UK Internet Security: State of the Nation

The Get Safe Online Report

November 2010
Foreword

Baroness Pauline Neville-Jones, Minister of State for Security and Counter Terrorism

Securing cyberspace is one of the highest UK national security priorities. The risks in cyber space range from hostile attacks from other states, from people using cyber space for terrorism purposes and, perhaps most obviously, from online criminals. At the same time, the internet continues to provide great opportunities for every one of us.

Both the threats and opportunities associated with the internet are likely to increase significantly over the next five to ten years, as our dependence on online communication and transactions increases. Therefore staying safe online becomes more important than ever.

In the six years since its creation, Get Safe Online has provided an indispensable advice service to UK citizens and small businesses. The changes in attitudes and behaviours outlined in this year’s report are a testament to Get Safe Online’s success and, I might add, to the importance of continuing the good work. Online criminals and their methods are increasing in sophistication. The use they make of social engineering techniques and ‘real-world’ tactics to defraud internet users can be defeated if we at all times deploy the simple security measures that we should.

It is essential that Government and industry continue to work together to raise awareness still further of these basic security and policy issues. Only by working in close partnership can we effectively tackle burgeoning online crime. I am therefore very pleased to support the Get Safe Online initiative in bringing together, for a sixth year, government bodies, law enforcement agencies and the private sector to tackle the safety needs of the UK’s internet users.

Welcome to Get Safe Online’s 2010 Annual Report, an analysis of the UK’s internet usage, key areas of threat and current attitudes to online safety.

Within the report we have set out some of the findings from our latest research, along with analysis and commentary from our sponsoring partners. We hope you find it an informative read!

1. Unless otherwise stated, all figures taken from the 2010 Get Safe Online survey by ICM Research. 2007 – 2009 figures from previous comparable Get Safe Online surveys also by ICM Research.
During the past year, law enforcement has had some excellent results in the prosecution of criminals in the virtual environment. It is rewarding for everyone involved when we get these results, and we must always have a focus on criminal justice outcomes. However, the speed and reach of crime on the internet will never be defeated by prosecutions alone.

There is greater recognition today that we must all work together to make the internet a safer place. As such, we find ourselves working not only with law enforcement colleagues from across the world – including the Federal Bureau of Investigation (FBI) – but also with those who coordinate, manage and map the web.

In SOCA e-Crime, we have developed a number of collaborative projects designed to create a more hostile environment for criminals. For example, Project Minstrel works with the Internet Corporation for Assigned Names and Numbers (ICANN) and the Regional Internet Registries (RIRs) to ensure that internet fraudsters are denied the opportunity to use online services to further their criminal exploits. This includes preventing the registration of spoof domain names and increased scrutiny of registration details in order to better identify false applications.

Earlier this year, I was asked to join the ICANN Review Team – the group responsible for maintaining Whois, the telephone directory for the internet. Whilst still respecting the privacy of individuals, this is the first time law enforcement has been involved in internet registration in this way. Part of my role involves canvassing the opinion and expertise of as many colleagues as I can to ensure we bring a 360° view to the table.

The importance of this type of collaboration should not be understated – it represents a critical step in preventing criminals from exploiting the services that we all may now have difficulty living without.

Life without the internet – now there’s a thought!
Since 2005 internet take-up at home has risen from just over half the population (54%) to seven in ten in 2009 (71%). And it’s not just the PC or laptop that’s being used – 28% go online via a mobile phone, rising to 50% of those aged 16–24.

The social and economic benefits of using the internet are becoming increasingly apparent – half of all internet users now say that using the internet has increased their contact with friends or family who don’t live nearby.

According to our latest Media Literacy annual reports, which reveal the UK’s media consumption habits and attitudes, three in ten adults now prefer to check their bank balance online, compared with just over two in ten in 2005. Over a third of adults now prefer to book holidays online or by email. Half of UK adult internet users say they have made significant savings by comparing prices online or buying something online. And overall, eight in ten UK adult internet users say they’ve saved money by using the internet over the past six months.

Of course, a major development in recent years has been the rise and rise of social networking activity. In 2009, 44% of people online said they’d set up their own social networking site profile, double the figure in 2007 (22%).

It’s not just people’s behaviour that’s changed: most UK adult internet users are becoming more knowledgeable about security issues, and somewhat less willing to provide personal information online than they were in 2007.

Adults with a social networking profile are more likely to only allow friends or family to see it, at 80% compared with 48% in 2007.

