Background

The **Interdisciplinary Research Centre in Cyber Security at the University of Kent in Canterbury** recently launched a second online survey[1] in order to get a better picture of the prevalence and impact of cybercrime victimisation, cyber security practices, and risks as seen by a sample of the UK population.

Executive Summary

The survey was composed of 8 questions that covered a wide range of cybercrime and cyber security related issues, and was carried out between the 22nd and the 24th of January, 2014. A total of 1,502 individuals from throughout the UK responded to the survey, of the 968 who indicated their gender, 407 were male and 561 were female. Ages were recorded in bands from 18 to 65+. Participants were asked about their experiences of cybercrime and cyber security practices over the last 12 months between January 2013 and January 2014. All eight questions were answered by each participant.

1. The majority of respondents felt at risk of being a victim of online crime over the last twelve months (67.7%), representing 926 individuals from the total sample (n=1,502). However, a significant proportion declared not feeling any risk at all (6.6%), just under 100 people, suggesting more work needs to be done in terms of campaigns for raising public awareness and education over the threat presented by online crime.

---

1 Through Google Consumer Surveys. More details of the service at http://www.google.com/insights/consumersurveys/home

2. Over a quarter of respondents reported being a victim of a cyber-dependent crime over the last twelve months (26%), representing around 390 individuals, and a proportion of them experienced multiple incidents. These findings suggest a relatively high prevalence, despite the wide availability of security software and well-known best practices.

3. Eleven percent of respondents affirmed being a victim of a cyber-enabled crime over the last twelve months, representing 165 individuals from the total sample (n=1,502). Worryingly, of these, 102 individuals reported being a victim of either online harassment/bullying (n=43), stalking (n=34) or online sexual offenses (n=25). Despite the seemingly small numbers, these figures appear comparatively high in relation to traditional crime rates (CSEW, 2013) and indicate the necessity for further research in this area.

4. Whilst the vast majority of respondents did not report any significant impact as a result of being a victim of cybercrime, psychological and/or emotional consequences of victimisation were the most common response given, selected by 82 individuals from the total sample (n=1,502). Very little research has been dedicated to the impact of cybercrime in the United Kingdom, in particular beyond financial losses. These findings suggest there are other noticeable effects from online crime, which require further research in order to understand how best to address the needs of victims.

5. Of those respondents who reported a cybercrime, the majority did it to a financial institution (5%) or their Internet Service Provider (3.8%). The least common avenue for reporting a crime was through official channels, such as Action Fraud (2.7%), and law enforcement agencies (3.5%). These troubling findings indicate a low level of awareness on how and whom to report experiences of cybercrime to, highlighting the sore need for increased awareness among the general population covering the different options for properly reporting a cybercrime.

6. Just under 13% of those respondents who did not report being a victim of cybercrime, chose not to because they thought it was a waste of their time or they did not know where to report the crime. These results suggest a lack of awareness of available support from law enforcement agencies.

7. The prevalence of the Cryptolocker ransomware (3.4%) seems much higher than expected. The proportion of Cryptolocker victims that claim to have agreed to pay the ransom to recover their files (41%) seems to be much larger than expected (3% was conjectured by Symantec, 0.4% by Dell SecureWorks).

Detailed Main Findings

In the following sections, we outline the preliminary findings from the survey by discussing the results of each of the questions. The full findings will be written up for publication in a peer reviewed journal in the coming months.

Q1. To what extent do you feel at risk from cybercrime?

The majority of respondents identified feeling at risk of being a victim of an online crime (67.7%). Of these, 41.1% picked "I feel at risk, I am careful when online", 20.9% picked "I feel at risk, I'm very vigilant online" and 5.7% answered "I feel the risk is unbearably high", as shown in Figure 1.

