# UK Internet Security:

# State of the Nation

## Get Safe Online Report

November 2009

Expert advice for everyone

# Introduction

## Tony Neate, Managing Director, GetSafeOnline.org

**As the Get Safe Online initiative enters its fifth year we continue to witness the positive impact that the internet has on the daily lives of people and businesses in the UK. Communication, shopping, auctions, banking and entertainment are being done online by more and more people, and the rise in popularity of both social and business networking means that personal and commercial worlds online are converging.**

At the very heart of GetSafeOnline.org is our belief in the need for collaboration, education and sharing best practices to prevent internet crime – across law enforcement, government and industry – as well as placing knowledge and tools directly in the hands of every internet user so that they can protect themselves.

But we have to recognise that there are still many people who do not yet benefit from being online, or do not enjoy all the opportunities that digital participation offers. Part of Get Safe Online's remit and passion is to ensure that the negative aspects and risks of the internet do not contribute to digital exclusion, and that any such fears are mitigated so that trust and confidence in the internet can contribute to the UK's objective of full digital engagement in the future.

The Get Safe Online initiative continues to educate individuals and smaller businesses to become more capable, confident and safe online, by raising awareness of internet security risks and threats, and providing advice about how to avoid them. There has been a notable increase in protecting PCs with the essential anti-virus and anti-spyware tools, but one of the barriers to motivating people to take proper precautions online is still that the risk of internet fraud can feel very remote and unlikely to happen to them.

This report sets out some of the findings from the latest GetSafeOnline.org[1] research, and includes analysis and commentary from our sponsoring partners – examining the UK's internet usage, key areas of threat, and current attitudes to online safety.

We hope you find it informative!

GetSafeOnline.org

HM Government HSBC

Microsoft SOCA Ofcom

Cable&Wireless PayPal

[1] Unless otherwise stated, all figures taken from the 2009 Get Safe Online survey by ICM Research. 2008 and 2007 figures from previous comparable Get Safe Online surveys also by ICM Research.

# Our lives online

Since the last Get Safe Online Report, one of the most significant factors affecting our daily lives is the economic downturn. While there are some signs that this is influencing our online behaviour – for example, almost half of internet users (**47%**) say that they now will only buy online from trusted brands – over a third (**34%**) say that the recession has made no difference to their online behaviour.

Indeed, this year's Get Safe Online survey indicates that online activity is increasingly an integral part of everyday life. For example, **70%** now make purchases online compared with **61%** in 2007. Similarly, **60%** use the internet for financial management – including banking and paying bills – compared to **47%** just two years ago.

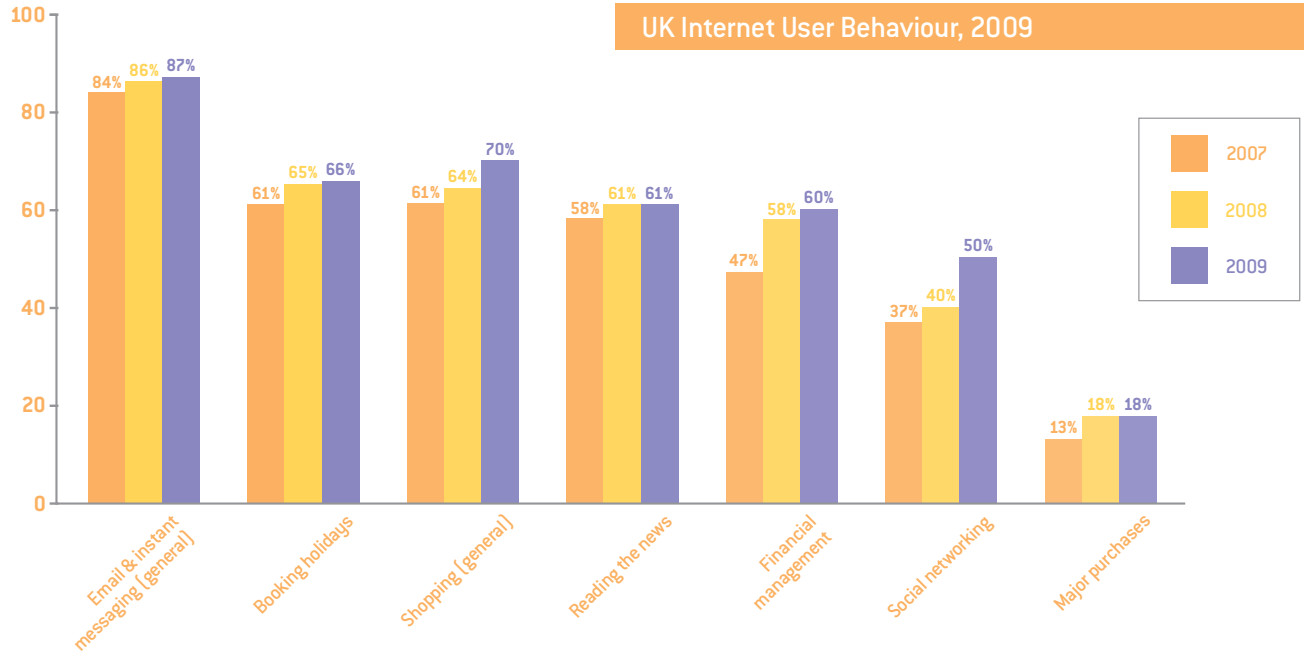
The use of mobile devices[2] to access the web is also becoming a growing part of our online activity. Over 1 in 4 (**28%**) of us now access the internet this way, led by 18-24 year olds for whom the proportion rises to **50%**.

