against the rate of change and innovation, and the difficulty of keeping pace with the latest technology, the risk to public confidence is clear.

The Government have insisted in evidence to this inquiry that the responsibility for personal Internet security ultimately rests with the individual. This is no longer realistic, and compounds the perception that the Internet is a lawless "wild west". It is clear to us that many organisations with a stake in the Internet could do more to promote personal Internet security: the manufacturers of hardware and software; retailers; Internet Service Providers; businesses, such as banks, that operate online; the police and the criminal justice system.

We believe as a general principle that well-targeted incentives are more likely to yield results in such a dynamic industry than formal regulation. However, if incentives are to be effective, they may in some cases need to be backed up by the possibility of direct regulation. Also, there are some areas, such as policing, where direct Government action is needed. So Government leadership across the board is required. Our recommendations urge the Government, through a flexible mix of incentives, regulation, and direct investment, to galvanise the key stakeholders.

The threat to the Internet is clear, but it is still manageable. Now is the time to act, both domestically, and internationally, through the European Union and through international organisations and partnerships.

# Personal Internet Security

## CHAPTER 1: INTRODUCTION

---

- 1.1. The Internet is a global network of millions of interconnected computer networks linking hundreds of millions of machines used by over a billion people. It transfers data between these machines in such a way that the computers at each end of a connection need not be aware of each other's physical location, or the technical details of the many intervening data transmission systems.
- 1.2. The origins of the Internet lie in the 1970s, but it was opened to commercial traffic in 1985, began to be widely used by individuals in the early 1990s and is now so important that it is deemed to be part of the critical national infrastructure of all developed nations.
- 1.3. The Internet underpins a considerable amount of global economic activity, permitting huge changes in traditional business models. It has also radically changed the way in which individuals are able to access information, entertain themselves, and even the way in which they meet their partners. It has undoubtedly been, and continues to be, a powerful force for good.
- 1.4. It is also a complex phenomenon that continues to evolve and grow at a rapid pace. In March 2007 the total number of Internet users world-wide was put at 1.114 billion, or 16.9 percent of the world's population. Internet penetration continent by continent varies from 3.6 percent in Africa to 69.7 percent in North America. In the United Kingdom Internet penetration is 62.3 percent, among the highest in Europe, with growth from 2000–2007 put at 144.2 percent.<sup>1</sup> Some eastern European countries have seen growth over the same period, albeit from very low levels, of well over 1,000 percent.
- 1.5. The fast-changing technology underpinning this growth in Internet use is very poorly understood by the vast majority of its users. Indeed, one reason for the prodigious success of the Internet is that users can “surf the web” without having to understand the technical means by which information is accessed or communicated. The many layers of technology that lie beneath the interface seen by the user, typically a software application known as a web browser, are effectively hidden. But just as the technology is for most users invisible, so are the risks.
- 1.6. These risks are manifold. They threaten personal security—that is to say, they may undermine the individual's ability to control the information that they have entered into or stored on connective devices such as PCs, mobile telephones, or databases operated by commercial organisations, government agencies and others. Victims typically suffer financial loss through fraud, though in cases of identity theft they may also suffer loss of reputation, or, in extreme cases, may be accused of crimes they did not commit.
- 1.7. Online risks may also impact upon personal safety—by which we mean they may lead to direct physical or psychological harm to the individual. One high-profile threat is that posed to children by predatory paedophiles, who conceal their true identity whilst using the Internet to “groom” potential

---

<sup>1</sup> Source: Internet World Stats (<http://www.internetworldstats.com/stats.htm>).



































































































































































































































