

# UK Internet Security: State of the Nation

## The Get Safe Online Report

November 2011



[www.getsafeonline.org](http://www.getsafeonline.org)

Expert advice for everyone



# Foreword

The Rt Honorable Francis Maude, MP, Minister for the Cabinet Office

It is becoming increasingly difficult to remember life before the internet. People do their shopping and banking, book holidays, and communicate with friends and family – all online.

The internet is a vital part of our economy. The UK is now Europe's leading e-retail economy with sales set to reach approximately £69 billion by the end of this year. The sector is growing at a rate of 18% per annum with an average of approximately £1,144 spent per person.<sup>1</sup>

It is easy to see why this is the case, as the internet is often cheaper, quicker and more convenient than traditional means, offering 24/7 access. Mobiles are increasingly being used for more than just calls and sending text messages, with 39% accessing the internet from a mobile phone<sup>2</sup> in the past year. With worldwide tablet sales estimated to rocket by 400%<sup>3</sup> over the next two years, the internet economy will continue to grow.

Unfortunately, this thriving marketplace doesn't escape the notice of those who would seek to exploit it unlawfully. Criminals have been quick to take advantage of the ease of access to victims and the relative anonymity that the internet affords.

We want to ensure that everyone is able to go about their business online with confidence. Cyber security is a particular priority for this Government and we have put in place funding for a national programme to help give us a competitive advantage in cyberspace.

Working in partnership with industry is an integral part of this work as we all stand to gain from a safe and secure online environment. This is why we are supporting getsafeonline.org alongside private sector partners. The Get Safe Online campaign reaches out to online consumers and gives them the right kind of authoritative and trustworthy guidance on how to use the internet safely.

It is our shared responsibility to make the internet a safe place to do business. We are doing our part in Government and we would ask businesses small and large, as well as individual consumers, to play their part too.

*Francis Maude*



1. Interactive Media in Retail Group

2. Get Safe Online survey, independently carried out by ICM Research in October 2011.

The survey interviewed a nationally representative sample of 1,000 GB adults aged 18+ via CATI [Get Safe Online survey 2011]

3. eMarketer, December 2010



# Cyber Security Takes Centre Stage

Sharon Lemon OBE, Deputy Director e-Crime, Crime Techniques, Prevention and Alerts, Serious Organised Crime Agency

I can't believe that I have been involved in Get Safe Online for nearly seven years. During that time we have had some fantastic events and successes, but without a doubt the most activity and the greatest interest in cybercrime has been during the past year.

As part of the Strategic Defence and Security Review, the Government made Cyber Security a 'Tier One' threat putting it at the heart of the national security strategy. It allocated £650 million to various departments to boost their efforts at tackling cybercrime, including SOCA, the Police Central e-Crime Unit (PeCU) and the National Fraud Authority (NFA). All of these parties are working very closely together, under the guidance of the Home Office, to make the most effective use of this opportunity.

It would be good to think that we could arrest and prosecute every cyber criminal and clean up the virtual environment - but the speed, reach and scale that the internet provides means that this will never happen. While there will always be cases where we need to see people brought to justice, an equally important activity is prevention and awareness.

That is where Get Safe Online comes in – we continue to provide independent, free and contemporary advice and guidance on how people can protect themselves and their businesses online. In the past couple of years, we have run campaigns on bogus ticket vendors, phishing scams disguised as e-cards, malware disguised as anti-virus software, and fake holiday property rentals, to name just a few.

We have also supported the Metropolitan Police in their efforts to mitigate fraud around the London 2012 Olympics. As criminals continue to find new ways to exploit the web, the need to maintain awareness is critical and our job is never done.

Technology has changed so much since the beginnings of Get Safe Online in 2005. Back then, most of our advice was based on desktop machines connected to the internet by a fixed line; now most people also carry a smartphone (or two!) and public WiFi access is an expectation across the globe. Our mission remains the same though – getting everyone to experience and enjoy the virtual environment safely.





# Our Lives Online

James Thickett, Director of Market Research, Ofcom

As a nation we are using the web in more of our daily activities than ever before. Ofcom's Media Literacy research<sup>4</sup> indicates that broad use of the internet has increased in the last couple of years.

In 2009, 38% of internet users could be classified as 'broad' users, i.e. carrying out between 11 and 18 types of internet activity; in 2010, this rose to 49%.

Four in five (81%) adult internet users say they have shopped online – and it appears that we are enjoying the benefits.