However, around a quarter of internet users say they lack confidence in installing filtering software and installing security features.

Our very latest research also suggests that younger people aged 16–24 are much more comfortable with sharing details of their lives online than their older counterparts. They are much more likely to share information about what they’re doing or feeling, along with posting photos from holidays or nights out.

These developments mean that it’s increasingly important that people are confident about their security online and know how to protect themselves – and only share information with people they trust.

---

2. All figures in this article taken from Ofcom’s Media Literacy Audits 2005 – 2010.
For the average web user, the concept of a computer virus is now well understood. It’s in our everyday vocabulary and we usually have a clear idea if we’ve been affected by one – if it doesn’t announce itself, at the very least, your computer slows down and starts behaving strangely.

Today, the bigger threats appear to be those that sit silently on our computers without the owners knowing they are there. Microsoft’s latest Security Intelligence Report revealed that, globally, the number of machines that are part of a botnet [see right] have more than doubled – to 6.5 million in just three months in the early part of 2010, compared to 3 million in the same period last year.

Unlike viruses, botnets sit in the background – some are even capable of ‘protecting’ machines from other botnets and malicious software (malware) in order to keep the infected computer solely for its own use. However, once part of a botnet, a machine can be one of thousands being used to send out spam and mine personal data.

The spam they send out can contain malware, viruses, links to fraudulent websites or scams that trick users into providing sensitive information (phishing). In other words, they are mass platforms for much of the online crime that web users encounter everyday.

So, is it all doom and gloom? Of course not – and in many ways, this increased criminal effort is partly indicative that they have to work a lot harder these days in order to be successful. But it does mean we all have to stay on our toes when it comes to keeping safe and secure online.

---


4. Source: Microsoft.

---

What is a botnet?

- **Bot (from robot)** refers to software programs that perform network tasks with a degree of autonomy.
- Bots can perform beneficial or vital functions – they are used by many popular search engines.
- Unfortunately, bots are also developed for malicious purposes, such as assembling networks of compromised computers—botnets—that are controlled remotely and surreptitiously by bot-herders.
- Computers in a botnet, called nodes or zombies, are often ordinary computers sitting on desktops in homes and offices.
- Computers become nodes when attackers illicitly install malware that secretly connects the computers to the botnet.
- Nodes perform tasks such as sending spam, hosting or distributing malware or other illegal files, or attacking other computers.
- Attackers usually install bots by exploiting vulnerabilities in software, or by using social engineering tactics to trick users into installing the malware. Users are often unaware that their computers are being used for malicious purposes.
The first line of defence against online fraud is securing your computer. Whilst there is a general awareness and an increased sense of personal responsibility amongst internet users in this respect, there is still room for improvement. The key threats include viruses, malicious software (malware), spyware and spam email, all of which continue to become more sophisticated as the years move on.

To give an idea of the scale of the problem, it’s estimated that over a thousand new computer viruses emerge every month and an unprotected computer can be infected within minutes of connecting to the internet.

There is, however, a light at the end of the tunnel and it is encouraging to see that web users appear to be taking on board messages about PC security, and are much better today at making sure the basics are in place.

This year’s Get Safe Online survey results indicate that the majority of people accessing the internet from their home PC or laptop are using virus protection software and other forms of PC security. 87% of respondents state that they have up-to-date virus protection software, and a third (33%) of those update their anti-virus software when they switch their computer on, or update it very regularly (within the past week). Although the number of those that have virus protection remained steady (up by 1% on 2009), those keeping it updated regularly has decreased by 14% compared with last year.

We must not forget however, that virus protection is not the only factor which will protect against online threats. Anti-firewall and anti-spyware software is integral for security and internet users are showing signs of improvement with 83% and 74% respectively, having these measures in place.

However only half of UK web users have anti-phishing/website authentication software installed, which highlights an area of vulnerability. Something to consider given than 23% of web users have fallen foul of a phishing scam, and 1 in 5 (20%) have been the victim of a scam email or website.

As my colleagues will go on to say, being safe online isn’t just about having the right technology in place, however it is a very important foundation.

- 87% of internet users have up-to-date virus protection software
- 40% have had virus attacks on their PC
- 19% have been a victim of online identity fraud
- 23% have been targeting by phishing attacks
Savvy Surfing

Rob Skinner, Head of PR, PayPal UK

Keeping safe online is about attitudes as well as technology. Consumers who are vigilant and aware of possible risks are well placed to defeat the best efforts of fraudsters.

