THE GOVERNMENT RESPONSE TO THE
TWELFTH REPORT FROM THE
SCIENCE AND TECHNOLOGY COMMITTEE
SESSION 2010–12 HC 1537

Malware and cyber crime

Presented to Parliament
by the Secretary of State for the Home Department
by Command of Her Majesty

April 2012

Cm 8328

£6.25

Any enquiries regarding this publication should be sent to us at:

beth.hiles@homeoffice.gsi.gov.uk

This publication is also available for download at www.official-documents.gov.uk

ISBN: 9780101832823

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office

ID P002482987 03/12 19480 19585

Printed on paper containing 75% recycled fibre content minimum.

THE GOVERNMENT RESPONSE TO THE TWELFTH REPORT FROM THE SCIENCE AND TECHNOLOGY COMMITTEE SESSION 2010-12, HC 1537

Introduction

1. On 19 July 2011, the Science and Technology Committee announced an inquiry into the impact of malware on individuals, the responsibilities of Government to aid in preventing malware infections and the economy that has grown up around this industry. The Committee previously examined the risks of cyber crime in its third report of the 2010-12 Session, *Scientific advice and evidence in emergencies*, which focused on national security and events that would require a national response.

2. The Government welcomed the report of the Committee's inquiry as a valuable contribution to the debate on cyber crime. The Home Office Parliamentary Under-Secretary of State for Crime and Security, James Brokenshire MP, appeared before the Committee to give oral evidence on 14 November 2011.

3. The Report of the Committee's inquiry was published on 2 February 2012. The Government has considered the Committee's recommendations carefully and this paper sets out the Government's response. For ease of reference the paper responds to each of the Committee's recommendations (in bold type) in turn.

The importance of trusted information

Recommendation 1. The Government is clear that many government services will move to online provision either directly or through a range of providers. It is also clear that an increasing proportion of UK economic activity will be conducted through or related to the internet. We ask the Government to provide, in response to this report, details of how they intend to engender greater trust in online products and services within the UK population and an assurance that online by default will mean better and more secure, rather than merely cheaper, government services. (Paragraph 74)

Government Response

4. Maintaining trust in the internet and digital technologies will be crucial in realising their potential. The public, businesses and Government need to be confident that, as they continue to use and depend upon cyberspace, they can do so safely.

5. Prevention is a key part of our response. Most common cyber incidents could be prevented by quite simple 'cyber hygiene'. UK Government Communications Headquarters (GCHQ) estimates that 80% or more of currently successful attacks could be defeated by simple best practice, such as updating anti-virus

software regularly. We will use social media to provide warnings about scams or other online threats, improve cyber security education at all levels and provide clear cyber security advice through Get Safe Online.

6. The first eight UK universities conducting world class research in the field of cyber security have been awarded “Academic Centre of Excellence in Cyber Security Research” status by GCHQ in partnership with the Research Councils’ Global Uncertainties Programme (RCUK) and the Department for Business Innovation and Skills (BIS). The Centres of Excellence will help make the UK government, business and consumers more resilient to cyber attack by extending knowledge and enhancing skills in cyber security.

7. We will ensure our law enforcement remains effective by making sure we have the right legal framework and enforcement capabilities to disrupt and prosecute cyber crime. We are making it easier to report cyber crime and ensure that the intelligence from reporting is fed back into effective action and advice to the public. Within Government, we will model best practice in the way we set up our own systems, by setting strong standards for suppliers. We will improve the information available to people buying security products, by encouraging the development of security ‘kitemarks’ to help customers to navigate the market.

8. One of the principal ways in which Government intends to build trust in online products and services is through the development of authoritative identity assurance. We have established an Identity Assurance Programme (IDAP), based at the Government Digital Service (GDS) and supported by a Board representing senior officials across Government, which will ensure an effective, collaborative approach is developed.

9. The programme supports the 'digital by default' policy. Digital transactions offer both convenience for customers and cost saving opportunities for public service providers.

10. Identity assurance is an important element in establishing trust. People and businesses must be assured of who they are interacting with and what will happen to their personal or business data. The problem that the programme will address is not limited to the public sector or to the UK. The programme seeks to align with equivalent international initiatives and to make use of rapidly developing solutions emerging from the private sector.

11. We also announced in the Cyber Security Strategy that we will create a forum, led by Ministers, which will bring together representatives from industry, law enforcement agencies and Government to drive forward work on designing out crime online, developing best practice for security and effective crime prevention advice for all levels of business.

