DynaRisk™

# Cyber Security Behaviours Study

2018

# Preface

As Commissioner of the City of London Police I was the national policing lead for cyber-crime. During my five-year tenure I saw the sheer scale of the problem and inability of governments to tackle the threat, with the anonymity of the internet enabling a huge growth in international crime. Cyber crime now accounts for over 50% of all crime being experienced by society in the UK. Crime prevention and helping people to protect themselves 'on line' is the most important challenge we face in this modern age and we need to get much better at it.

Prior to the advent of the Internet, policing in the UK became proficient at crime prevention to the extent that theft and burglary offences were halved. This wasn't because the police were arresting more people, it was because society had learned to protect itself. If we are going to make similar inroads into the cyber-crime challenge, we must first understand the problem; and listening to victims is a crucial first step.

This survey commissioned by DynaRisk provides a fascinating insight into how people think and feel in terms of cyber-crime and more importantly what they need to do to protect themselves. The findings accord entirely with the national work I was previously involved with and indeed with engagement I now have in the private sector. It's a vital read for anyone involved in cyber security.

The survey results show quite clearly the challenges we face but also provide some clear pointers as to what we should be doing about it. Crime prevention in this area must encompass work and home lives combined; we need to get smarter about giving people more practical 'hands on' advice about what to do and we need to nail the most basic elements such as safe use of social media, anti-virus, phishing emails and better password management. DynaRisk is really innovating in this space by making cyber security simple and relevant to anyone.

Victims have differing views on who is responsible for helping them protect themselves 'on line', but there is little doubt that they need support and we all must get smarter at understanding how to provide it.

**Adrian Leppard CBE QPM**
**Commissioner (Rtd) City of London Police**

DynaRisk™

# Contents

# Cyber Security Study

With more and more people all over the globe deepening their relationship with and use of the digital world, the need to keep them safe and secure has never been greater.

After all, in the UK you are **10x** more likely to be robbed online than in person and **35x** more likely to be robbed online than someone breaking into your home.[1]

We keep hearing from people that protecting yourself online is hard. There are so many different things to do from using proper passwords to updating devices, enabling encryption, setting privacy controls on social media websites and more. Ultimately most people simply don't understand what they need to do or how to protect themselves either at home or at work.

This study was conducted to learn more about people's security behaviours and attitudes by surveying over 300 respondents in the UK.

The following report outlines the key findings from this research. You can find more details on its methodology in the Appendix A.

**DynaRisk**
**March 2018, London**

*1 - Source: 'Overview of fraud and computer misuse statistics for England and Wales' (2018)* https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25

# Summary

There are 5 major findings that seem to be the most illustrative of the current situation of cyber security for individuals. They basically boil down to people don't know how to protect themselves.

We can visualise a person physically breaking into our home so we know we need locks on the doors and an alarm system. This is not the case with cyber risks which are invisible and intangible.

### 1. Getting attacked is a coin toss

More than half (56.1%) of people have experienced cyber crime in some shape or form. (Page 5)

### 2. We don't want to be trained, just tell us what to do

Most of us have very little time and patience as 61.5% of people prefer to be told what to do and how to do it vs 38.5% preferring to be trained.

The education and cyber security industry focus on in class teaching, computer based training with rudimentary quizzes and simulations and games. The issue is people just don't want training. (page 8)

### 3. We can do more to protect ourselves

A subset of the respondents agreed to run a quick security check where we found that 90.2% of them had at least one cyber security issue. (page 10)

### 4. Protection is very inconsistent

We asked respondents if they used 13 different tools and techniques to protect themselves, only anti virus has a penetration rate of over 75%. (page 12)

The solutions to most of our cyber security problems are available, people either don't know about them and why they are important or don't use them.

### 5. We are lost when it comes to cyber

38.6% of respondents said that not knowing where to start was the biggest reason for not doing more to protect themselves. (page 20)

# Experience with Cyber Crime

## Prevalence of cyber crime

We started by asking if the respondents had experienced any cyber crimes in the previous year: virus, phishing or scam emails, information being stolen, impersonation on social media and so on.

We found out that **56.1%** of the respondents experienced cyber crime in the previous year while **43.9%** did not.

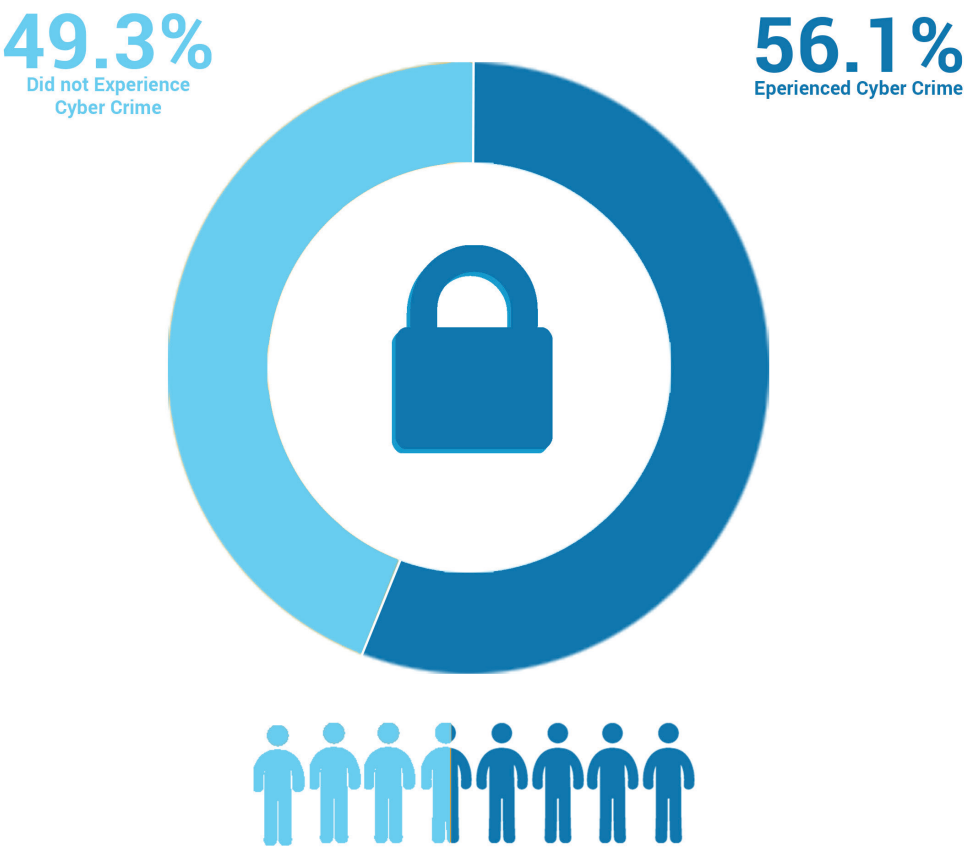



*Figure 1. Prevalence of cyber crime*

## Types of cyber crime experienced

The most prevalent cyber crime turned out to be phishing and scam emails, as **40%** of the respondents claimed to have received them. Furthermore, almost **17%** of people said they had their personal devices or online accounts hacked, often affecting their email and social media accounts.