This year’s Get Safe Online survey suggests that most people have got the key messages about online security. For example, just 7% say they’ve replied to or clicked a link in a phishing email. And just 19% admit to opening an email attachment from someone they don’t know.

But we mustn’t be complacent. Fraudsters are adept at finding new ways to operate, especially given the fast changing nature of the online world. The rise of social networking sites has led many people to share more information about themselves online, which can aid fraudsters. For example, over a quarter (26%) of people surveyed by Get Safe Online admit sharing phone numbers, email addresses and even their mothers’ maiden names on social networking sites. (The figure rises to 38% amongst 18 to 24 year olds.)

Vigilance, common sense and good computer security are the frontline in our defence against online fraud.

Katie Kitiri, Gumtree Head of Trust and Safety

In the UK it is estimated around £5 billion per month is now spent trading online. This growth is also bringing an increased variety of successful marketplaces to the web. These marketplaces which span both business to consumer (B2C) and consumer to consumer (C2C) platforms, offer unique places within which to do business.

No matter what the type of online buying and selling taking place, there are some fundamental principles to ensuring a safe and successful trading experience:

1. Understand and follow the recommended way to transact
   All good sites will have processes and guidance in place to help ensure their users can trade safely and successfully. Some sites offer specific forms of payment that provide buyer and/ or seller protection. Local classifieds sites like Gumtree.com encourage and facilitate local in-person trade, which in itself is effective mitigation against the risk of fraud normally associated with trading with someone remotely.

Not understanding and following the recommended way to trade on a particular platform is the opportunity that sophisticated fraudsters often use to exploit consumers. They will often recommend their own alternative and unsafe methods such as payment for goods via money transfer services.

2. Beware of anything that’s “too good to be true”
   The old adage really does continue to apply to trading safely online, just as it does offline. While there are absolutely bargains to be had, many successful fraud attempts continue to be powered by people prepared to suspend common sense and the usual precautions in favour of a great deal.

3. If in doubt, seek advice
   Many sites now have good quality information online as well as improved accessibility to contact them for advice and support. User forums offered on many sites, including Gumtree.com, are also proving to be a highly effective way for people to get fast advice and information from peers.

5. IMRG/ Cap Gemini Sales Index October 2010.
The year of mobile malware

Rik Ferguson, Senior Security Advisor, Trend Micro

The number of attacks on mobile devices may not be growing substantially, but circumstances are conspiring to create a genuine risk for consumers. As the number of people using mobile devices to surf the internet, shop online and email grows, so does the attraction for hackers of this potentially lucrative target.

The more people who use their phones to carry out sensitive financial transactions, the more the same criminal networks that target our computers will start developing ways to attack our phones. In addition, data created and stored on our mobiles is more portable, more accessible and more widely disseminated than ever before.

Yet still the majority of users don’t secure their devices in even the simplest ways against online crime or data theft. Over half (57%) of smart phone users fail to protect their devices with a pin or password – the first form of defence against potential information theft.

It is true to say that consumers have become increasingly savvy to anti-virus protection on their desktops and laptops, however mobile devices are increasingly taking on greater functionality and are essentially operating as mini-computers. The lessons learnt and vigilance developed over the last 5-10 years and put in place in our homes and offices need to be applied when we are on the move too.
It's estimated that fraud costs the UK over £30.5 billion, and of that total, individuals lose at least £3.5 billion every year. In the past six months, 109,000 people have called Action Fraud, the national fraud reporting centre, or visited the website (www.actionfraud.org).

A third of these crime reports relate to fraud perpetrated online. These are predominantly online shopping and auction frauds, but include attempts to obtain access to financial accounts and also romance scams, whose victims can feel very embarrassed or ashamed.

On its own, online fraud represents a sizeable challenge. However, in recent years it has become apparent across Government, industry and law enforcement that, by drawing together the counter fraud community, we can focus efforts to combat fraud in the UK to greater effect. This is why the National Fraud Authority was established in 2008, why we set up Action Fraud, and why we joined Get Safe Online earlier this year.

Through Action Fraud, we can now capture fraud data and intelligence that was not previously reported. Action Fraud passes all confirmed crime reports to the National Fraud Intelligence Bureau (NFIB), operated by the City of London Police, which analyses them alongside fraud data supplied by business organisations and public sector partners to build a more detailed picture of fraud and how it is committed.