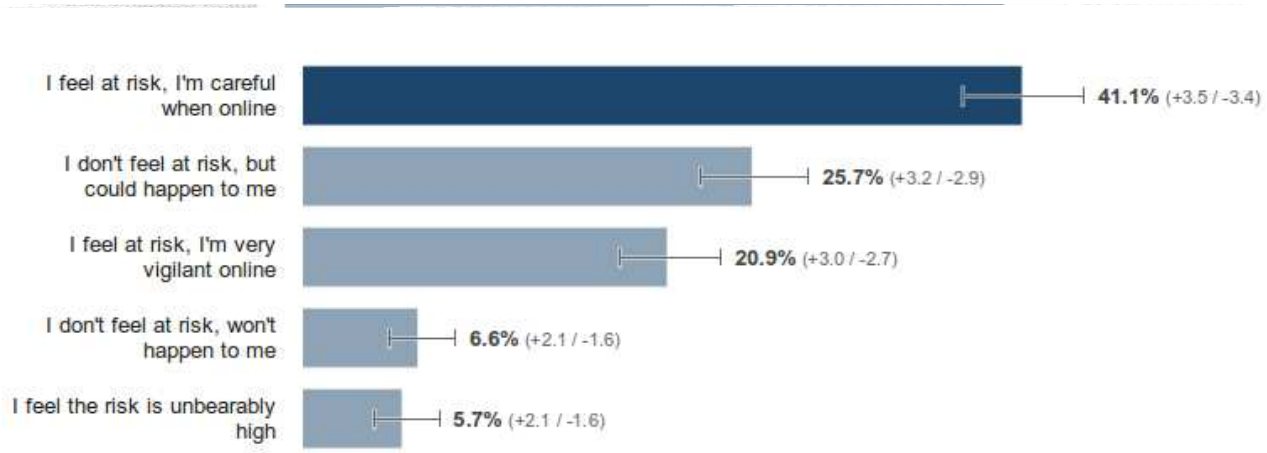


Figure 1. Answers to *Q1: To what extent do you feel at risk from cybercrime?*

Surprisingly, around 6.6% of the respondents surveyed do not feel at risk online and have the impression they will not ever become a cybercrime victim, suggesting there is a lack of public awareness around the threat presented by cybercrime. More cyber security education and awareness would do these users well, as they are in all likelihood the ones that will engage in

the more risky online practices and easy targets for cyber criminals. There are notably more men than women in this category: 10.6% vs. 4.4%.

Q2. Over the last 12 months, have you been a victim of a successful...?

This question accepted multiple answers as outlined in Figure 2 and focused on cyber-dependent crimes (e.g. hacking, viruses etc.). Over a quarter of respondents had been a victim of at least one of the listed cyber-dependent attacks over the last year (26%). Interestingly, a number of participants reported being victims of more than one cyber-attack. These findings suggest a relatively high prevalence of cyber-dependent crimes being committed, despite the wide availability of cyber security software and common industry practices. That offers a quite worrying perspective over the current threat that cyber-attacks represent for the average individual, especially serious and damaging ones like compromised email accounts, which is often the gateway to all online accounts, and online banking. We found a relatively high number of people affected by an online bank attack (3.9%) which could be potentially very costly. This data is shown in greater detail in Figure 2.

Answers	Unduplicated reach	# of answers
Online account attack (email,facebook, etc.) Phishing scam Virus/Malware attack Denial of Service attack Online banking attack	26.0% of respondents	5
Online account attack (email,facebook, etc.) Phishing scam Virus/Malware attack Online banking attack	25.1% of respondents	4
Online account attack (email,facebook, etc.) Phishing scam Virus/Malware attack	22.0% of respondents	3
Phishing scam Virus/Malware attack	17.2% of respondents	2
Virus/Malware attack	11.9% of respondents	1

Response metrics | Results table

Figure 2. Answers to Q2: *Over the last 12 months, have you been a victim of a successful...?*

Q3. Over the last 12 months, have you been a victim of…?

This question accepted multiple answers, as outlined in Figure 3 and focused on cyber-enabled crimes (e.g. fraud and theft, harassment/bullying, online stalking and online sexual offending). Just over four percent had recently been victims of online fraud or theft, very much in line with the 3.9% found in Q2 to have suffered an online banking attack.

Harassment and bullying seem to be quite common also, with around 2.9% of the respondents claiming they have been victimised in the last 12 months. A similar percentage (2.3%) were victims of online stalking. Approximately 1.7% had recently been victims of some sort of online sexual offence. Worryingly a number of respondents had been victims of multiple cyber-enabled offences over the last year.

Despite the seemingly small numbers, these figures appear comparatively high compared to traditional crime rates (CSEW, 2013) and indicate the necessity for further research in this area. A diagram with the results can be seen in Figure 3.