Recommendation 2. We welcome the Government’s commitment in the *Cyber Security Strategy* to enhance the ability of the public to report cyber crime. We recommend that the Government consider how to encourage (or require) businesses to report incidence of cyber crime. Additionally, we urge internet

security companies to work with Government to find a way to use the development of a cyber hub to facilitate the detection of malware. (Paragraph 23)

Government Response

12. We announced in the Cyber Security Strategy that we would build a single reporting system for citizens and small businesses to report cyber crime, so that action can be taken and law enforcement agencies can establish the extent of cyber crime. The Action Fraud reporting service has now been expanded to take crime reports and information on all financially-motivated online crime, including hacking and denial of service attacks.

13. Since publication of the Cyber Security Strategy, the public-private sector information-sharing 'hub' pilot has been launched. The hub includes organisations from defence, telecoms, finance, pharmaceuticals and energy and heralds a new era of unprecedented cooperation between the Government and industry on cyber security. It allows the Government and the private sector to exchange actionable information on cyber threats and manage the response to cyber attacks. If the pilot is successful, one key output will be to consider how this model might be extended to include more private sector organisations.

14. Regarding the detection of malware, our work with internet service providers (ISPs) to develop a set of guiding principles is outlined below under Recommendation 8.

Recommendation 3. Knowledge is the best defence against fear and we recommend that Government-provided information focuses on how to be safe online rather than warns about the dangers of cyber crime. We also recommend that the Government work with the industry partners announced in the *Cyber Security Strategy* to promote the equivalent of a 'Plain English' campaign to make the technology easier to understand and use. (Paragraph 28)

Government Response

15. We identified in the National Cyber Security Programme (NCSP) and Cyber Security Strategy that raising awareness is a crucial part of improving safety online. As part of the NCSP, the National Fraud Authority (NFA) launched a major awareness campaign in March, targeted at those members of the public most at risk from internet crime. This innovative campaign is targeting eight million adults through social media sites.

16. The Get Safe Online website, GetSafeOnline.org, explains online safety in plain English and provides independent, trustworthy advice and tools to help people stay safe online. It has produced a 'Rough Guide to Internet Security' in conjunction with Rough Guides.

Recommendation 4. We recommend that the Government take note of the importance of addressing different messages to different generational groups of UK internet users. (Paragraph 31)

Government Response

17. The NFA's customer segmentation work categorises the adult population by their vulnerability to fraud and internet crime. This is now being used to target specific messages through the most effective channels and measure any changes in the steps which people are taking to protect themselves. This includes directing victims to where they can make a report. The NFA online fraud campaign directs people to the Get Safe Online website, as well as to Action Fraud.

18. In addition to the information provided to citizens, the Government also considers it important that messages are tailored to different sizes of business across industry sectors. BIS is working with both the NFA and Get Safe Online to understand small and medium-sized enterprises' understanding and perceptions of online security and the channels of support and advice which they trust.

Recommendation 5. We recommend that the Government invest in the Get Safe Online site to ensure that it integrates all of the relevant organisations necessary to provide a single authoritative source on which computer users could rely. We also recommend a prolonged public awareness campaign to raise awareness of the issue of personal online security and the presence of the website to achieve the best possible information level among all computer users. (Paragraph 61)

Government Response

19. The Government, alongside industry, has a responsibility to educate the general public on how to stay safe online. This is not only to protect individuals from online crime but also to protect the Government's investment in the expansion of online services.

20. The NCSP includes greater funding for awareness. It has been agreed by Government departments and private sector sponsors that Get Safe Online should be the single point of reference for the general public and small businesses on internet security.

21. Get Safe Online has achieved a good level of awareness with limited funding from Government. We are working with Get Safe Online to explore options to expand the service over the coming year, working both to improve the quality of the website and the general awareness of it as a source of advice.

22. The UK Council for Child Internet Safety (UKCCIS) has produced guidelines for website owners and ISPs to help ensure the internet safety messages they give to parents and children are consistent and effective. These include guidance on safe downloading and how to protect against online fraud.

Recommendation 6. We agree with the Government that effort is needed to raise awareness of the advice available on the Get Safe Online website. We expect the joint action plan mentioned in the *Cyber Security Strategy* to provide details of what will be done to raise awareness. Moreover, the Government should persuade private industry to cross promote Get Safe Online. Television exposure is crucial to gain the widest possible exposure to the safety message. We also recommend that all Government websites should point towards Get Safe Online and feature security updates from the Get Safe Online website. (Paragraph 62)

Government Response

23. The additional support we are aiming to provide to Get Safe Online will make the website more appealing and interactive, with more tools to educate people and ultimately to change their behaviour. The Get Safe Online team are already conducting outreach events to raise awareness. The Joint Action Plan will include further details of how we will improve awareness, as well as plans for the expansion of Get Safe Online.

24. A number of key Government websites already link to Get Safe Online and, as mentioned above, the NFA online fraud campaign directs people to Get Safe Online as well as Action Fraud. Directgov, the official website for Government information and services, links to Get Safe Online as part of its advice on keeping individuals and their computers secure.