Eight in ten internet users (82%) say that they have saved money in the last six months by using the internet, for example comparing prices online or buying online rather than in the shops. Close to half of all internet users (46%) say they have made 'significant' savings by buying something online rather than in the shops.

The popularity of social networking sites also shows little sign of abating. Over half of internet users say they have a social networking profile (54%) compared to 44% in 2009. One half of those with a profile (51%) now use it daily compared to 41% in 2009.

One of the most notable trends, however, is the continuing rise of smartphone use and internet usage on the mobile in non-home locations. According to the latest Ofcom data<sup>5</sup>, over a quarter of adults (27%) and almost half of teenagers (47%) now own a smartphone.

When asked about the use of these devices, 37% of adults and 60% of teenagers admit they are 'highly addicted'. Over half (51%) of adults and two thirds (65%) of teenagers say they have used their smartphone while socialising with others, nearly a quarter (23%) of adults and a third (34%) of teenagers have used them during mealtimes and over a fifth (22%) of adult and nearly half (47%) of teenage smartphone users admitted using or answering their handset in the bathroom or toilet!

As our online activity shifts towards mobile platforms, people need to be even more vigilant about their use of personal data on the internet.



4. Unless otherwise stated, all data in this article is taken from the Ofcom Adults' Media Literacy Report 2011

5. Ofcom Communications Market Report 2011



# Cybercrime in the UK

Anna Sampson, Senior Manager, Direct Marketing,  
VeriSign Authentication Services EMEA, Symantec

As new technologies like mobile transactions emerge, cybercriminals are evolving their techniques to capture and make money from personal information.

The good news is that users are becoming more vigilant – 87% of this year's Get Safe Online survey respondents have virus protection software on their computer, consistent with last year. In addition, we're getting better at keeping this protection up to date, with 41% of people updating their software every time they turn on their computers or within the past week, a 14% jump since last year.<sup>6</sup>

At VeriSign we're constantly trying to educate people about online threats and raise awareness about the dangers of social engineering, which is the main trick used by cybercriminals. With 40% of internet users revealing personal information or other content online that cybercriminals can use to their advantage, it's important for people to think seriously about how they are protected. To help ensure you are surfing safely, some tips and statistics are included below.

## Top Tips:

**Don't be fooled!** – Don't click links that supposedly take you to online shops or deals. Always type the company address into the browser window, or navigate via a search engine.

**Keep your identity safe** – Don't share passwords or choose one that can be easily guessed. Make sure to change them often. Password or PIN numbers protect your mobile phone and tablet device.

**Treble check the URL** – Check the web page where you enter personal information such as your address or credit card details, using sites with data encryption. These sites will have an address starting "https." A green coloured address bar also indicates that the website is has an Extended Validation SSL certificate. This means that the organisation has also been rigorously authenticated and so can be completely trusted.

**Protecting your bank details** – Always look out for the 'padlock' icon at the bottom of the browser frame when making a payment online.

**Up-to-date internet security package** – Security software from a recognised name is the best and safest option when it comes to stopping malicious software" at the end

## Quick Facts:<sup>7</sup>

Cybercrime is costing the UK on average **£474 million** a year

**19 people** fall victim to cybercrime every minute in the UK

**51%** of those in the UK have experienced cybercrime in their lifetime

**3 times** as many Brits have been victims of online crime in comparison to offline crime in the last 12 months

6. Get Safe Online Survey 2011

7. Norton by Symantec Cybercrime Report 2011



# Mobile Malware Intensifies

Rik Ferguson, Director of Security Research & Communication, Trend Micro

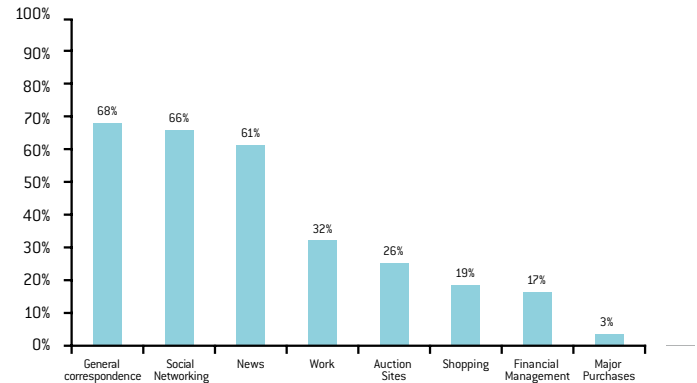
2011 has been the year that mobile malware has come of age. Criminals are putting increasing time and resource behind exploiting the rich functionality of today's smartphones.