Answers	Unduplicated reach	# of answers
Online fraud or theft Online sexual offences Online harassment/bullying Online stalking	9.3% of respondents	4
Online fraud or theft Online harassment/bullying Online stalking	8.1% of respondents	3
Online fraud or theft Online harassment/bullying	6.5% of respondents	2
Online fraud or theft	4.1% of respondents	1

Figure 3. Answers to Q3: *Over the last 12 months, have you been a victim of…?*

Q4. What were the impacts from the online crime(s) you experienced over the last 12 months?

Also multiple answers were possible for this question, where we tried to investigate the various impacts felt by the victims of cybercrime. The 87.4% who have felt no impact at all from cybercrime is substantially higher than the 74% on Q2, so it includes a significant number of cybercrime victims suffering no significant impact. The most frequent type of impact is of psychological or emotional nature (5.5%), closely followed by a relatively mild financial impact of less than £1,000 (around 4.7%). Loss of reputation was next (2.4%), this may relate to the incidence of harassment/bullying (2.9%) in Q3 but also to social media account takeovers.

Finally, 1% reported some sort of physical impact as a result of being a victim of cybercrime. Interestingly, around 1.9% of the respondents declared relatively heavy losses over £1,000 over the last 12 months. Dividing the financial loss in this way, instead of allowing for an open question was intentional, to avoid common biases expressed in recent publications[2].
Although it is not possible to reliably extrapolate a global amount lost from the data, we can certainly conclude that having 1.9% of the respondents claiming to have lost more than £1,000 and 4.7% more than zero but less than £1,000 implies heavy losses for individuals across the country as a result of cybercrime.

It is worth noting that 1.2% of the respondents ticked both of the financial possibilities (under £1,000 and over £1,000). Whether this was due to error, exaggeration, or in reference to multiple incidents within the same 12 month period, we don't know; in any case we believe it is a very small percentage that doesn't affect the overall results or conclusions.
Whilst financial losses and loss of reputation are probably the most expected consequences of online crime, the survey suggests there are other important impacts on individuals (e.g. psychological, emotional and physical), which existing literature has paid little attention to so far and thus requires much closer attention in future research.

---

2 Sex, Lies and Cyber-Crime Surveys, by Dinei Florencio & Cormac Herley, in Bruce Schneier (ed.): "Economics of Information Security and Privacy III", Springer 2013.
http://research.microsoft.com/apps/pubs/default.aspx?id=149886

Answers	Unduplicated reach	# of answers
Financial - under £1000 Financial - over £1000 Loss of reputation Physical Psychological/Emotional	12.6% of respondents	5
Financial - under £1000 Financial - over £1000 Loss of reputation Psychological/Emotional	12.1% of respondents	4
Financial - under £1000 Loss of reputation Psychological/Emotional	10.9% of respondents	3
Financial - under £1000 Psychological/Emotional	9.5% of respondents	2
Psychological/Emotional	5.5% of respondents	1

Figure 4. Answers to Q4: *What were the impacts from the online crime(s) you experienced over the last 12 months?*

Q5. Who did you report the cybercrime to?

Again, multiple answers were allowed to this question, as it is possible for a crime to be reported to multiple parties (e.g. bank and law enforcement). Most crimes were reported to the banks and other financial services (5%), which is hardly surprising as the large majority of them would likely involve illegally accessing the victim's bank accounts, transferring money, etc. and it seems natural to contact them first to try to stop these operations from being carried out. More surprising is that in second position came the victim's Internet Service Provider with 3.8%. One of the official avenues for reporting cybercrime, (e.g. Action Fraud) came last, with 2.7%, suggesting that awareness on how to properly report cybercrime is worryingly low.

Other law enforcement was picked by 3.5%, and the victim's computer security provider (antivirus vendor, etc.) by 3.1%, as shown in Figure 5. We aim to take a closer look to how this relates to successful virus attacks (Q2) and antivirus usage (Q8), and how many of the respondents choosing "None of the above" did experience a cybercrime of some sort – this

should be well over 10% already based on Q2 results.