Another common issue indicated by **14.2%** of the respondents was having a virus on their computer. **10.8%** of them shared that they had experienced incidents affecting their finances, such as having their credit cards cloned, having their bank accounts taken over and having loans taken out in their name.

Finally, **3.4%** of the respondents complained about spam emails while **2.7%** of them said there had been attempts to impersonate them on social media.

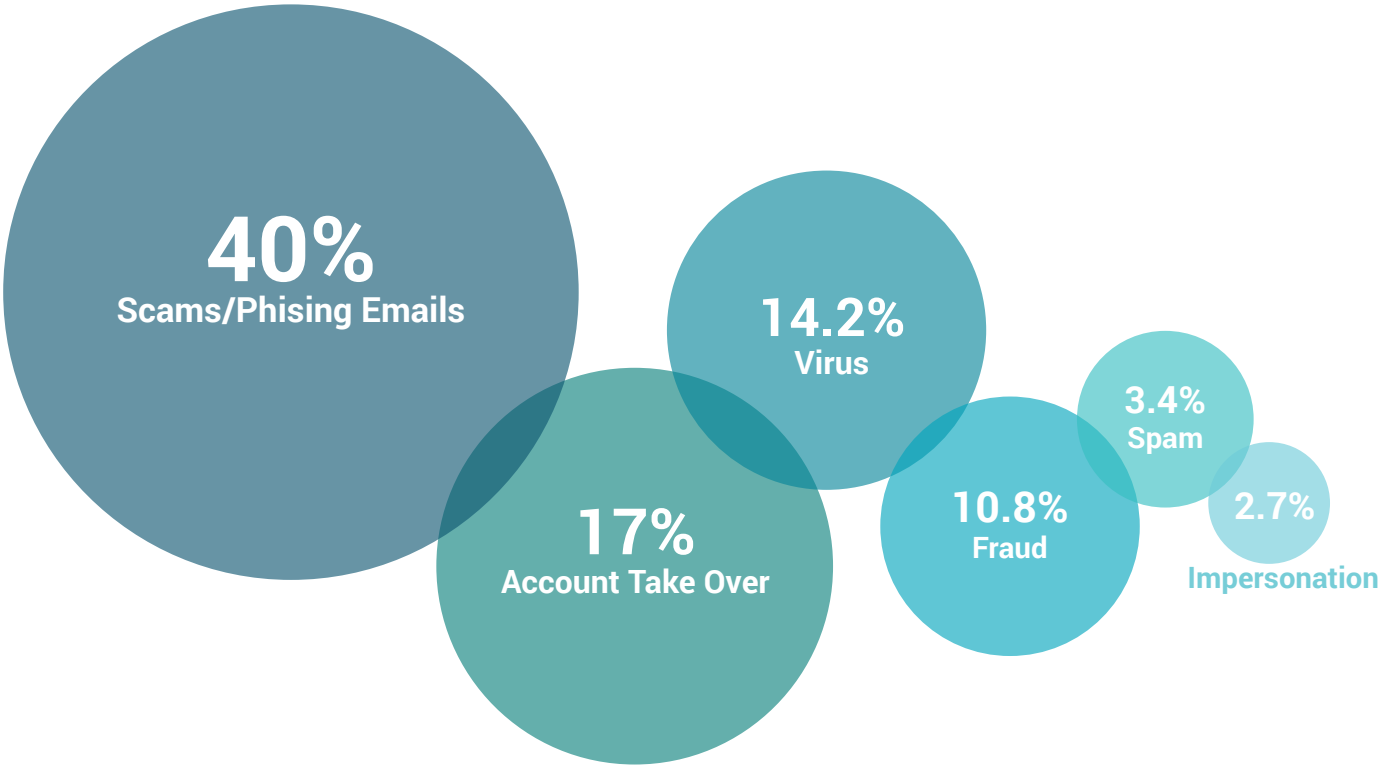



*Figure 2. Types of cyber crime experienced*

# Emotions Induced by Cyber Crime

We asked respondents how these incidents made them feel. The most common reaction was anger (24.7%), annoyance (17.6%) and shock (15.7%) followed by feeling scared (11.9%) and helpless (8.7%).

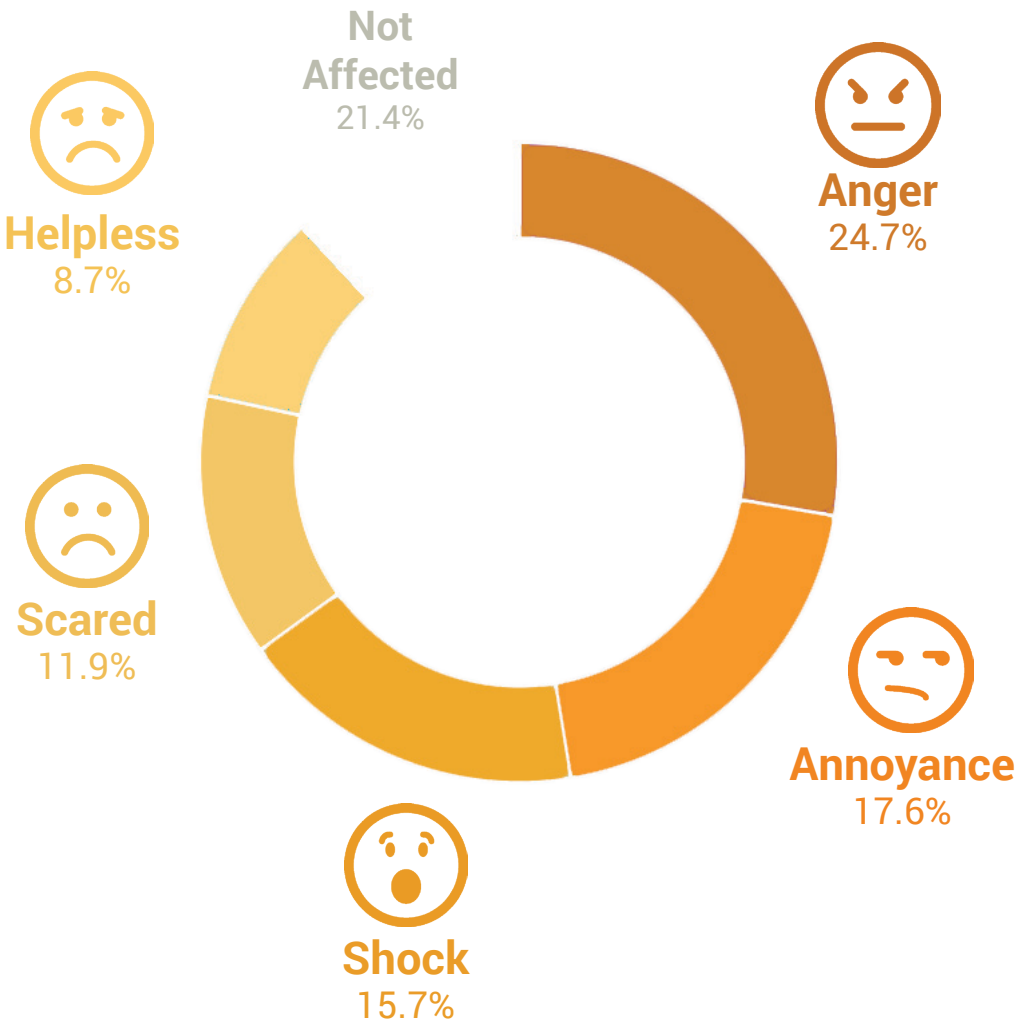



*Figure 3. Emotions induced by cyber crime*

**Cyber crime causes a range of emotions and can affect our daily life not only through direct financial loss but also by depriving us of our emotional stability and peace of mind.**

# Training vs Telling

## We prefer to be told

When we were planning for this study we wanted to ask a very fundamental question.