Increased bandwidth and the unlimited use packages offered by network operators means mobile web has become commonplace over the last two years. As such, use of smartphones for online banking, shopping, social networking and other activities involving our personal information - previously the domain of our desktop computers and laptops - is increasing. Criminals are driven by consumer behaviour, and as the money-making opportunities move to mobile platforms, fraudsters are following.

One of the major triggers has been the popularity of smartphone applications (apps), which are now being exploited to trick users into downloading malware. Some form of social engineering may be involved to entice users to download malicious apps, for example under the guise of additional 'free' levels to popular games, or increasingly we see legitimate apps being "trojanised" and reuploaded to marketplaces by criminals. Once downloaded, criminals can then gain access to the victim's phone, enabling them to steal data, send and intercept communication and download further malware. With users now installing and removing apps with increasing frequency, this overall volume means the chance of encountering a rogue app is now higher than ever before.

The volume of mobile malware has not yet reached the epidemic proportions of computer-based malware, but criminal interest is clearly there and growing. We are seeing multi-platform attacks distributed by the same criminal groups that traditionally have focused on conventional systems. Smartphone security, such as encryption and anti-malware, is available but not widely deployed. The need is already there for it to be commonplace.

**Figure 1: Mobile Web Use**





# Zero-day: Behind the Headlines

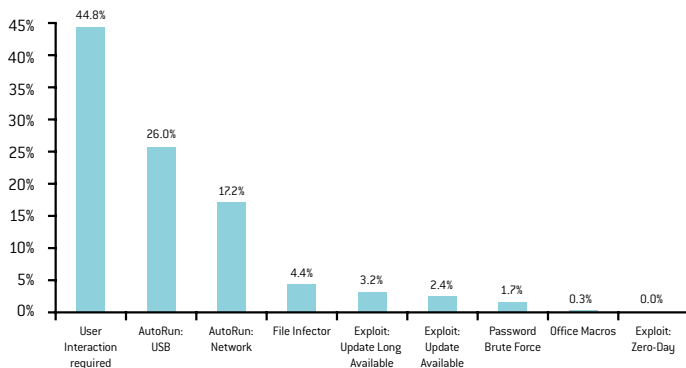
Stuart Aston, Chief Security Advisor, Microsoft UK

The latest 'zero-day' exploit is rarely far from media headlines. These exploits take advantage of software vulnerabilities for which no update exists – typically carrying out attacks in the narrow window between being detected and being 'patched' by software engineers.

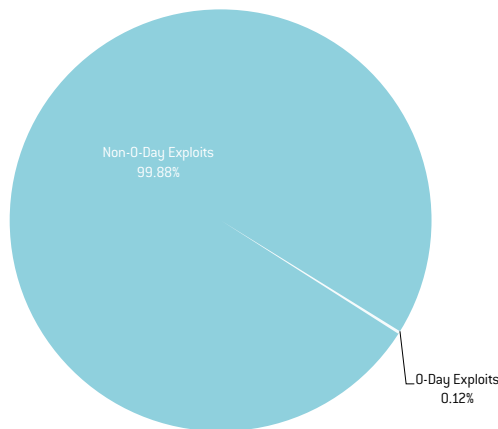
Latest research from Microsoft<sup>8</sup> indicates that approximately 6% of infections detected in the first half of 2011 were due to software exploits (see figure 1). Of this, zero-day exploitation accounted for only for 0.12% (see figure 2). So, although potentially damaging, zero-day threats are only a small part of the overall security picture.

The risk represented by zero-day exploits is real and should be factored into everyday security measures. This new information can help you prioritise how to approach IT security - for web users, this means keeping anti-virus software up to date, not opening attachments in unsolicited emails and regularly downloading security updates for all software.

**Figure 2: Malware detected by the Microsoft Windows Malicious Software Removal Tool, Jan-June 2011, categorised by propagation methods**



**Figure 3 : Percent of zero-day exploits, Jan-June 2011**



When it comes to consumer education and awareness, perhaps what is more interesting is the number of infections that rely on user interaction to allow them to infect systems. Figure 1 shows that these infections accounted for almost 45% of attacks, making it by far the most 'popular' method to spread software infections.

Criminals are continuously developing new ways to trick users into 'allowing' malware to be downloaded onto their computers. Ensuring web users are aware not only of the latest threats and scams, but also how they are spread, will enable us all to be more vigilant while online.