Answers	Unduplicated reach	# of answers
Action Fraud Other law enforcement (e.g. police) Financial services (bank, etc.) Your internet service provider Your computer security provider	15.1% of respondents	5
Action Fraud Other law enforcement (e.g. police) Financial services (bank, etc.) Your internet service provider	13.1% of respondents	4
Other law enforcement (e.g. police) Financial services (bank, etc.) Your internet service provider	11.1% of respondents	3
Financial services (bank, etc.) Your internet service provider	8.4% of respondents	2
Financial services (bank, etc.)	5.0% of respondents	1

Figure 5. Answers to Q5: *Who did you report the cybercrime to?*

Q6. If you did not report a cybercrime, what was your main reason?

This question aimed to gain an understanding of why individuals may fail to report a cybercrime. Some of the recent press discussion on overall crime figures referred to the reporting rate of cybercrime.

The most relevant finding (see Figure 6) probably was to find a relatively high percentage of people thinking that reporting was a waste of time (7.6% overall, but especially men at 9.6%) or not knowing who or how to report it (5.1%).

These results suggest a lack of awareness of available support from law enforcement agencies regarding cybercrime and what they could do to get help. More information and investment in awareness campaigns could be a way to address this in the future.

Figure 6. Answers to Q6: *If you did not report a cybercrime, what was your main reason?*

Q7. Have you ever been affected by CryptoLocker, or other similar malware or virus demanding a ransom?

In this question, we tried to ascertain the prevalence of a recent and quite dangerous strand of malware called CryptoLocker[3], which encrypts data files in victim's systems, and asks for a ransom to recover them. General knowledge about the prevalence and success of this (and similar) ransomware is very limited, so a better understanding of how many people were infected and paid, and whether they were able to recover their files is interesting and quite a hot topic at the present time.

The findings of this question are quite remarkable and defy previous estimations of prevalence and success by a large margin, sometimes tenfold. Of course we have to be cautious about the validity of the results shown here, for a number of reasons like the size and the bias of the sampled population and possibly others. Taking that (and its reflection in the relatively wide confidence intervals on some of these answers) into account, some figures are still remarkably high when compared with previous estimates.

It is surprising that approx. 9.7% of the respondents claim to have been victims of some sort of ransomware. This figure is at least twice as high as the one we were expecting, judging from the scarce and quite speculative previous literature. Most of the ransomware victims seemed to have chosen not to pay the ransom, but a very high percentage of them indeed complied and sent the money to the cyber criminals. This percentage seems to be around 41% for

3 National Crime Agency (NCA) alert - Mass ransomware spamming event targeting UK computer users. 15 Nov. 2013 http://www.nationalcrimeagency.gov.uk/news/256-alert-mass-spamming-event-targeting-uk-computer-users

CryptoLocker and approx. 30% for other strands of ransomware (Icepol/Reveton, and many others). This is at least 10 times more than the last previous estimation by Symantec[4] of around a 3% of paying victims (a previous one by the Dell SecureWorks CTU research team[5] put this figure at 0.4%).

If this were true and other researchers' findings corroborate this figure in the future, it shows a lack of success of the multiple public calls discouraging victims to pay the ransom, and would explain the enormous success of this particular ransomware (from the criminals' point of view, of course) and why copycats are rapidly emerging. Finally, both the prevalence of Cryptolocker (at around 3.4%) and that of other ransomware (6.4%) are much higher than expected.

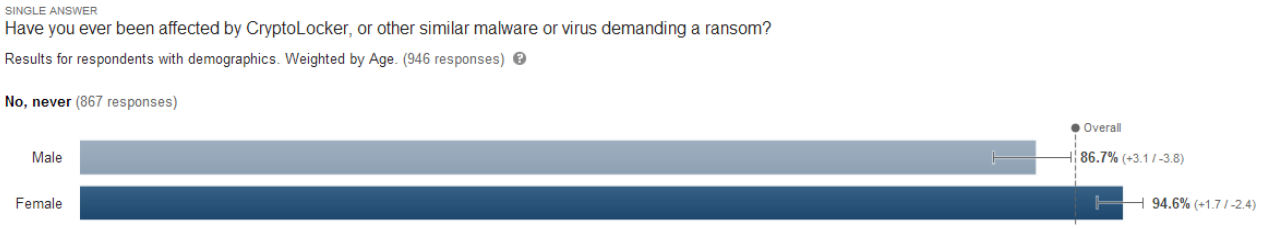


Figure 7a. Answers of *No, never* to Q7, sorted by sex

A curious insight (shown in Figure 7a.) into this question is that it seems that women are less affected by this kind of malware, as they significantly picked the answer *No, never* more than men. This may or may not be a particularity of CryptoLocker and other ransomware.