25. BIS is leading the awareness-raising effort with businesses and will consider campaign activity in light of its preliminary work into understanding business requirements.

Recommendation 7. We recommend that the Government require that access to Get Safe Online advice is provided by vendors with every device capable of accessing the internet. (Paragraph 64)

Government Response

26. A Retail Cyber Security Forum (RCSF) has been established following publication of the Cyber Security Strategy. The RCSF will play its part in supporting economic prosperity and growth by building a more trusted and resilient digital environment.

27. The RCSF will work with the retail industry to address domestic and international cyber security challenges and issues of common concern, including examining what measures could be taken to improve consumer safety online.

28. UKCCIS has been working in partnership with retailers to look at the opportunities for providing child internet safety advice at the point of sale. Several major retailers now provide information as leaflets, on till receipt wallets and online when an internet-enabled device is purchased.

The need for standards

Recommendation 8. We recommend that the Government work with ISPs to establish an online database where users can determine whether their machine has been infected with botware and gain information on how to clean the infection from their machine. We think that this should also be integrated with the Get Safe Online website. (Paragraph 47)

Government Response

29. The Cyber Security Strategy acknowledges that ISPs can make an important contribution to identifying and preventing cyber attacks on UK networks. With this is in mind, it was announced that the Government will work with the main ISPs to co-design a set of guiding principles which could be adopted on a voluntary basis.

30. Under consideration as part of these principles is a proposal to notify customers whose machines have been infected by malware and botnets, and potentially provide advice and support. We believe that this would be a more effective mechanism to address the problem than the creation of a database.

Recommendation 9. It would be possible to impose statutory safety standards on software sold within the EU, similar to those imposed on vehicle manufacturers, but we would prefer a solution based on self-regulation. However, the industry must demonstrate that any proposed solution would be an effective way forward and that voluntary commitments would provide sufficient incentive for the industry to improve security in a fast-moving competitive marketplace. In the event that the industry cannot demonstrate an effective self-regulatory model, we recommend that the Government investigate the potential for imposing statutory safety standards. (Paragraph 57)

Government Response

31. Safety standards in the automotive industry relate to devices performing specific functions, whereas the functions that can be performed by software are almost limitless. As a result, the specification in statute of security standards capable of offering meaningful security would be likely to stifle innovation in future. It would also require a vast library of options to cater even for devices which are available at present.

32. We encourage software developers to focus on the principles for creating good software and to test and highlight that this has been done. We consider that software standards and adherence to them should continue to be voluntary and we will consider them as part of the work which is outlined under Recommendation 10 below.

Recommendation 10. In relation to kitemarks, we recommend the Government look to investigate the potential for solutions that will lead to a less clear cut division of the market by allowing lower up-front costs for smaller software developers and a range of security standards. (Paragraph 67)

Government Response

33. It is key to the creation of new standards and promotion of existing ones that they should be widely accepted in the market, cost-effective for small providers and affordable to average users.

34. Although these principles may limit what can be achieved, they are essential if we wish to achieve a universal level of increased security and create solutions which are accessible by small-scale developers and users. BIS is working with GCHQ to analyse the wide range of standards that is currently available and determine how we may best work with them to develop appropriate ones further.

Recommendation 11. We judge that there will be a need for an automated way to assess the security of software, even if simply to provide smaller companies with a means of testing and redesigning their software prior to spending money on kitemarks. We recommend that the Government explore whether this might best be developed by Government, for Government, in partnership with private industry or by entirely private concerns. (Paragraph 70)

Government Response

35. The creation of standards and testing routes which are accessible to smaller companies is part of our requirement for a standards regime that improves cyber security. However, automated testing on its own is a tool which only does part of the job. It can lead to the creation of software which passes the tests but is not particularly good.

36. The focus should thus be on embedding good software writing principles rather than performing simple tests. Automated testing can highlight issues of concern to be investigated, but should not be presented as a definitive quality mark. It could therefore be offered to software writers as an initial indicative test of their software's security, but not as something to market the software against. We will consider as part of our standards review (noted under Recommendation 10) how software may be improved, focusing on voluntary take up by industry.

Expertise and policing

Recommendation 12. We are impressed by PhonepayPlus' expertise on the dangers of criminal exploitation of smartphones. We recommend that PhonepayPlus has a dedicated part of the enhanced Get Safe Online website and that they are consulted closely in the development of regulatory policy to

take into account, for example, online services involving micropayments. (Paragraph 34)

Government Response

37. PhonepayPlus are already closely engaged with Get Safe Online and they are working together to expand their contribution to the site. We will engage with relevant stakeholders including the Financial Services Authority and PhonepayPlus in any policy development work relating to online payments, including micropayments.