# Live Events Become Big Business

Rob Skinner, Head of PR, PayPal UK

Online ticketing fraud has become hugely lucrative for criminals. Research from the National Fraud Authority indicates that the loss from online tickets is estimated at £168 million.

Although the internet provides a great resource for consumers looking to secure sought-after tickets while providing them with the luxury of browsing for events without facing huge queues, there is sometimes a need for caution. Criminals are going to increasing effort to dupe consumers into visiting fake ticketing websites, running their operations as 'businesses' and willing to make up-front investments for high returns. Cyber scammers will often pay for search advertising so that their fake sites appear at the top of event search results. They are also known to enlist professional web designers so that their sites appear genuine.

According to Get Safe Online research<sup>9</sup>, more than 1 in 10 people (or their friends and family) have been a victim of a ticketing scam online. With 38% of people turning to the internet to get hold of tickets to sold-out events, criminals also play on the emotions of those desperate to see their favourite artists. One method used by scammers is to target music fan websites and forums and other social networking sites. Posts will be displayed from 'fans' claiming they have bought tickets from a certain site, encouraging those not yet successful in obtaining tickets to visit it. More consumers are then driven to the fake site and more genuine fans fall for the scam.

Earlier this year, Get Safe Online ran an awareness campaign with the City of London Police. During the programme, Detective Chief Superintendent Steve Head, who runs its Economic Crime Directorate, highlighted the lag time between purchasing and receiving tickets as a key issue, allowing fraudsters the time to set-up professional looking sites to lure fans in.

The longer the time lag, the greater the potential risk of non-delivery for consumers. The City of London Police is working with the ticketing industry to make changes to this practice so that tickets are issued as quickly as possible, not just right before the event.

As always, however, consumer education goes a long way and simple measures can do much to avoid falling foul of the fraudsters. In addition, the usual rules for making safe, secure payments while online still apply. Consumers need to remember that if an offer for tickets seems too good to be true, then it probably is.





# Guarding Your Online Wallet

Nick Staib, Senior Manager and Security and Mobile Specialist,  
Digital Solutions Centre of Excellence, HSBC

Like many online businesses, banking is continually re-inventing itself. It has adapted to changing consumer demands, and has become something we do whenever we wish, rather than something conducted in a building, during set opening hours.

On the back of the explosive growth in broadband access, it is no surprise that internet banking grew from a niche channel to the principal way in which customers interact with us. In fact, this year's Get Safe Online research found that 65% of us use the internet to manage our finances, which includes anything from banking to paying bills to making transfers and purchases, almost a 20% increase over the past four years.<sup>10</sup>

With multiple millions of online banking transactions being made, it is inevitable this facet of the internet would become a ripe target for international fraudsters. The story of online banking is therefore also one of a secret 'arms race', where increasingly sophisticated threats need to be countered with ever smarter methods of protection for our consumers and their bottom lines.

Not that long ago, security experts explained that we needed 'smart' passwords, which were difficult to guess. This is no longer adequate for a banking site. With the advent of sophisticated spyware that targets banks, avoids detection, and captures keystrokes, passwords began to be captured despite their length and complexity. Additionally, we also started to see hundreds of 'phishing' sites trying to trick customers into handing over these passwords.

**Did you know...65% of users manage their finances online in some way? And 16% have used the internet to make a major purchase, like a property or car.**

HSBC, like many banks, absorb resulting internet losses to protect customers, but also recognise a duty of care for the privacy of our customers' financial information. In the face of such threats, and in parallel with better fraud detection systems, we have been sending our customers our new SecureKey that can generate dynamic or 'one-time' passwords, as well as electronically sign payments to new beneficiaries.

Coupled with the widespread use of advanced anti-spyware software provided by banks, as well as the excellent advice from Get Safe Online, HSBC believes our online customers are now safer than ever. It is inevitable that for this facet of the internet, tomorrow's challenges will almost certainly revolve around the fledgling mobile banking and mobile payment services. As ever the balance between convenience and security will be critical, but I'm convinced that banks will rise to these challenges, as the mobile reinvention flourishes, and as we continue to protect customers.



10. Get Safe Online Survey 2011



# Gathering Intelligence

Peter Wilson, Director, National Fraud Authority

'As Sharon Lemon notes [page 3], the Government has put cybercrime high on the national security agenda. As part of this effort, it has tasked Action Fraud – the UK's national fraud reporting centre, run by the National Fraud Authority – with providing a single reporting centre for online crime.