While the primary activities are email and messaging (**71%** of mobile internet users), **56%** access social networking websites, **21%** use auction sites such as eBay and **19%** shop via their mobile device.

While the potential threat landscape for mobile devices is still emerging, there are some indications that greater security vigilance is required. For example, **67%** do not secure their handsets using the PIN or password function and 1 in 5 (**20%**) have lost their device or had it stolen. At the same time, **20%** synchronise their mobile devices with a desktop or laptop, meaning they potentially carry a wealth of personal information.

The popularity of social networking continues to rise with the survey revealing a **10%** increase in use since 2008, with half (**50%**) of UK internet users using Facebook, Twitter, MySpace and other such websites.

## UK Internet User Behaviour, 2009




[2] Mobile devices include mobile phones, smart phones, iPhones and Blackberrys

# The threat landscape

Cliff Evans, Head of Security & Privacy, Microsoft UK

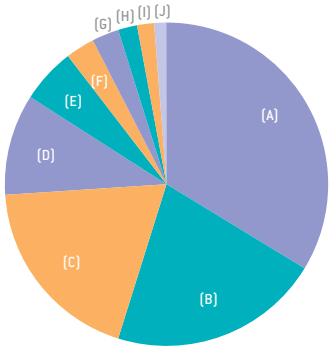
In an ever-changing global security landscape, it is essential that all internet users – from consumers to multi-national businesses – are aware of emerging threats and can make informed decisions to maximise their protection against them. In recent years, significant progress has been made in protecting against online threats, but with criminals continually developing new malware, trojans and other threats to compromise PC security, there is no room for complacency.

Microsoft's recently published Security Intelligence Report[3] indicates that while rogue security software is still a major threat, infection rates have levelled off – declining by **20%** in the last six months. However, in its place there has been a notable resurgence of worm attacks – with almost a **100%** increase in the second half of 2008 – which have become the second most prevalent threat detected in the first half of 2009. In particular, the top worm threat globally is Conficker – found on the internet more than ever before. This worm uses several methods to disseminate itself that work most effectively within a firewalled network environment.

Compared to trojan-like attacks, worm threats rely on access to unsecured file shares and removable storage drives. This makes them more of a threat in the business environment than in the personal one, but it does mean that we all need to be more vigilant in updating our operating systems via automatic updates and using the latest anti-malware security. In addition, despite the notable growth in worm attacks globally, the most dominant threats in the UK are trojans and adware, accounting for **33.7%** and **21.1%** of infections respectively, meaning individual PC security is as vital as ever.

With economic recession still engulfing the UK, we can only anticipate intensified efforts by criminals to capitalise on vulnerabilities and exploit potential weaknesses. It is critical that we all maintain efforts to deploy the most up-to-date methods against the latest threats.

