UNDER EMBARGO UNTIL 00.01AM MONDAY 20TH OCTOBER 2014

Media contacts: 020 7025 6662 *or* press@getsafeonline.org

CYBERCRIME HITTING BRITISH WALLETS TO THE TUNE OF £670 MILLION, WITH HIGH EMOTIONAL COST TOO

- *51 per cent of Britons have experienced an online crime*
- *Half of victims of online crime 'very or extremely violated' by their experience*
- *54 per cent of Britons now want to unmask the cyber crooks behind online crimes*
- *'Don't be a victim' is theme for Get Safe Online Week 2014*

20th October 2014: Get Safe Online, the public private joint internet safety initiative, today revealed both the financial and the emotional cost of cybercrime. In a specially commissioned poll[1] for Get Safe Online Week (20th-26th October), half (50 per cent) of those who said they were a victim of cybercrime (*including online fraud or cases resulting in economic loss; I.D. theft; hacking or deliberate distribution of viruses; and online abuse*) said they felt either 'very' or 'extremely violated' by their ordeal.

Separate figures, prepared by the National Fraud Intelligence Bureau (NFIB) for Get Safe Online Week, show the sheer extent of financial loss with over £670 million[2] lost to reported online-enabled fraud cases between 1st September 2013 and 31st August 2014. However, as a significant number of online fraud cases still go unreported, the true economic cost of cybercrime is likely to be significantly higher.

The Get Safe Online survey also revealed that over half (53 per cent) of the population now sees online crimes as seriously as 'physical world' crimes, destroying the notion that online crime is 'faceless' and less important than other crimes. As a result, more cybercrime victims (54 per cent) wish to unmask a perpetrator but only 14 per cent succeeded.

Over half (51 per cent) of those surveyed for Get Safe Online have been a victim of online crime[3] although only 32 per cent of these reported the crime. Around half (47 per cent) of victims did not know who to report an online crime to, although this figure is expected to drop through the on-going work of Action Fraud, the UK's national fraud reporting centre, and the considerable Government resources now dedicated to fighting cybercrime.

---

[1] Poll of 2,000 people by Vision Critical

[2] Figure gained from the top 10 online enabled fraud types reported to Action Fraud between 1 September 2013 – 31 August 2014

[3] Including online fraud or cases resulting in economic loss; I.D. theft; hacking or deliberate distribution of viruses; and online abuse

On a positive note, the victims in the Get Safe Online poll said that their experiences have shocked them into changing their behaviour for the better, with nearly half (45 per cent) opting for stronger passwords and 42 per cent being extra vigilant when shopping online. Over a third (37 per cent) always log out of accounts when they go offline and nearly a fifth (18 per cent) have changed their security settings on their social media accounts.

But, in stark contrast, most people still don't have the most basic protection. More than half (54 per cent) of mobile phone users and around a third (37 per cent) of laptop owners do not have a password or PIN number for their device. That figure rises to over half (59 per cent) for PC users and two thirds (67 per cent) of tablet owners.

Francis Maude, Minister for the Cabinet Office, comments:

> *"The UK cyber market is worth over £80 billion a year and rising. The internet is undoubtedly a force for good but we cannot stand still in the face of these threats, which already cost our economy billions every year.*
>
> *"As part of this Government's long-term economic plan, we want to make the UK one of the most secure places to do business in cyberspace. We have a £860m Cyber Security Programme which supports law enforcement's response to cybercrime and we are working with the private sector to help all businesses protect vital information assets.*
>
> *"Our 'Get Safe Online' and 'Cyber Streetwise' campaigns provide easy to understand information for the public on how and why they should protect themselves. Cyber security is not an issue for Government alone – we must all take action to defend ourselves against threats."*

Tony Neate, Chief Executive of Get Safe Online, comments:

> "*Our research shows just how serious a toll cybercrime can take – both on the wallet and on well-being, and this has been no more apparent than in the last few weeks with various large-scale personal photo hacks of celebrities and the general public. Unfortunately, this is becoming more common now that we live more of our lives online.*
>
> *"Get Safe Online Week this year is all about 'Don't be a victim' and we can all take simple steps to protect ourselves, including putting a password on your computer or mobile device, never clicking on a link sent by a stranger, using strong passwords and always logging off from an account or website when you're finished. The more the public do this, and together with better conviction rates, the more criminals won't be able to hide behind a cloak of anonymity."*

Detective Superintendent Pete O'Doherty, Head of the City of London Police's NFIB, said:

> *"Cheap and easy access to the internet is changing the world and transforming our lives. What many of us may be less aware of is that financial crime has moved online and poses a major threat to people of all ages and from all walks of life living in the UK today. Men and women, young and old, rich and less affluent – it matters little who you are, where you live or what you do.*
>
> *"It is vitally important people are fully aware of the dangers of fraud and cyber-enabled fraud, which is why the City of London Police, which is the National Policing Lead for Fraud and home to the National Fraud Intelligence Bureau, is fully supportive of Get Safe Online's week of action.*
>
> *"I would call on anyone who has fallen victim to an online fraud to report to Action Fraud. Only by doing this will local police forces be able to track down the main offenders, ensure victims receive the best possible service and provide support to help them recover from what can be an extremely difficult and upsetting experience."*

Who you need to speak to

- If you think you have been a victim of cyber-enabled economic fraud (i.e. where you have lost money) you should report it to Action Fraud, the UK's national fraud reporting centre by calling 0300 123 20 40 or by visiting www.actionfraud.police.uk.