Recommendation 13. We recommend that the police have dedicated pages on Get Safe Online on which they might communicate directly with the general public, to gather information and intelligence about what is happening to individual computer users and to provide consumers with an authoritative policing voice on current cyber crime issues. (Paragraph 37)

Government Response

38. The police already provide much advice on current cyber crime issues to Get Safe Online and we would not wish to duplicate effort on other law enforcement websites. As mentioned above, the NFA's Action Fraud reporting tool has been expanded to be a single reporting point for financially-motivated cyber crime. Information is then passed to the police, informing law enforcement activity and improving the intelligence picture.

Recommendation 14. We recommend that the Government ensures that the Strategic Policing Requirement addresses individual-level cyber crime, not least because much of it appears to be directed by organised crime gangs. Given competing local priorities for funding policing activities, only establishment within the Requirement will ensure that police forces invest the money necessary to guarantee that local officers are able to respond to individual victims of cyber crime. (Paragraph 39)

Government Response

39. The Strategic Policing Requirement is a statement of national threats and the national policing capabilities needed to counter them. It is focused on those threats that cross police forces' boundaries and therefore require them to undertake an element of joint planning, or ensure interoperability between their capabilities. The shadow Strategic Policing Requirement, which the Home Secretary published in November 2011, identifies two cyber threats of this description: a large-scale cyber incident (which might include a criminal attack on a financial institution, or an aggregated threat where many people or businesses across the UK are targeted) and large-scale cyber crime with an organised crime element.

40. The Government is committed to mainstreaming the capacity to tackle cyber crime across the police service. We said in the Cyber Security Strategy that we would ensure the development of new training, giving local forces more capability to understand, investigate and disrupt cyber crime. We are creating a National Cyber Crime Unit in the National Crime Agency, which will act as a centre of expertise to support the enhancement of law enforcement capacity.

41. As mentioned above, the Action Fraud service has been expanded to help improve the response to individuals and small businesses who have been affected by cyber crime.

Recommendation 15. Both the Government and the police appear to want the response to low-level cyber crime to be a mainstream part of UK policing. Only when police officers are comfortable operating in online contexts and using existing legislation to tackle online theft and fraud will it be possible properly to identify whether additional legislation is required. However, we think it is important that those engaged in lowgrade cyber crime can be punished without recourse to courts and that the Government should work hard with the industry to develop effective online sanctions for cyber criminals as indicated in the *Cyber Security Strategy*. (Paragraph 43)

Government Response

42. The Committee suggests that penalties for lower-level cyber crime should be available without recourse to courts. The Government does not believe the introduction of a fixed penalty notice in these circumstances would be appropriate. Traditional crime such as fraud, theft or harassment is covered by existing legislation and sanctions, whether it is carried out online or offline. Appropriate penalties are also available under the Computer Misuse Act for crime which targets information systems directly. The fact that a crime is conducted online should not cause it to be regarded less seriously, as in many cases its impact may in fact be increased.

43. As well as being inappropriate for the seriousness of many of these offences, fixed penalty notices are intended for offences which are straightforward (for example, not generally requiring an investigation). They should act as a deterrent, which would not be the case where committing an offence could be highly lucrative for a criminal. A new scheme should also respond to a 'gap in the market', where existing disposal options present either an excessive or inadequate response. In the case of cyber crime, the option to take offenders to court is used appropriately following investigation, and where court is not necessary or appropriate a caution may be administered.

44. As we said in the Cyber Security Strategy, we will work to ensure that law enforcement agencies and the judiciary are aware of the additional powers the courts already have to protect the public when there is strong reason to believe someone is likely to commit further serious cyber crime offences.

Recommendation 16. We welcome the commitment in the *Cyber Security Strategy* to make it easier and more intuitive for the public to report online crime. We urge the Government to ensure that this reporting function is integrated with the development of the Get Safe Online site as a one-stop shop for online security information and issues. (Paragraph 44)

Government Response

45. Action Fraud is working closely with Get Safe Online to ensure a joined up approach to providing advice for members of the public and businesses. This work includes co-ordinated planning for communication. Get Safe Online will add a "Report Fraud" button to most of their website pages, to direct people to Action Fraud as the single place to report fraud and online crime. Get Safe Online is looking at new and innovative ways to attract people to their site and Action Fraud is supportive of this work.

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries: 0870 600 5522
Order through the Parliamentary Hotline Lo-Call 0845 7 023474
Fax orders: 0870 600 5533
E-mail: customer.services@tso.co.uk
Textphone: 0870 240 3701

The Parliamentary Bookshop
12 Bridge Street, Parliament Square
London SW1A 2JX
Telephone orders/General enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: bookshop@parliament.uk
Internet: http://www.bookshop.parliament.uk

TSO@Blackwell and other Accredited Agents

ISBN 978-0-10-183282-3