Introduction

Tony Neate, Managing Director, GetSafeOnline.org

“The internet is now an integral part of daily life for the majority of people and businesses in the UK – and many of us can’t imagine life without it. Understanding the threats, and taking steps to minimise the risks, is becoming a natural part of our online behaviour. With internet crime, however, there is no room for complacency; a vigilant approach has never been more important.

Get Safe Online is the UK’s leading source of unbiased, user-friendly advice about online safety for consumers and micro-businesses. A joint initiative between HM Government, the Serious Organised Crime Agency (SOCA), HSBC, Microsoft, Cable & Wireless, PayPal and Symantec, the campaign is now in its fourth year. We continue to raise awareness of the risks of the internet, and to educate individuals and smaller businesses to become more capable, confident and safe online.

The good news is that growing awareness of both the risks and the benefits means that more people are enjoying the virtual world, and all the positive things that come with it. But as our use of the internet evolves, so the methods of criminals adapt to keep pace. It is the responsibility of everyone, therefore, to ensure they are aware of these threats, and have taken steps to protect themselves against them.

This report sets out the latest research¹ from GetSafeOnline.org – including valuable analysis from our sponsors – examining the UK’s internet usage, key areas of threat, and attitudes to online safety. We hope you will find it an interesting read.”

¹ Unless otherwise stated, all figures taken from the 2008 Get Safe Online survey by ICM Research. 2007 and 2006 figures from previous comparable Get Safe Online surveys also by ICM Research.
The 2008 Get Safe Online survey shows that UK citizens are increasingly confident about using the internet for everyday activities. A third (33%) of UK internet users spend between one and two hours a day online; and almost one in six (15%) spend three to four hours a day surfing the web. Only 4% stated their use as ‘rare’, while 3% of internet users do not have access to a computer at home.

More than half (58%) use internet banking or other online tools to manage their finances, an increase of 6% compared to 2006; and nearly two-thirds (64%) are online shoppers, with a notable increase in the number using the internet to make larger transactions. 65% are now buying holidays online, up by 30% compared to 2006; and almost one in five (18%) use the internet as part of making major life purchases such as property or cars, an increase of 11% on two years ago.

Since the launch of Get Safe Online in 2005, also noticeable is the increased popularity of newer online activities such as social networking. A relatively unknown phenomenon five years ago, this has radically changed our way of communicating. 40% of UK internet users network online, an increase of 6% compared to 2007, though it is most popular among 18-24 year olds where the figure is 70%. While it may be becoming more socially acceptable, online dating is still a relatively low level activity, with only 4% having tried it.
Preventative Measures

Encouragingly, 85% of UK internet users today have some form of virus protection software. Though this figure has been relatively stable over the last two years, significantly, the frequency with which this software is updated by users has risen. More than half (52%) had updated their antivirus software in the last month, compared to just over a third (38%) two years ago. There is, however, still room for concern – the proportion of internet users who do not take this basic preventative measure remains worryingly high, with 36% admitting to having been the victim of a virus attack.

84% of respondents have a firewall in place, but other basic measures such as anti-spyware and anti-phishing software are being used less frequently (77% and 53%, respectively).

Of those who hadn’t taken basic measures such as these, almost one in five (19%) said it was because they did not know what they were. On a positive note, cost appears to be less of a significant factor than in previous years – only 8% cited this as a problem in 2008, compared to 21% in the previous year.

Software alone is not sufficient, however. Our own behaviour and decisions online can put us at increased risk. 17% admit to opening email attachments from an unknown source, though this is an improvement on the 23% in 2006.

Identity theft is a growing issue and it appears that we are making fraudsters’ lives easier than we should be – almost a quarter (23%) of internet users have posted confidential or personal information about themselves online, and more than two-thirds (66%) use the same password for more than one website; with 46% using the same 2 to 3 passwords for every website they access.

<table>
<thead>
<tr>
<th>The Impact: Key Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>The number of UK internet users, or someone they know,</td>
</tr>
<tr>
<td>who have been the victim of:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Computer virus attack</td>
</tr>
<tr>
<td>Phishing</td>
</tr>
<tr>
<td>Scam email or website</td>
</tr>
<tr>
<td>Identity theft</td>
</tr>
<tr>
<td>Computer hack</td>
</tr>
<tr>
<td>Harassment/bullying</td>
</tr>
</tbody>
</table>

23% of UK internet users fell victim to phishing attacks in 2008, compared to 8% in 2007.
"Threats in the virtual world are becoming increasingly sophisticated and complex. Random phishing attacks sent to all and sundry in the hope that a few individuals will respond are no longer the primary concern – today’s attacks are targeted, organised and professional. At the same time, crime formerly conducted off-line has rapidly moved online, and now frequently operates in both worlds. Identity fraudsters, for example, ‘harvest’ personal data by intercepting victims’ post as well as looking online to find or buy other information.

Adding to this complexity is the fact that the internet is always changing and developing – the increasing popularity of social networking sites in the last few years is a prime example. These areas of growth are also new opportunities for online criminals, who are constantly diversifying their activity.