***'Do people want to be trained on how to protect themselves or just be told what to do?'***

The results were incredible, **61.5%** of people would rather just be told what to do.

The classic way to go about training is to bring in a consultant to run a workshop for staff and complement this with a computer-based training course. The training courses usually have a rudimentary quiz at the end which the person can take over and over again until they pass.

These training approaches are used to comply with regulatory requirements but offer little real value to the person being trained.

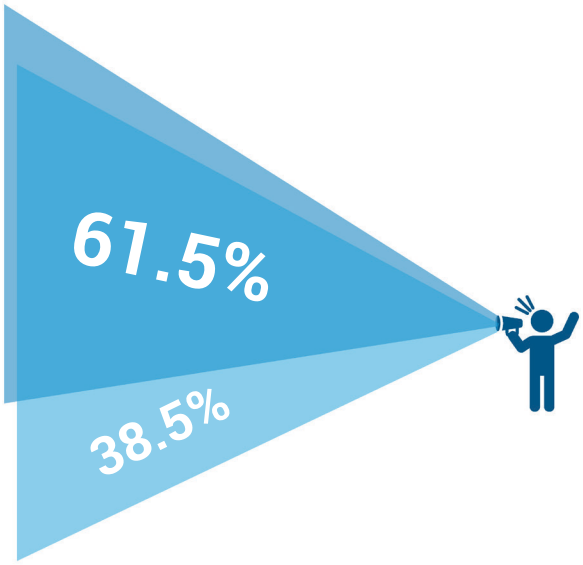



*Figure 4. Preference of protection by training or being told what to do*

**There are several issues with using training as the basis for improving our safety online.**

1. Training is only given at work, and usually only in larger corporate environments

2. People are not trained in their personal lives and are left to fend for themselves

3. Those who do not work (students, the elderly & unemployed) receive no training

4. Staff in small businesses, which represents over 99% of the workforce in the UK, may receive no training

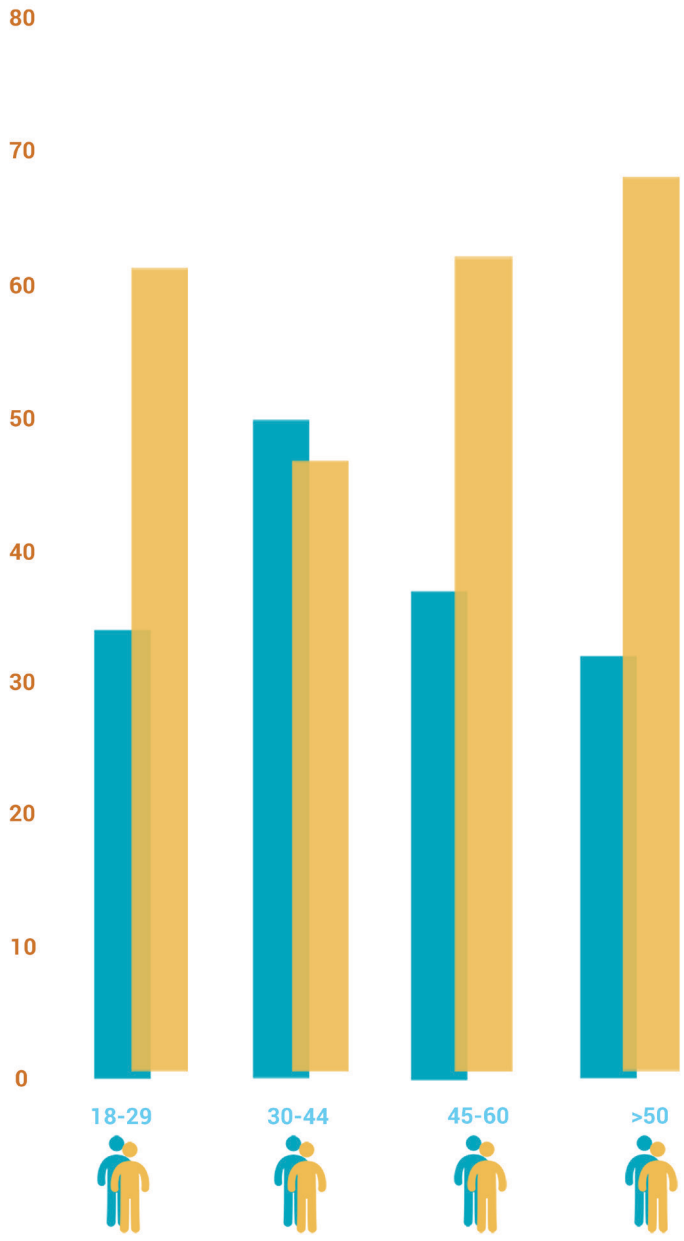
5. Most people don't even want to be trained!

The alternative to training is to just tell people what to do and how to do it. This approach is faster, scalable, more cost effective, drives tangible results and can be measured more effectively.

## Age-related trends

We found that different age groups preferred had different views on being trained vs being told.

People younger than 30 and older than 45 preferred to simply be told what to do, while 30-44-year old respondents had a preference for training.




It may be that 30-44 year olds are young enough to be well versed in technology, but also experienced enough to take an active interest in their security and ways to improve it.

Some respondents commented that they are able to understand and remember the information better if it is explained in detail and that is why they would prefer training options, while younger and older individuals often chose being told what to do citing a lack of time to explore the details.


*Figure 5. Preference of protection based on an age group*

# Feeling at Risk

Awareness of being at risk is critical in order for someone to take action to reduce it. We asked our respondents if they felt at risk of cyber crime to find out how much of an actual threat they believe it to be and how motivated they are to do something about it.

**49%** of respondents said they think they are at risk of cyber crime, with **37.8%** said they are probably at risk and **11.2%** claimed that they are definitely at risk.

More troubling however is that a third of respondents were either unsure or did not feel they were at risk.

This is directly opposed to the results of our security scanning where we found that **90%** of people had at least one cyber security issue that needed to be addressed.