## UK Malware and PUS* by Category (listed in clockwise order)




* Potentially unwanted software

- 33.7% Misc trojans (A)
- 21.1% Adware (B)
- 19.1% Trojan downloaders and droppers (C)
- 10.1% Misc potentially unwanted software (D)
- 5.5% Worms (E)
- 2.9% Backdoors (F)
- 2.7% Password stealers and monitoring tools (G)
- 1.9% Viruses (H)
- 1.7% Spyware (I)
- 1.2% Exploits (J)

[3] All figures in this article taken from the Microsoft Security Intelligence Report Volume 7, published November 2009. Based on data collected January – June 2009, with comparisons drawn with data collected July – December 2008.

# Safe in the knowledge

Phil Male, Operations Director, Cable & Wireless Worldwide

It is encouraging to see that this year's Get Safe Online survey results show 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. In fact **86%** of respondents state that they have up-to-date virus protection software, and almost half (**47%**) of those people update their anti-virus software when they switch their computer on or update it very regularly (within the past week).

Only **2%** of respondents state that they do not have any security measures installed on their PC and the main barrier to doing so is a lack of time (**16%**, compared with **9%** in 2008) or cost (**11%** compared with **8%** in 2008). Interestingly, the main reason for not installing security measures in 2008 was a lack of knowledge of what these measures are (**19%**), which has since reduced to only **7%**.

The large number of people who have installed security software on their PCs and laptops may contribute to the relatively low feeling of risk that people have about internet crime. According to the survey, only **14%** feel most at risk from internet crime in their daily lives – the same percentage as those who are concerned about burglary – compared to **32%** who feel at risk from offline bank card fraud. Yet over half (**56%**) of those asked say that they, or their close friends, family or colleagues have been the victim of some kind of internet crime.

The most prevalent internet crimes cited by respondents to the above question are virus attacks to the PC (**34%**), phishing attacks (**22%**), online identity theft (**21%**, up from **15%** in 2008) and scam emails or websites (**15%**). And, while internet users may feel more concerned about bank fraud and other offline crimes, these internet offences exact a high price – with **29%** of people who stated they have fallen victim to these fraudsters estimating that the personal financial cost to them was over £2,000; rich pickings for internet criminals when they are successful at scamming consumers!

**Impact: Key Numbers**

**Number of UK internet users who have been victim of:**

| | |
|---|---|
| Computer virus attack | 34% |
| Phishing | 22% |
| Scam email or website | 15% |
| Identity theft | 21% |
| Computer hacked | 10% |
| Harassment/bullying | 8% |
| Social networking site hacked | 7% |

# Security and safety habits

Garreth Griffith, Head of UK Risk Management, PayPal

Technical computer security is paramount to protecting against a swathe of internet crime, but it is equally important that we remain vigilant ourselves while using the internet. All the software in the world cannot protect against fraud if you end up 'giving' personal information away yourself.

What is encouraging, however, is that web users appear to be taking on board messages about internet security, and are beginning to improve their online safety habits and behaviours. The 2009 Get Safe Online survey reveals they are increasingly aware of dangers such as opening email attachments from an unknown source. This year, only **15%** of respondents admitted to having done this, compared with **17%** in 2008 and **24%** in 2007.

This positive trend seems also to be reflected in other key areas of risk. For instance, the proportion that use different passwords to access password-protected sites is showing a positive, albeit slow, move in the right direction – with **31%** in 2007, **32%** in 2008 and **33%** in 2009. That said, **17%** still use the same password for every site they access showing there is plenty of room for improvement. And as we move increasingly towards accessing the internet through mobile devices, figures show that more than two-thirds of us (**67%**) avoid using the PIN and password function on mobile devices.

When it comes to online scams, our research shows there are still areas where progress is needed. For example, almost 1 in 7 people [**15%**] say they or a close friend/family have fallen victim to a scam email or website. Although better known about now, these scams are also becoming increasingly sophisticated. Today, we are a long way from misspelt emails and unprofessional-looking scam websites – but even the most security-savvy web users can be fooled unless they are constantly on their guard. Ongoing vigilance and education are the best defence for staying a step ahead of the criminals.

**20%** have listed confidential personal information, such as their phone number, online

**15%** still open email attachments from unknown sources

**12%** do not use privacy settings on social networking sites, or don't know what they are

**22%** have experienced a phishing attack

Over **1 in 5 (21%)** have been a victim of online identity theft

# The rise of social networks

Robin Blake, Head of Media Literacy, Ofcom

In the last five years, one of the most significant impacts of the internet on our daily lives has been the proliferation and popularity of social media, taking into account the whole spectrum of blogging, micro-blogging, chat rooms, social networks and forums.