Online crime can be extremely profitable, too. Contrary to their popular ‘geek’ image, many attacks by hackers – particularly to corporate sites – are all about the money. Some recent attacks have seen the personal data of more than 45 million\(^2\) individuals being compromised. With the right tools – which can be easily obtained online if you know what you are looking for – basic data can be translated into hard cash.

That said, online criminals have to be quick, and increasingly so. The combined efforts of individuals, the private and public sectors, and law enforcement are preventing these data from being worth much for very long.

By following advice from sites like www.GetSafeOnline.org, consumers are becoming more aware of the threat, being more cautious about where they shop online and keeping a closer eye on their transactions.

Banks’ fraud departments are constantly monitoring accounts for unusual activity and are increasingly quick in alerting customers and taking immediate action. At the same time, law enforcement is using the power of the internet to work quickly and efficiently across borders, to arrest offenders, dismantle websites and take actions which prevent the online criminals being effective.

We must all continue this combined, effective action to let the cyber-criminals know that there is no place to hide.”

“What was once a great story device for film makers has, in the internet world, become part of our everyday vocabulary. ‘Identity Theft’ is big business for criminals. Whether it’s your address or your mother’s maiden name, even the most trivial pieces of personal information can be incredibly valuable when joined together.

While many enjoy the convenience of online banking, customers face attempted identity theft in many ways. ‘Phishing’ emails, where users are led to counterfeit websites in an attempt to get them to disclose private information such as passwords, can be a regular nuisance in our inboxes. Alternatively, more serious forms of ‘spyware’ lurking on a family computer are capable of recording every username and password typed, along with every credit and debit card used for purchasing online bargains.

Whatever the method, these tactics help fraudsters build a comprehensive profile – creating a ‘virtual customer’ whose tattered reputation, after multiple credit cards have been maxed out, damages the real victim.

The good news is that, with dedicated 24/7 fraud teams and international co-operation, banks do much to protect their customers and stop criminals in their tracks. However, there’s never room for complacency.

Part of the battle with identity theft comes down to technology, making sure your computer has the right software to guard against viruses, spyware and the like, and that it is regularly updated. However, the other part is very much down to our own behaviour.

Internet users need to know what the danger signs are so they can spot a phishing email at once, and be cautious about posting personal information online, such as on networking sites, where it’s easy for fraudsters to find. We mustn’t forget the things that banks have been telling us for years – don’t share your PIN and online passwords with anyone, and don’t write them down!

GetSafeOnline.org provides internet users with crystal clear advice on protecting their identities. Our advice to our customers and all internet users is to read the advice, and then follow it. Think of it as a good investment in your identity!”
“Recent years have seen significant progress in protecting internet users from online threats. However, organised crime on the internet continues to grow and is becoming more sophisticated, as evidenced by increases in malware detections and disinfecions.

Microsoft’s recent Security Intelligence Report indicates that the total amount of malware and potentially unwanted software (PUS) removed from computers worldwide increased more than 43% during the first half of 2008. In the UK specifically, we’ve seen an increase of 66% in the number of computers infected. Trojan downloaders, or ‘droppers’, account for more than 30% of the global malware threat, making them the most prevalent form of unwanted software.

Of even more concern is that the criminals’ methods are evolving almost Darwin-like. The pace can be astonishing; there were 86,000 variants of ‘Zlob’ (a Trojan downloader) in the first half of 2008, equivalent to 571 variants a day. In addition, vulnerabilities rated as ‘high severity’ have increased 13% compared to the second half of 2007, accounting for approximately 48% of all vulnerabilities.

Why are criminals going to these lengths? Of course, they are after our usernames and passwords, but increasingly the real prize is our computers. If your computer is compromised, criminals may use it to spread their malware, generate spam, host illegal content, perpetuate click fraud and launch attacks against websites. Together, these compromised computers form botnets, designed to operate in the background without any visible evidence of their existence – often the victim has no idea that their computer is infected.

From a technical perspective the security industry is investing heavily in building intelligent anti-malware (anti-virus and anti-spyware) products, and building operating systems and application products with fewer vulnerabilities. The Security Intelligence Report indicates that software vulnerability disclosures across the software industry as a whole are falling, down 19% in the first half of 2008 compared to the same period in 2007.

Against a backdrop of global economic downturn, however, it’s possible that we may see more intensified efforts from criminals over the coming year. It’s critical that we all maintain efforts to employ the most up-to-date methods against the latest threats. Turn on your firewall, turn on automatic updates in your operating system, and ensure you’re using updated anti-spyware and anti-virus software.”

---

1 All figures and data taken from Microsoft Security Intelligence Report Volume 5, published November 2008, which examines data collected during January to June of 2008.
“Small enterprises – from local tradesmen through to small retailers – are increasingly reliant on technology to run their businesses, making it critical for them to pay attention to online security issues. With these ‘micro businesses’ accounting for approximately 95% of all UK businesses, the potential consequences of online security problems are significant.

The challenge for the owners of these small companies, without the budget for IT support, is they have to take responsibility for IT issues themselves. A Get Safe Online survey of 1,008 UK micro businesses indicates more than 95% of business owners are in this situation.