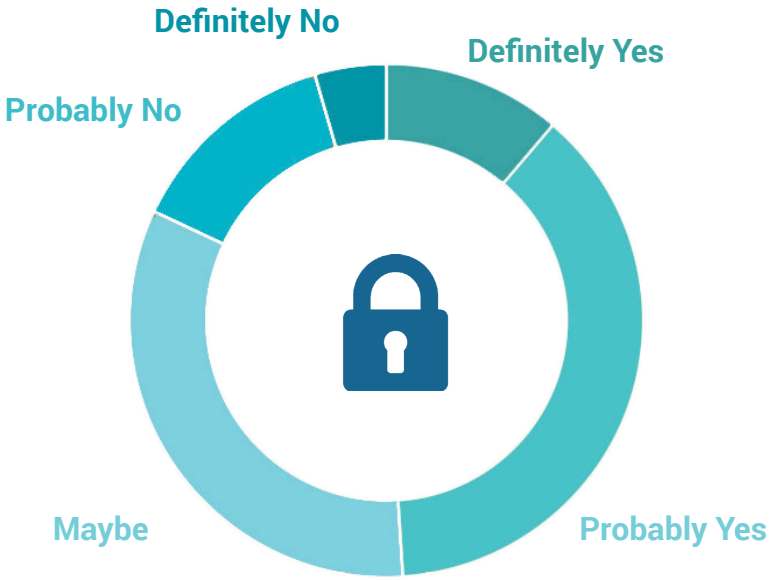
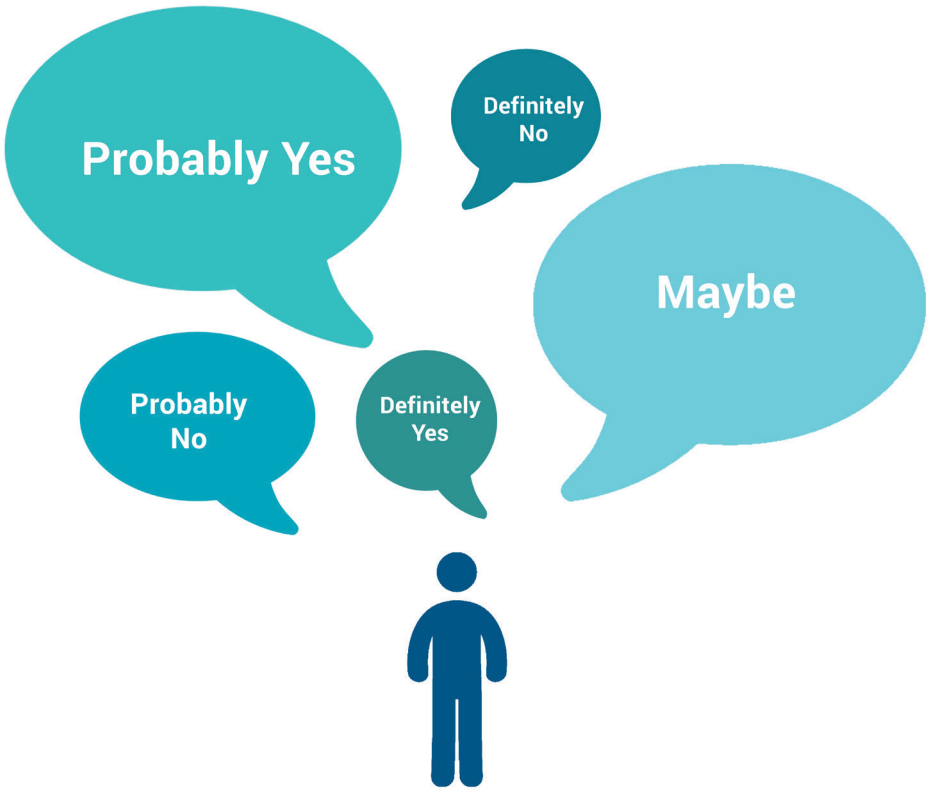



*Figure 6. Feeling at risk of cyber crime*



Interestingly, when we analysed this data in relation to the experience with cyber crime, the data revealed that the feeling of risk is more pronounced when the respondents have had experience with cyber crime before.

**55%** of people believe they are at risk of cyber crime if they have experienced it, whereas only **40.9%** of people who have not experienced cyber crime feel they are at risk.

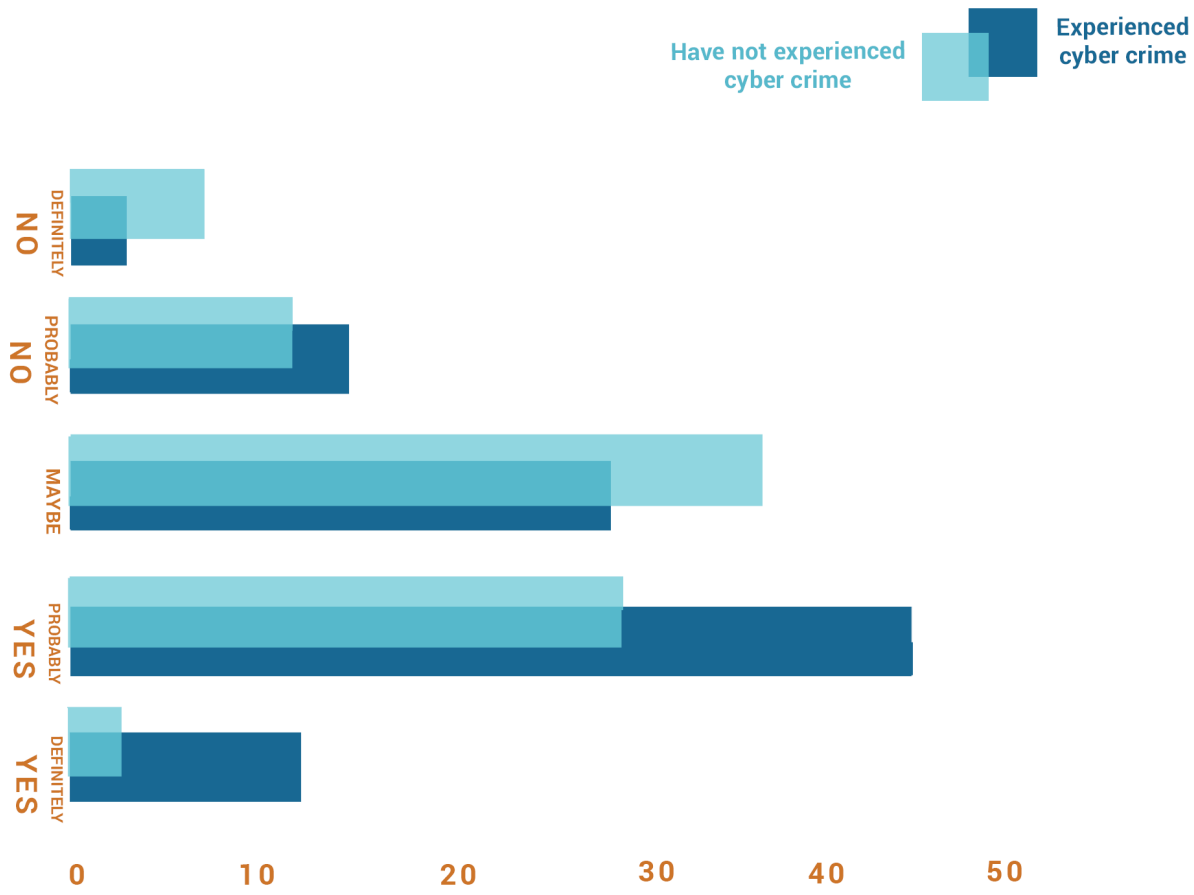



*Figure 7. Feeling at risk based on experience with cyber crime*



www.dynarisk.com | +44 (0) 203 086 8875 | info@dynarisk.com

# Tools used to Stay Safe

Since so many people suffer from cyber crime and are at risk, we wanted to find out how they are protecting themselves online, and how those ways differ based on their past experience with cyber crime.