Recent research carried out by Ofcom[4] shows almost twice as many people have a social networking site profile in 2009 compared to 2007 (**38%** up from **22%**). Some **41%** of users now say they use a social networking site daily, compared with **30%** two years ago, while **26%** contribute comments to somebody else's blog.

The research also highlights some interesting gender differences in internet use. Men are more likely to use the internet at least weekly to read the news (**27%**, compared with **16%** of women), while women seem more socially inclined with **39%** using the internet for social networking on a weekly basis compared to **28%** of men.

There's no doubt that these online networks have opened up new opportunities to share knowledge, ideas and common interests in a way that would otherwise be impossible. However, openly sharing details of our personal lives online can pose potential security risks. Although these details may seem harmless, they can make life significantly easier for identity fraudsters; being able to find a date of birth or home address on an online profile can be the final piece in a jigsaw puzzle that allows them to set up a credit card in someone else's name.

The good news is that there is an increased level of awareness of the potential risks and how to avoid them – as well as clear changes in behaviour to mitigate them. For example, three quarters of those with a social networking profile (**78%**) now say that it can only be seen by family and friends, a significant increase from **48%** in 2007.

Internet users appear also to be less willing to provide personal information online in general than was the case in 2007; one in five (**21%**) say they would never enter their credit card details online, and nearly one quarter (**23%**) say they would never share their mobile phone number, up from **17%** and **19%** respectively.

All in all, rather than limiting use, making internet users aware of the tools and information available to help them avoid risks seems to be the key to allowing people to fully enjoy the benefits of online social networks.

[4] Ofcom UK Adults' Media Literacy, interim report, 2009. The research involved 812 in-home interviews with adults aged 16 and over from April to May 2009 and is designed to give an accessible overview of media literacy among UK adults aged 16 and over.

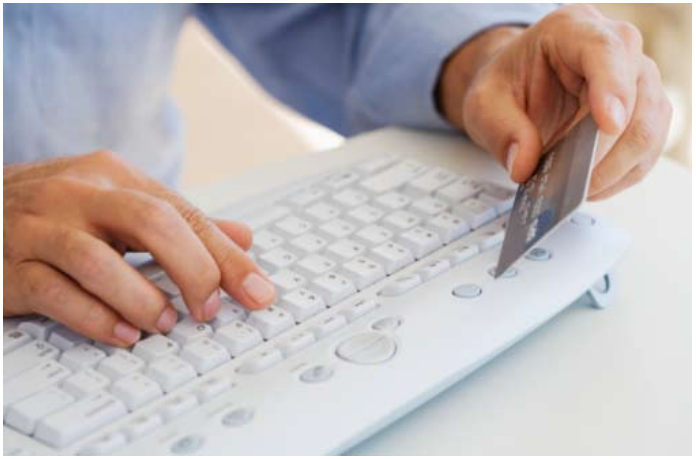
# Safer online banking

Nick Staib, Senior Manager, Digital Security & Mobile Banking, HSBC

From the perspective of a major global bank, we are witnessing the alarming 'industrialisation' of criminal activity in international internet fraud. Fraudsters' techniques have developed from primitive phishing emails with more than a few spelling and grammar mistakes, to very plausible messages that even have our own experts looking twice at them. And the proliferation of malware (malicious software) targeting online bank accounts now ranges from log-on details taken from the unwary to money being moved in amounts designed specifically – but usually unsuccessfully – to evade our security systems.

Online fraud has grown from an occasional incident to a fully-fledged 24 hours a day, 7 days a week 'cat and mouse' operation with the banks' expert security teams being driven to use ever more sophisticated techniques to keep up with, and be one step ahead of, the criminals. Our global teams work around the clock to keep online banking as safe as it must be – whether our customers are at work or at home. On a good day we can get phishing sites closed down before the associated emails are even sent out. On a bad day we pay the price of guaranteeing that our customers won't lose their money.

What it comes down to is a balancing act between conflicting factors; the desire to make things as intuitive as possible for customers, yet fiendishly hard for fraudsters. The aim is always to avoid as much 'hassle factor' as possible but still make customers feel safe and secure. Like many banks we are considering the benefits of two-factor



authentication, which usually involves a gadget creating a one-time password. Such dynamic passwords will almost inevitably be used right across the UK for critical websites such as online banking.