In fact, we have reasons to believe this would most likely happen with any other malware infection as women in general probably engage in less risky practices, and use security measures more frequently. Scotland seems to have been less affected by these ransomware strands than the UK average. For more on this, see Figure 7b and further discussion on the results of Q8.

---

4 Ferguson, D. (2013, October 18) CryptoLocker Attacks That Hold Your Computer to Ransom. Retrieved Feb. 7, 2014, from http://www.theguardian.com/money/2013/oct/19/cryptolocker-attacks-computer-ransomeware

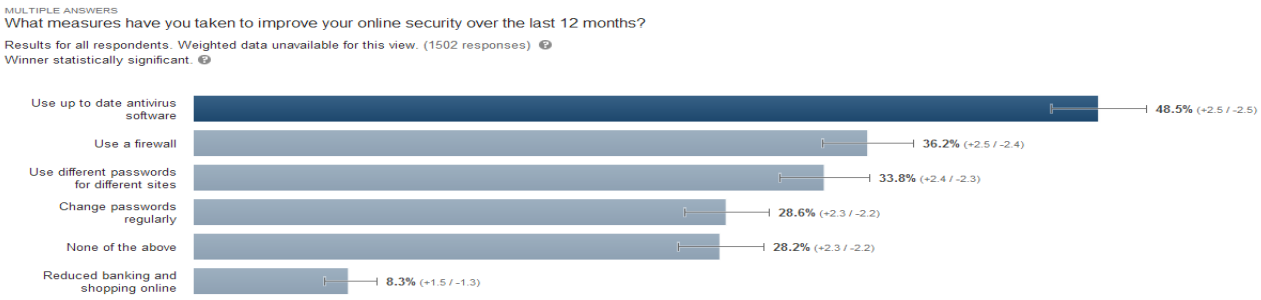
5 http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware/

Figure 7b. Answers to Q7: *Have you even been affected by CryptoLocker, or other similar malware or virus demanding a ransom?*

Q8. What measures have you taken to improve your online security over the last 12 months?

In this question, we aimed at understanding better what security measures respondents had put in place to increase their security over the last year. Multiple answers were again allowed to this question, as multiple measures can be used simultaneously.

Most used an up-to-date antivirus software (48.5%) or a firewall (36.2%) and a sizeable proportion used different passwords for different sites (33.8%) or changed them regularly (28.6%). It is particularly interesting that 8.3% decided to reduce their online banking and shopping activity in response to the threat of cybercrime.