The most popular tool was **antivirus software**, with 76.9% of respondents saying they used it.

**Strong passwords** were another common theme with 72.4% of respondents using them however possibly due to these complex passwords, only 40% of respondents are using unique passwords.

More than half of all the respondents use **social media privacy settings.**

More than half of all the respondents **update their software** to be safer online.

**Encrypting personal devices** is less common with only over 15% of respondents using this means of protection.

**Password manager** is also used by 15% of respondents as a means of protection.

In addition, 13.1% of respondents use a **Virtual Private Network (VPN).**

**Identity monitoring** turned out to be used by 4.2% of the respondents.

3.8% said they had a form of **cyber insurance.**

1.6% of them said they use a **security score.**

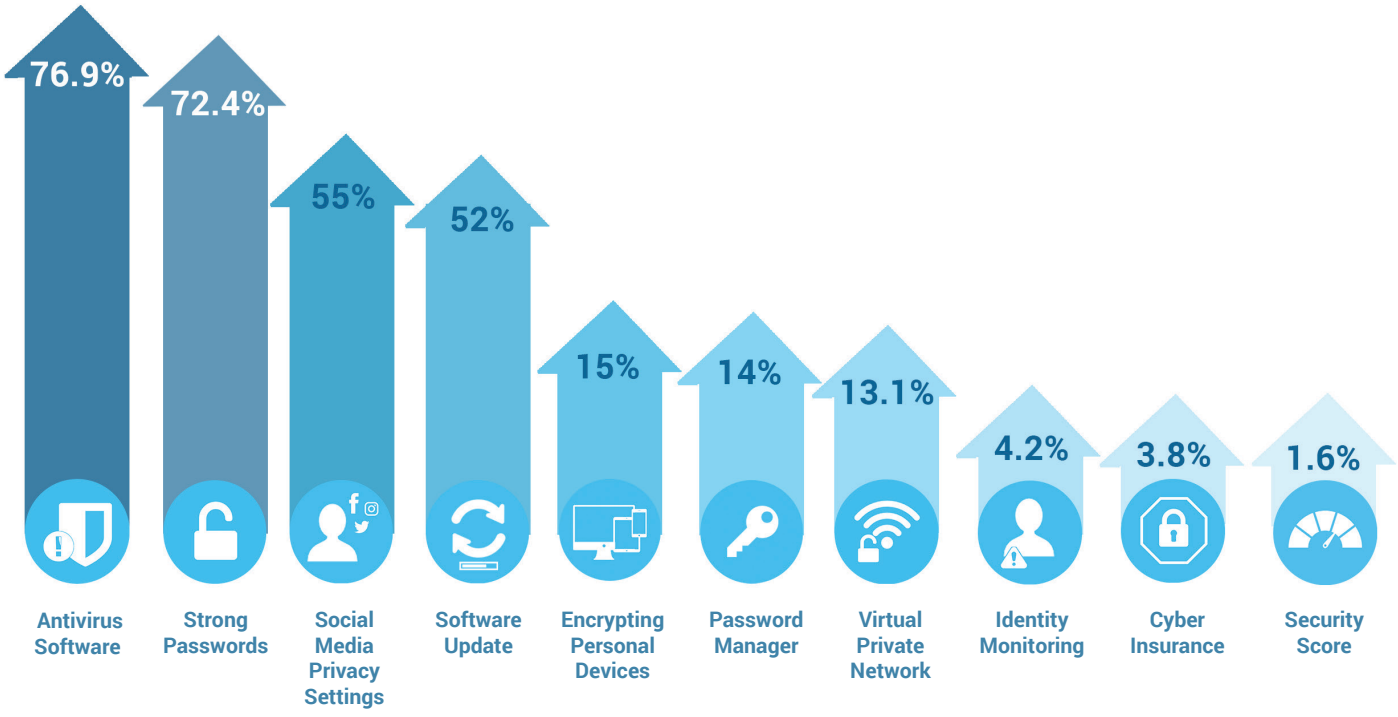



*Figure 8. Ways of protecting oneself online*

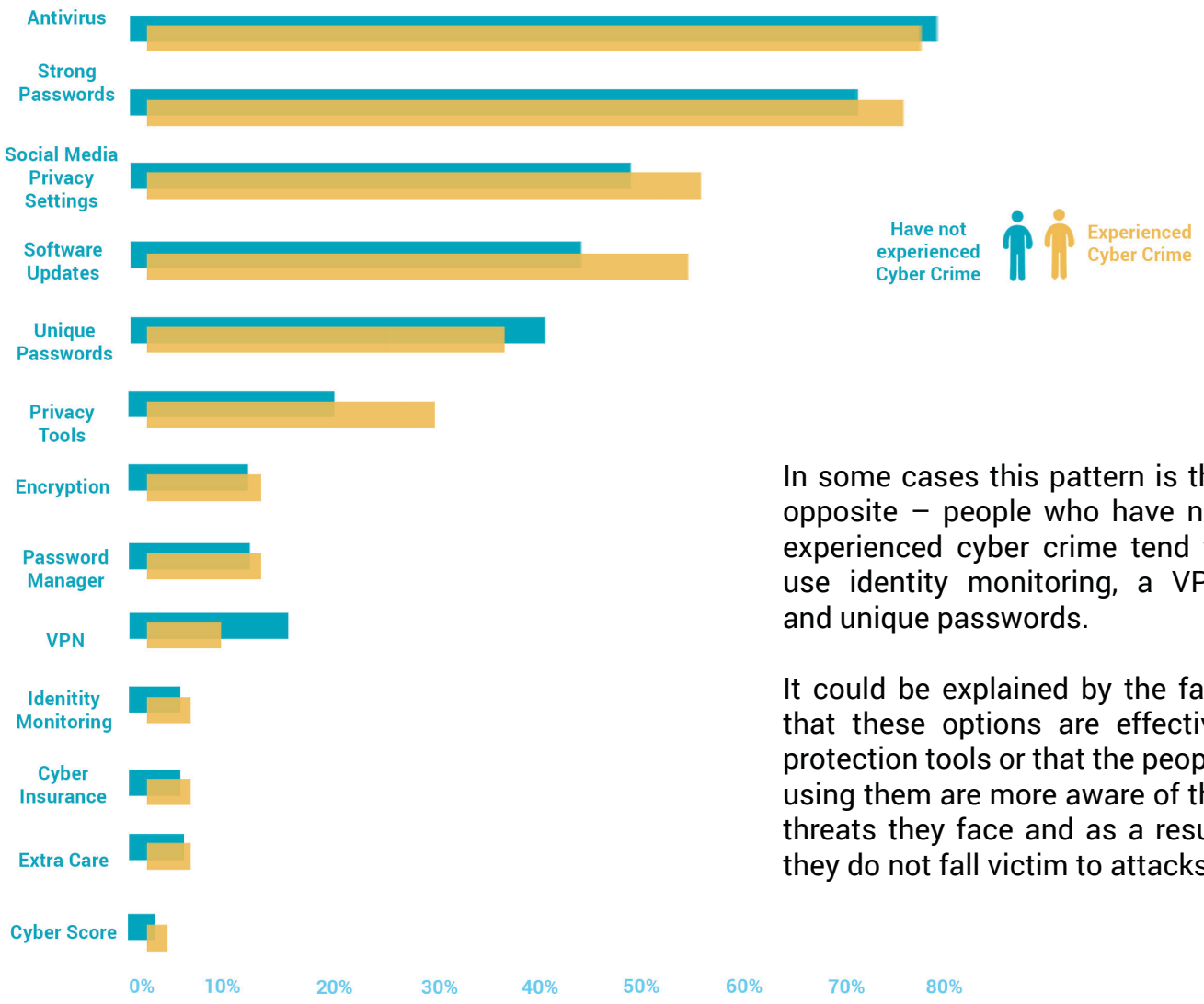
**An interesting way to look at this data is by focusing on how many people do not use the common tools.**