When time and resources are short, online security gets pushed down their list of priorities but it’s difficult to understand why.

44% of small businesses in the UK have been a victim of some form of cyber-crime, including internet scams, identity fraud, phishing or data theft. And significantly, around 60% of those interviewed said their businesses would grind to a halt if their IT system failed.

Of those who had experienced online crime or other IT-related problems, almost a fifth (19%) said they lost revenue as a result of downtime. It’s clear that there is an impact on the bottom line whether you are a sole trader or a small business and, as economic conditions tighten, business owners need to ask whether they can afford to be victims.

With organisations such as GetSafeOnline.org providing clear and easy-to-follow advice, there are indications that the security message is reaching the UK’s small enterprises. Around 97% are taking the basic steps such as protecting their IT equipment with anti-virus software.

Unfortunately, this is not enough. As cyber crime becomes increasingly sophisticated, so the basics need to be reinforced. Business owners now need to look at access control, data encryption and secure password protection, as well as other measures such as staff training, policies and procedures.

As daunting as it may sound, regularly looking at the information on Get Safe Online’s website will provide small businesses with straightforward, jargon-free advice, so the online risks don’t overshadow the benefits the internet brings to UK businesses.”

* Source: DTI 2005. A micro-business is defined as fewer than 10 employees. All other statistics from GetSafeOnline.org survey of 1,008 micro-businesses conducted by Vanson Bourne, May 2007.
36% have been affected by a computer virus

60% said their businesses would grind to a halt if their IT system failed

Less than a 1/3 consider themselves to be up-to-date with internet security issues

One in five have been victims of internet scams

An average of £1,540 is lost due to downtime during IT failure, equating to £750 million in estimated losses

Two-thirds (66%) store vital documents on their PCs
"Reviewing this year’s Get Safe Online survey results, the figure that jumped out at me immediately was that over a quarter (26%) of the UK’s internet users are more afraid of being a victim of online crime today than they were 12 months ago. This is unsurprising – in the last year, identity fraud in particular has been hitting the headlines on a fairly regular basis.

In many ways, making internet users aware of the risks they face is an essential part of helping them to protect themselves. Critically, though, it’s not about scaring people – part of the ethos behind Get Safe Online is to equip everyone to use the internet with confidence. If we know what to look out for, and the steps to take to protect ourselves, there’s no reason why we can’t all enjoy the benefits of the online world.

Having said that, this year’s survey also found that fear of online crime has deterred 14% of people from using the internet altogether. Although this is a small improvement compared to 2006 (when the figure was 17%), this is still too high a number. We would like to see everyone online!

Similarly, around one in five internet users (22%) have been put off internet banking – though the efforts of high street banks to clamp down on the fraudsters seems to be having a positive impact, as this is much improved compared to last year’s figure of 31%.

Confidence appears to be a big factor. Around one in three (34%) of internet users say they know the basics of online security, but are not necessarily sure that they are always safe and protected.

In line with this, 62% said they could benefit from further information about online safety – though this is 10% lower than in 2006, indicating that more are using tools like the Get Safe Online website to source this information.

Encouragingly, 35% of internet users today feel that they are primarily responsible for their own internet security, compared with less than a quarter (24%) in 2006. This is the key to surfing with confidence – for each of us to make sure we know how to protect ourselves, with help from Get Safe Online, of course!"
### Get Safe Online’s Top Tips for Safer Surfing

<table>
<thead>
<tr>
<th>Protect your PC</th>
<th>Avoid online rip-offs</th>
<th>Take care of your identity and privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get anti-virus software, anti-spyware software and a firewall</td>
<td>When you’re shopping online, look for clear signs that you’re buying from a reputable company</td>
<td>Use an up-to-date web browser</td>
</tr>
<tr>
<td>Keep your computer up-to-date</td>
<td>On an online auction site, learn how it works and learn to pick good sellers</td>
<td>Always use strong passwords</td>
</tr>
<tr>
<td>Block spam emails</td>
<td>Use safe ways to pay, such as a secure payment service, or credit and debit cards</td>
<td>Don’t use the same few passwords for all websites</td>
</tr>
<tr>
<td>Use an up-to-date web browser</td>
<td>Look for evidence of a physical address and telephone contact details</td>
<td>Activate privacy settings on social networking sites</td>
</tr>
<tr>
<td>Make regular backups</td>
<td>Be wary of anything that is offered in an unsolicited or spam email</td>
<td>Don’t give away too much personal information on blogs and social networking sites</td>
</tr>
<tr>
<td>Encrypt your wireless network</td>
<td>Use your common sense to avoid scams – if it sounds too good to be true, it probably is!</td>
<td>Use good judgement – if you wouldn’t tell someone in the street, don’t tell them online!</td>
</tr>
</tbody>
</table>

Get detailed advice on all the above at [www.getsafeonline.org](http://www.getsafeonline.org)
About Get Safe Online

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

Founding Partners

HM Government  HSBC  Microsoft  SOCA

Partners

Cable&Wireless  PayPal  symantec