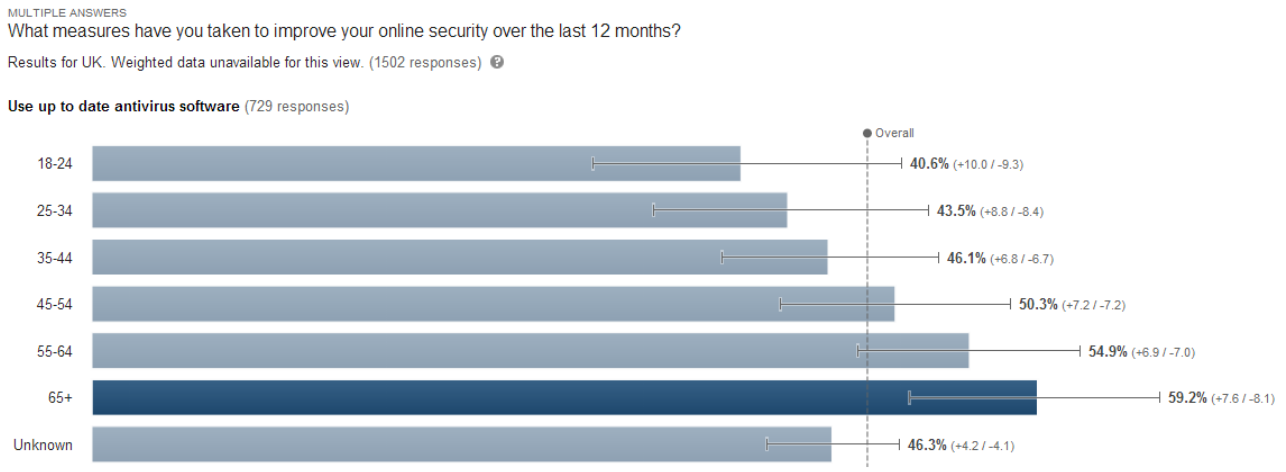


Answers	Unduplicated reach	# of answers
Use different passwords for different sites Use up to date antivirus software Change passwords regularly Reduced banking and shopping online Use a firewall	71.8% of respondents	5
Use different passwords for different sites Use up to date antivirus software Change passwords regularly Use a firewall	70.7% of respondents	4
Use up to date antivirus software Change passwords regularly Use a firewall	64.9% of respondents	3
Use up to date antivirus software Change passwords regularly	57.5% of respondents	2
Use up to date antivirus software	48.5% of respondents	1

Worryingly enough, a 28.2% of the respondents did not engage in any of these security

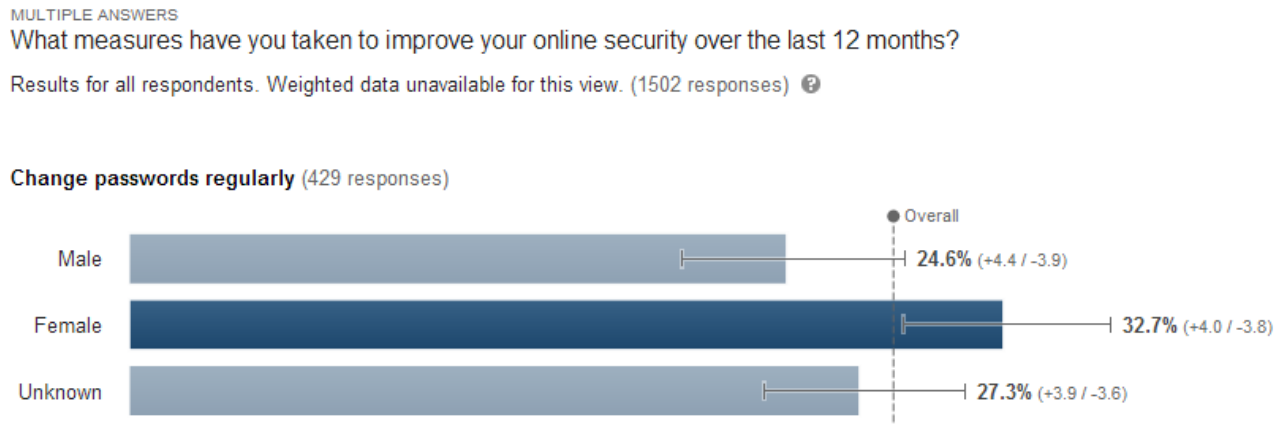
practices. Again, perhaps a case for furthering wider education in the matter.

The direct analysis of Q8 results by age, gender, and region led to a number of interesting insights. For example, it seems that the usage of antivirus steadily increases with age in the UK:



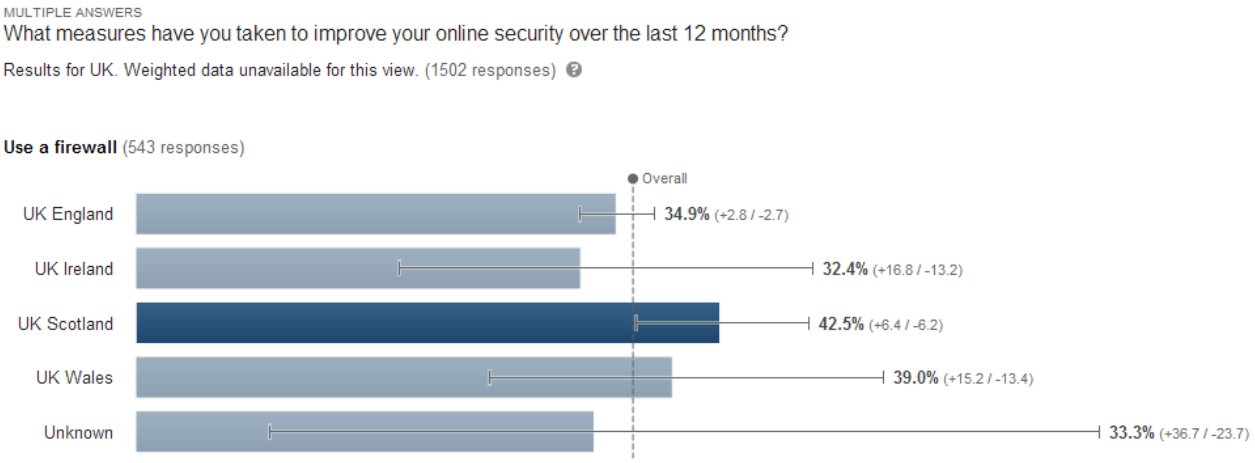
This, on the other hand, is less clear over the use of a firewall (where 65+ seem less inclined to use it than people in the 55-64 band) and this or a similar pattern is common to other security measures like changing passwords regularly.