What does this mean? Well, now the NFIB is able to link previously unconnected crimes, victims and suspects, building compelling intelligence packages and cases for investigation. Cases prompted by reports to Action Fraud are now being investigated by City of London Police and regional forces.

Being able to share intelligence in this way is critical in order to reduce the overall impact on the UK. However, preventing people from becoming repeat victims is also an essential part of the strategy - which is why our partnership with Get Safe Online works to raise the public's awareness of internet safety prevention measures, as well as signposting those people who have fallen victim towards Action Fraud.

Ensuring the safety and efficiency of the UK’s online banking systems, which need to work smoothly 24/7 to present accurate account balances and safely move millions of payments daily, is an ongoing battle. Botnets, phishing and ‘middlemen’ are some of the threats we have to deal with as banks on a daily basis.

We juggle priorities and balance what we say between being reassuring, yet encouraging caution; being confident, yet also being risk aware. However there is no doubt that banks now face more sophisticated threats (often from international organised crime rings) than they did a few years ago.

Malware (aka trojans or viruses) that update 50 times a day pose challenges to security vendors and customers alike. Increasingly banks are relying on stronger authentication, smarter risk engines, and the services of specialist third-parties to present new layers of defence-in-depth.

Security is also seen as a mutual obligation. We will certainly do whatever we need to do, but we also ask our customers to take certain sensible measures. And most of them do. For example to date, our customers have downloaded well over 3 million copies of Rapport, the specialist security software from Trusteer, that complements traditional anti-virus by offering dedicated defences to online banking sites such as ours.

As social media and instant news change our views of the world, the online sphere is rapidly merging with the ‘real’ one. We adjust to these changes by matching new threats with new defences. Our new online reality is also by no means an unwelcome situation; it also provides innumerable benefits of connectivity, pricing and convenience simply unimaginable by previous generations.
Confidence is Key

Andy May, Director of Governance Risk and Regulatory Affairs, Cable & Wireless Worldwide

At Get Safe Online, we are big advocates of the web. Our ethos centres on giving people the tools to make the most of the advantages the online world offers, but be able to do so with confidence.

As with any safety campaign, we have to highlight the risks to get people to sit up and take notice. But critically, the aim is never to scare or deter anyone from going online – in fact, we want to encourage its use.

As such, it is always a concern to hear the extent to which fear of crime can deter some from going online altogether. This year’s Get Safe Online survey indicates that this is the case for 14% of adults in the UK. Though this is a marginal improvement on previous years, when the figure was 17% (2006), this is still too high.

In addition, for those that do use the web, 31% say they avoid online banking, 23% are deterred from shopping online and 16% don’t use social networking sites for fear of falling foul of fraud. With many of us knowing how convenient, enjoyable and pain-free these services can be, it is a great shame to see so many missing out.

Our message is simple. Like most areas of life, crime is a risk when you go online. However, if you understand the risks, know the warning signs to look out for and what steps to take to mitigate the threats, there’s no reason why we can’t all enjoy all the internet has to offer.

---

Get Safe Online’s top advice for surfing with confidence

<table>
<thead>
<tr>
<th>Protect your computer:</th>
<th>Stay vigilant online:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing anti-virus software, anti-spyware software and a firewall</td>
<td>Using strong passwords</td>
</tr>
<tr>
<td>Updating your operating system</td>
<td>Not giving away too much personal information on blogs and social networking sites</td>
</tr>
<tr>
<td>Using up-to-date applications, such as your web browser or word processing package</td>
<td>Activating privacy settings on social networking sites</td>
</tr>
<tr>
<td>Encrypting your wireless network</td>
<td>Not opening email attachments from people you don’t know</td>
</tr>
<tr>
<td>Blocking spam emails</td>
<td>Blocking spam emails</td>
</tr>
</tbody>
</table>
About Get Safe Online

Get Safe Online is a joint initiative between the Government, the Serious Organised Crime Agency (SOCA), public and private sector sponsors from the worlds of technology, communications retail and finance to help individuals and smaller businesses protect themselves against internet security risks and threats. The Get Safe Online website www.getsafeonline.org provides unbiased, trusted, comprehensive information and advice about online safety.

w: www.getsafeonline.org    b: www.getsafeonlineblog.org    t: @GetSafeOnline

Founding Partners

HM Government    HSBC    Microsoft    SOCA

Partners

Cable & Wireless Worldwide    Ofcom    PayPal    Action Fraud

Get Safe Online is a trademark of Endurance (Internet Security Awareness) Limited.