It is striking that more than **23%** of people do not use any antivirus software (perhaps due to wide spread smart phone & tablet usage) and that more than half of them do not focus on how unique their passwords are.

This latter trend seems to be a common issue since even if a password is strong, reusing it could result in account breaches.

A password manager could potentially solve this issue, but with only **15%** of people using it, more should be done to ensure safety online.

It also seems that people who have experienced cyber crime tend to use different cyber protection tools more. For instance, almost a third of people who experienced cyber crime used privacy tools in comparison to only over a fifth of people who have not experienced it.




In some cases this pattern is the opposite – people who have not experienced cyber crime tend to use identity monitoring, a VPN and unique passwords.

It could be explained by the fact that these options are effective protection tools or that the people using them are more aware of the threats they face and as a result they do not fall victim to attacks.

*Figure 9. Ways of protection based on experience with cyber crime*

# Who Should Protect Us?

While there are lots of tools on the market, systematic help from trusted parties is needed to ensure the message of staying safe online is spread far and wide. We asked the respondents of our study who should help them to stay safe online.

The majority of people believe that their internet provider should be helping them to protect themselves, as **66.3%** of respondents claimed they would expect this type of help from them.

Furthermore, more than half of all study participants think that the government should provide this guidance, while **47.1%** of them feel that it is the duty of their bank.

A cyber security company is the expected source of help for **26.3%** of the respondents, and almost a fifth of them feel that their employer should play a major role in their cyber protection. Insurance companies are expected to help by **15.7%** of surveyed individuals.

Some less popular options were computer stores, email providers and independent consultants.

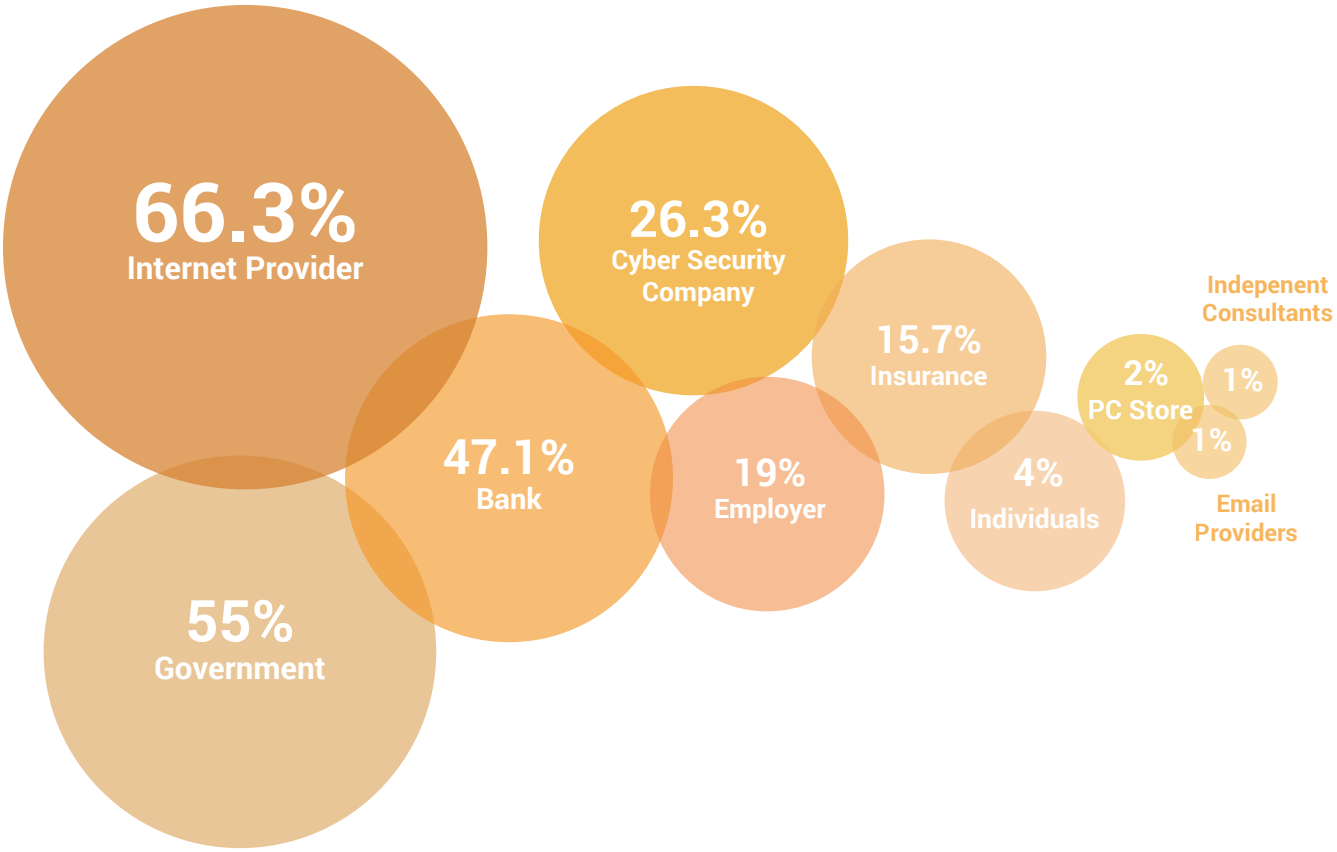



*Figure 10. Potential sources of cyber protection*

As discussed earlier, those who have experienced cyber crime before tended to have higher expectations for a wider variety of sources of help.

It is interesting to observe that the only category where this pattern did not hold was individuals, who claimed that only they and they alone should be responsible for their cyber protection.

Only people who have not experienced cyber crimes in the previous year believed that they should count on themselves only. Everyone who experienced a security issue indicated they would prefer to have an external source of help.