Online security is recognised as a major concern for many, but we also know that it is convenience that drives internet usage and growth. The path that we ultimately choose is derived not just from the advice of experts, but through consulting and understanding the needs of our online banking customers.

# Crime in a virtual world

Sharon Lemon, Deputy Director e-Crime, Serious Organised Crime Agency

One of the most difficult challenges we face in the e-crime world is convincing people that internet crime is a serious reality. There are no piles of drugs, no blood and no immediately obvious signs to indicate the severity of the crime; instead, the scene of the crime is a keyboard and monitor, the image of which does little to indicate the potential harm.

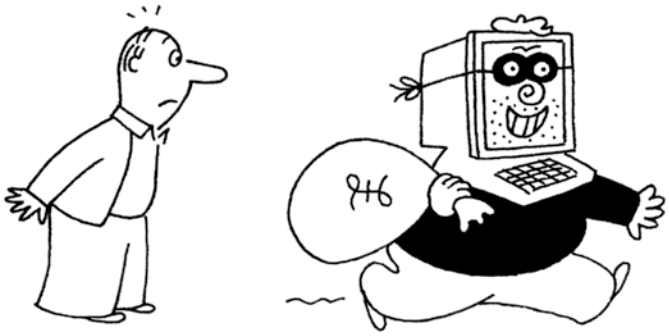
There is an additional challenge brought about by the language which surrounds online crimes – phishing, hacking, DDOS, botnets, to name just a few. These terms alienate the everyday users of the internet and reinforce the perception that online crime is nothing to do with real life but is something that happens in a different world to somebody else.

The fact is that crimes committed in the virtual world are exactly the same as those committed in the real world, just without the face-to-face experience. Financially-motivated crimes such as theft, fraud and extortion, and personal attacks including bullying or using social networking for criminal purposes, can destroy lives whether online or offline.

Most offline crimes now also take place online; the speed and reach of the internet, together with its perceived anonymity, provide new opportunities for criminals. We are witnessing new infrastructures, where criminals work with individuals all over the world, some of whom they have never met. All they know about each other is their nickname, but unrestricted by geography or scale, they can build networks which bring together all the necessary skills and manpower to enable them to carry out crime on a major scale.

Luckily, it is not a one-way street. Law enforcement is also reaping the benefits provided by the internet. By working with international law enforcement partners, we can take a global approach to tackling internet crime – sharing intelligence, knowledge, tools and techniques to make the greatest impact in order to catch and prosecute the fraudsters.

Of course, we cannot do this alone – which is why SOCA's role in the Get Safe Online initiative is a critical part of the work we do everyday. It's the 'neighbourhood watch' principle. To tackle internet crime effectively, we all must take responsibility for protecting ourselves and each other online – government, law enforcement, the public sector, the business community and every individual internet user. The straightforward advice provided by Get Safe Online means that this is something every one of us can do.



# Get Safe Online's Top Tips for Safer Surfing

| Protect your PC | Avoid online rip-offs | Take care of your identity and privacy |
|---|---|---|
| Use anti-virus and anti-spyware, and make sure your firewall is turned on | When you're shopping online, look for clear signs that you're buying from a reputable company | Use an up-to-date web browser |
| Keep your computer's operating system and applications updated | On an online auction site, learn how it works and learn to pick good sellers | Always use strong passwords |
| Block spam emails and never open any attachment received from an unknown source | Use safe ways to pay, such as a secure payment service, or credit and debit cards | Don't use the same passwords for all websites, especially financial and banking websites |
| Use an up-to-date web browser and a pop-up blocker | Look for evidence of a physical address and telephone contact details | Activate privacy settings on social networking sites |
| Make regular backups and store them separately from your computer | Be wary of anything that is offered in an unsolicited or spam email | Don't give personal or financial information on blogs or social networking sites |
| Secure your wireless network with a password | Use your common sense to avoid scams – if it sounds too good to be true, it probably is! | Use good judgement – if you wouldn't tell someone in the street, don't tell them online! |

Get detailed advice on all the above at **www.getsafeonline.org**

## 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.

Sponsors

HM Government HSBC Microsoft SOCA Serious Organised Crime Agency

Cable&Wireless Ofcom PayPal

GET SAFE ONLINE .org