The data collected by Action Fraud is fed directly into the National Fraud Intelligence Bureau (NFIB) at the City of London Police. By providing a central point to report everyday fraud, a national picture develops to aid law enforcement efforts. Research from the NFA estimates, for example, that the fraud loss associated with online ticketing is £168 million<sup>11</sup>. Earlier this year, the centre received reports of fake concert tickets for the popular music act, Take That. Intelligence gathered from those reports led the police to take action against a particular ticketing website, which was subsequently shut down.

In the same way, crime reported to Action Fraud enables us to identify which particular types of online fraud or scams are causing the most harm. One commonly reported scam has involved cold calls claiming to be from a genuine technology vendor, alerting consumers that their computers have been compromised and tricking them into downloading anti-virus software which is actually malicious software in disguise. Last year, this led Get Safe Online to run a national media campaign to alert UK web users to the warning signs. During the week following the campaign, Action Fraud received over 200 calls from consumers who recognised the scam and wanted to report it.

Now, we are working to capture even more intelligence from the public. When consumers contact Action Fraud, they are sometimes reporting incidents that don't always carry enough detail to meet the criteria of a full crime report, but may provide information which could be useful to the police in their investigation. As such, the centre's online reporting tool now includes an information reporting module to help the public share what they may know. This data can be used by police to create 'crime packages' to help prosecute fraudsters.

Action Fraud will also provide a central point for law enforcement. Over the next year, police forces in the UK will submit crime reports relating to fraud and cyber crime through the online reporting tool. This important development will ensure that all fraud crime reaches the NFIB and can be used to inform law enforcement efforts.



# Using Online Marketplaces Safely



**Katie Kitiri, Head of Trust and Safety, Gumtree**

This year Get Safe Online's annual survey found 72% of UK internet users use the internet to shop, and 52% are using auction sites to sell their goods and services to others. The speed, convenience and value for money offered by online trading helps with

its popularity, but unfortunately it can also mean that fraudsters want a slice of the action too.

When buying online from an individual or smaller retailer it can sometimes be difficult to know if they are reputable, but there are lots of tricks and things to look out for to ensure that you have a smooth and trouble-free process.

Just like all other activity online it is important to:

- Use a well-known and reputable site
- Read and understand the buyer and seller policies
- When trading remotely with someone online, conduct appropriate background checks before completing a sale or purchase, by checking ratings from other users or using search engines to probe for any negative or worrying information. And use the safest method of payment recommended by the site
- When trading locally with a buyer or seller who you have met online, always do so in a public place and let someone else know where you will be

Thankfully, for the vast majority of people the internet is a useful and easy place to sell items and for others to purchase needed goods - but it is always beneficial to take precautions. A few moments spent doing a background check is far less time consuming than dealing with fraud once it has happened.

## Consumer Confidence



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

Consumer attitudes to the internet have evolved with online activity. A decade ago, many consumers' computer use was spent in safe forums, with internet service providers (ISPs), anti-virus software and other technology being sufficient to protect their experience.

With the evolution of the internet and more social, financial, and professional exchanges taking place online than ever, online threats have not only increased but also changed in nature.

Mobile, tablet and console internet usage is also a new and growing indicator of how comfortable the consumer is with a lifestyle where the internet is the norm. Recent surveys suggested usage of alternative devices for browsing has increased by as much as 20% - convenience has always been a winner!

This comfort many of us now feel when online is often reflected in how we interact online. For example, many of us are happy to 'broadcast' what we do in our personal and professional time through social networks.

Our latest research indicates that almost a quarter of web users (24%) still share confidential or personal information such as phone numbers and email addresses when online, despite the fraud risks this can contribute to.

16% of UK web users also open attachments in emails from unknown sources, another action which carries potential risks. At the other end of the spectrum, the presence of online criminals has deterred users from fully utilising the internet. Over 10% avoid social networking, and nearly 20% avoid online banking or other forms of financial management. Furthermore, 11% avoid using the web altogether.<sup>12</sup>

Although online crime is a very real threat, the internet's benefits can be enjoyed as long as the appropriate protective measures are taken. This starts with protecting your computer, but also involves understanding and recognising the threats when engaging online.

Although there is still work to be done, this is compared with 21% in 2007, so the signs are encouraging.

## 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](http://www.getsafeonline.org) provides unbiased, trusted, comprehensive information and advice about online safety.

w: [www.getsafeonline.org](http://www.getsafeonline.org) b: [www.getsafeonlineblog.org](http://www.getsafeonlineblog.org) t: @GetSafeOnline

### Founding Partners



### Partners