*Figure 11. Sources of cyber protection based on experience with cyber crime*



www.dynarisk.com | +44 (0) 203 086 8875 | info@dynarisk.com

# DynaRisk Quick Score

## Wide-spread security issues

DynaRisk offers a free scan to check your device and email account for stolen information, out of date or vulnerable software and privacy issues. We asked the participants of our study[2] to run the scan in order to receive a quick risk score, which is calculated by taking into an account the threat that each of those aspects pose:

**5 stars** means we have not found any risk issues
**1 star** means the person is at significant risk.

We found that **90.2%** of respondents have cyber-security related issues, as they received **four or fewer stars** – that means that at least one aspect of their security or privacy is at risk. Almost **40%** of the respondents in this study got a 1 or 2 star rating, indicating they are at heightened risk. On average, our respondents received **2.9 stars**.

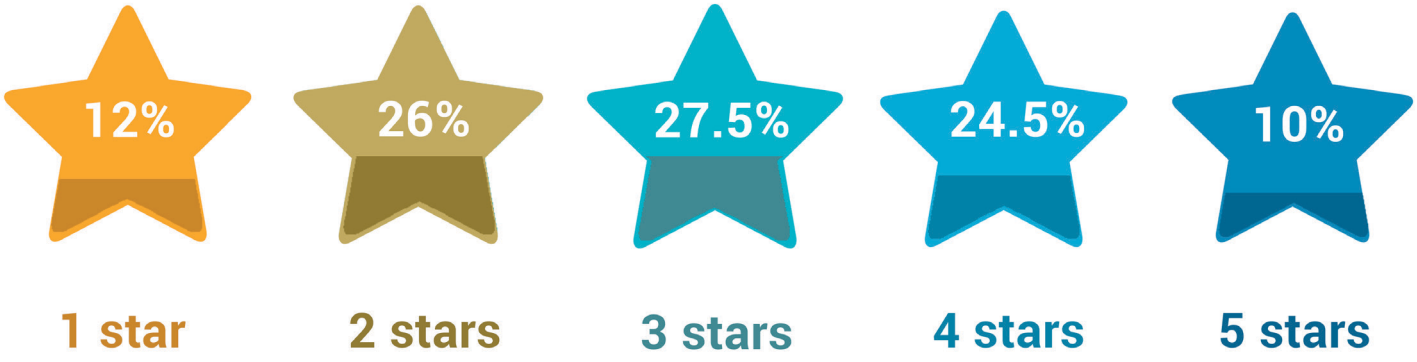



*Figure 12. Security score distribution*

The results show that the vast majority of the people who got to run the scan had at least some online security related issues. This fact is quite concerning given the potential consequences of it, so we asked our survey participants how their score made them feel.

*2 – the data in this section was obtained from the Study 1. Please see more information at Appendix A: Methodology, Study 1.*

## Emotions induced by risk score

The majority of people indicated that they are not surprised about the score. This choice was especially popular among the ones who had the score of **3** out of **5 stars** (40.5%). Almost a third of all respondents indicated that they are surprised about the score, especially the people who received **2 stars** out of 5 (45.2%).

The feeling of being shocked was expressed by 17.1% of the respondents and also common among the ones whose security was rated by **2 stars** (42.1%), while 16.2% people who indicated that the score made them feel reassured were the ones who mostly got a **4 star** score in 52.9% of cases.

The trend to relate positive emotions to positive scores was confirmed with the rest of the expressed emotions: 8.1% of the respondents felt confident, especially those 88.9% who received a **4** or **5 star** score, 8.1% of the respondents felt helpless, especially those 55.6% who received **1** or **2 stars**, 7.2% of the respondents felt scared, especially those 71.4% who received 1 or 2 stars, 3.7% of the respondents felt angry, and all of them received either 1 or 2 star score.

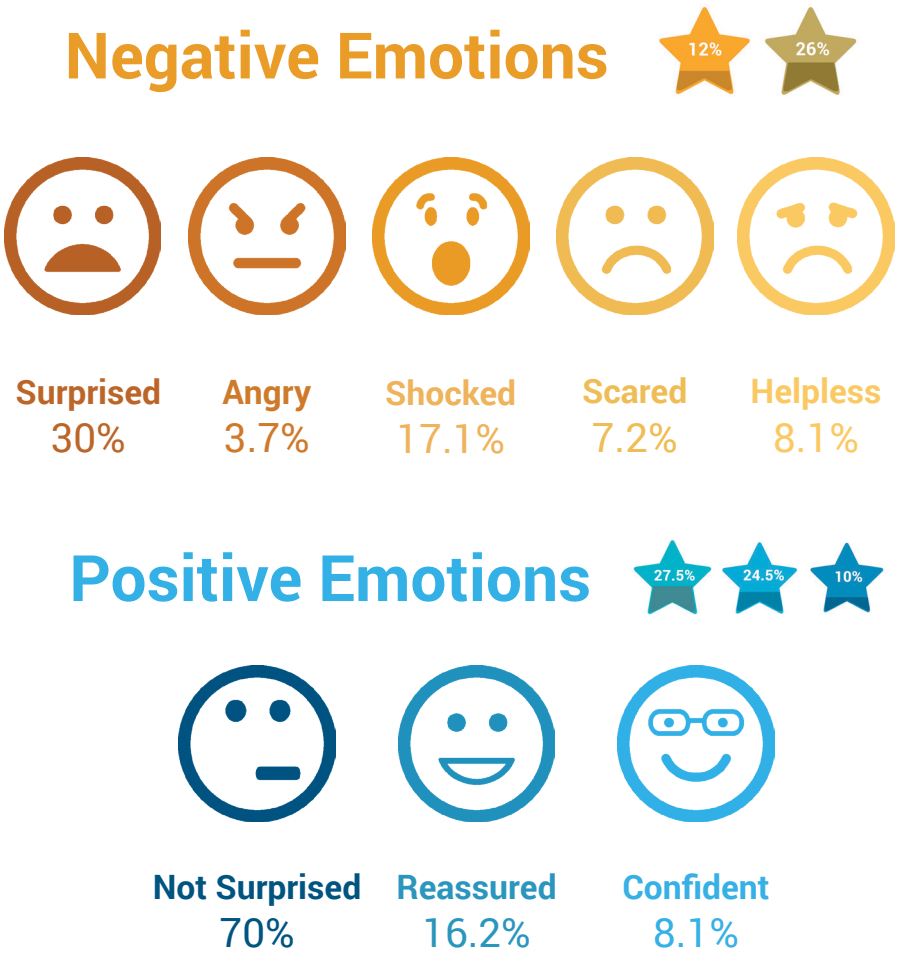



*Figure 13. Emotions Induced byrisk score*

# Going beyond current protection

## We want to do more

We used a second survey[3] to ask respondents if they would do more to protect themselves and their families.

The majority of people (57.2%) said that they would, 31.8% were not sure, while 11% said they would not do more to protect themselves.