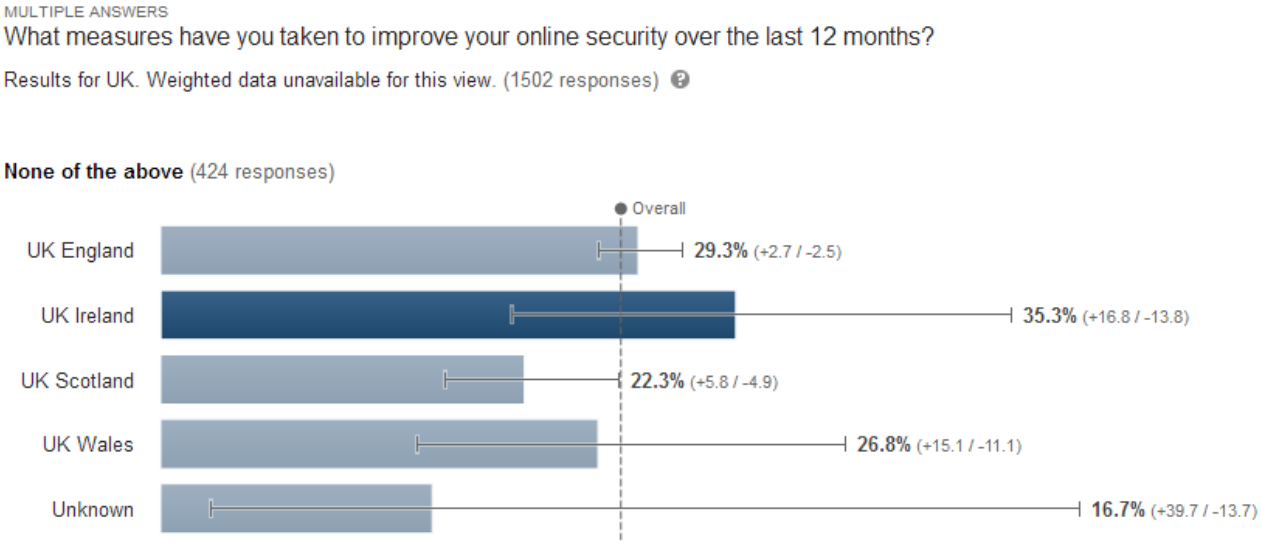
Additionally, and across almost all categories, it seems women take less risk and adopt better security practices than men. As an example, let's see what happens with regularly changing passwords:



But this also happens in the usage of antivirus software, firewalls, password management, and even with reducing shopping and banking online.

It also looks like Scotland has the best security practices across all of the UK. This is clear in a number of cases, but let's focus on just two examples:





The same holds for Scotland on the use of up to date virus protection, etc.

Cautionary Note

The relatively small size of this survey means that any extrapolation from these figures to total numbers of British citizens affected, total amounts of money lost, etc. are unlikely to represent the true national picture and should be approached extremely cautiously and conservatively.

Authors

Dr. Julio Hernandez-Castro and **Dr. Eerke Boiten**, of the School of Computing of the University of Kent, are the main authors of this survey and the accompanying documentation.

Magali Barnoux, of the Kent Faculty of Psychology, also contributed. The three are with the Interdisciplinary Research Center in Cyber Security.

For more info and media inquiries please contact

Katie Scoggins

Press Officer, University of Kent

K.Scoggins@kent.ac.uk