- If you are a victim of online abuse or harassment, you should report it to your local police force.

- For general advice on how to stay safe online go to www.GetSafeOnline.org.

-Ends-

ONLINE CODE OF CONDUCT: SIMPLE STEPS TO GET SAFE ONLINE

- **PUT A PIN ON IT**: Whether it's a phone, website or a social media account, your first line of defence is a PIN or password. Never use the same password, make sure it is hard to guess (don't use your pet's name, your birthday or your favourite football team) and never share your passwords with anyone.

- **BE SOFTWARE SAVVY**: Protect all your devices with anti-virus software and make sure you regularly install updates to *any* programs or apps, as they often include improved security settings.

- **KEEP IT PRIVATE**: Check the privacy settings on all of your social media accounts so that only the people you want to share your information with can see it.

- **SECURE THE WIFI**: Make sure your home WiFi is protected with a strong password that only you and your family know. When out and about never use a hotspot that may be unsecured, especially when what you're doing is personal or private.

- **LOOK FOR THE PADLOCK**: When shopping or banking online always check there is a padlock symbol in the web browser window when you have logged in or registered, and that the web address begins with 'https://'. The 's' stands for 'secure'.

- **BID SMARTLY**: When using an auction site, make sure you never transfer any money directly to a bank account or hand over any personal details. If you're thinking of making a big purchase like a car, or finding somewhere to live, always make sure it exists and is genuine.

- **LOG-OUT/LOG-OFF:** Always make sure you log out of your accounts when you've finished with them and log off a computer when you've finished using it.

- **POST IN HASTE, REPENT AT LEISURE:** What goes online stays online so never say anything that could hurt, anger or endanger yourself or someone else.

- **MANAGE YOUR MESSAGES:** Never open or forward a suspicious looking email, or respond to a social media message from someone you don't know.

For further information:

- Contact the Get Safe Online press office team on 0207 025 6662 or press@getsafeonline.org
- Visit www.getsafeonline.org

GetSafeOnline.org on social media:

- Twitter: @getsafeonline
- Facebook: http://www.facebook.com/GetSafeOnline
- Google+: https://plus.google.com/111686736307855785273

About the research

From 26 to 29 September 2014 an online survey was conducted by Vision Critical among 2,075 randomly selected British adults age 18+ who are also Springboard United Kingdom Community members. The margin of error—which measures sampling variability—is +/- 1.9%, 19 times out of 20. The results have been statistically weighted according to the most current data on age, gender, region, and education from the most recent census data, to ensure the sample is representative of the entire adult population of the UK. Discrepancies in or between totals are due to rounding.

About Get Safe Online Week

Now in its ninth year, the aim of Get Safe Online Week is to educate, inform and raise awareness of online security issues to make sure consumers and small businesses can use the internet safely and confidently. Partners and supporters are encourages to issue awareness posters, website banners

and promote internet safety advice on social media. Local communities also get involved by setting up regional 'Get Safe Online Week' events to raise awareness of this pressing issue, and to play their part in protecting people of all ages from becoming victims of fraud, identity theft, abuse and other issues. For more information on Get Safe Online Week, please visit: https://www.getsafeonline.org/get-safe-online-week/

About Get Safe Online

About Get Safe Online Get Safe Online (www.getsafeonline.org), which is now entering its ninth year, is the UK's national internet security awareness initiative. A joint partnership between the Government, the National Crime Agency (NCA), Ofcom, law enforcement bodies and private sector sponsors from the worlds of technology, communication, retail and finance, the initiative continues to educate, inform and raise awareness of internet security issues to encourage confident, safe use of the internet. GetSafeOnline.org is supported by Barclays, Bob's Business, Creative Virtual, HM Government, HSBC, Kaspersky Lab, Lloyds Banking Group, National Crime Agency (NCA), Symantec, Action Fraud, Ofcom, HSBC, Microsoft, PayPal, Symantec, Standard Life, Gumtree, Camelot, Detica, StubHub, Nominet, PurchaseSeal, ValidSoft, Business Link, Charity Commission, Citizens Advice, The Association of Chief Police Officers (ACPO), Information Systems Security Association (ISSA), e-Crime Wales, Information Risk Management Plc, Institute of Information Security Professionals (IISP), RG (Interactive Media in Retail Group), The International Association of Accountants Innovation & Technology Consultants (IAAITC), The Internet Services Providers' Association (ISPA), Neighbourhood and Home Watch, PTA-UK, SafeBuy, Safer Jobs, Scottish Crime & Drug Enforcement Agency, Scottish Police College, The Scottish Business Crime Centre and UK Online Centres. If you are interested in becoming a partner or supporter of Get Safe Online, please visit: https://www.getsafeonline.org/get-behind-us/