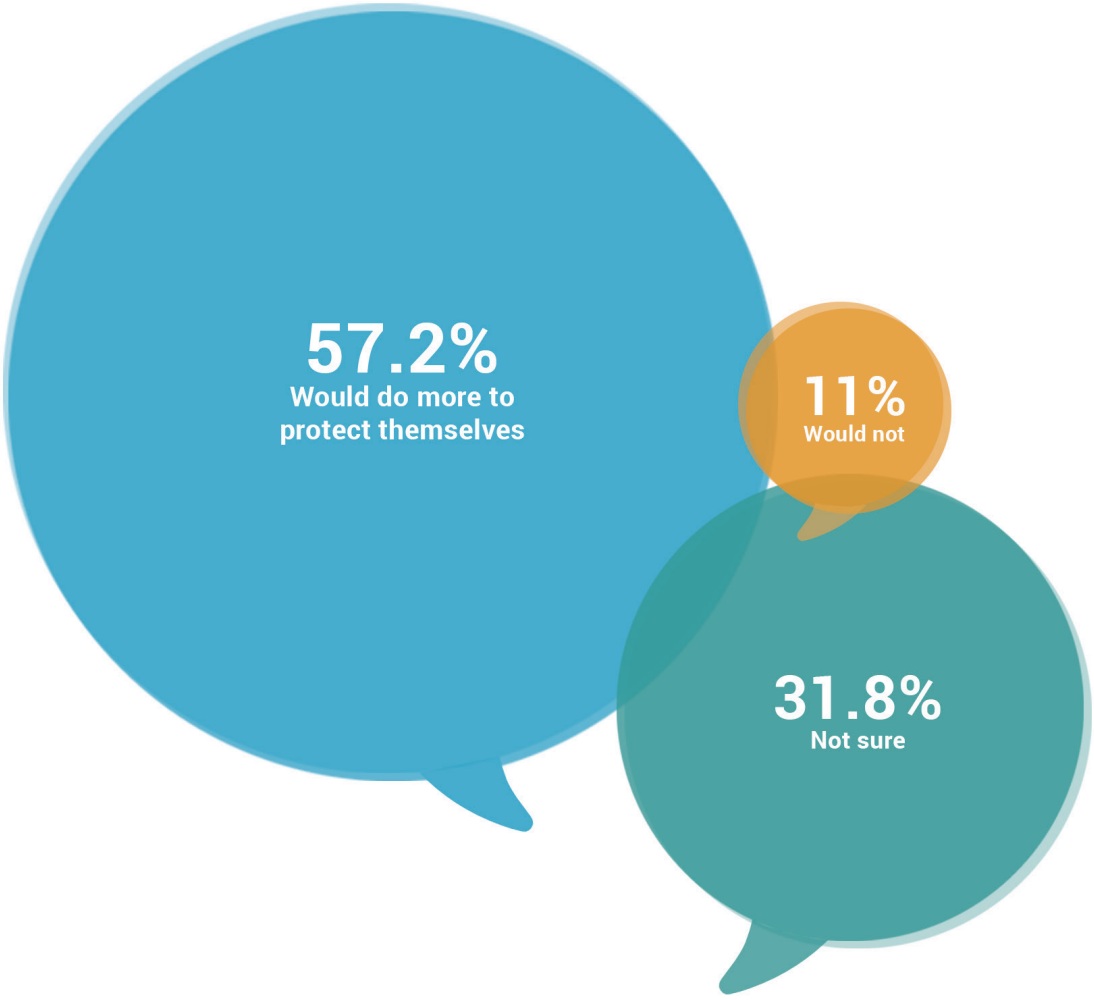



*Figure 13. Wanting to do more about one's cyber protection*

*3 – the data in this section was obtained from the Study 2. Please see more information at Appendix A: Methodology, Study 2.*

If people weren't sure or didn't want to do more to protect themselves, we asked for the reasons behind their decision.

The most popular reason was not knowing where to start, with **38.6%** of the respondents. The second reason was pricing, as **34.1%** of the respondents said that the cyber security software or services were too expensive.

More than a quarter of respondents said they don't know what to do to protect themselves. The rest of the reasons were less common: **14.5%** mentioned they don't have enough time, **10.1%** said it's not a priority and **2.8%** said that they do enough already.

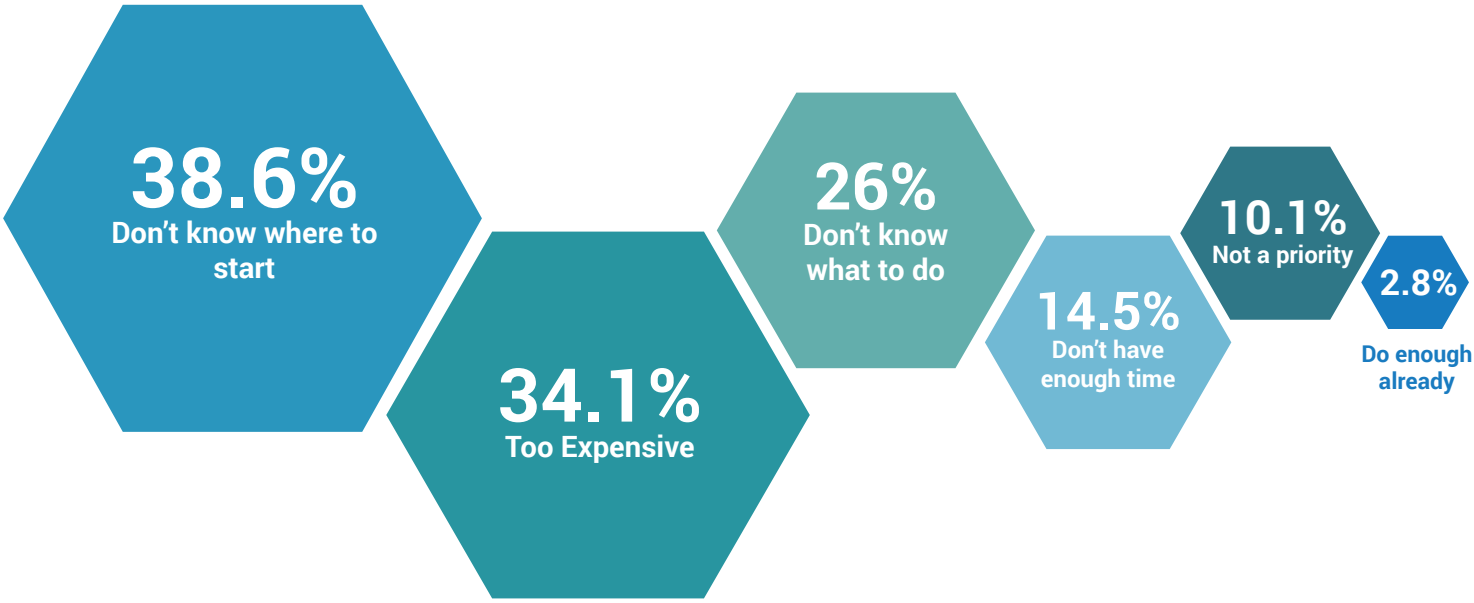



*Figure 14. Reasons for not wanting to do more about one's cyber protection*

## Age-related trends

When we analysed this data based on age, we found a few notable trends.

Firstly, younger people had a tendency to say they would do more to protect themselves online with **68%** of 18-29-year olds as well as **68.9%** of 30-44-year olds indicating this.

This decreases to **40.4%** of 45-60-year olds and **44.8%** of people who are older than 60 years.

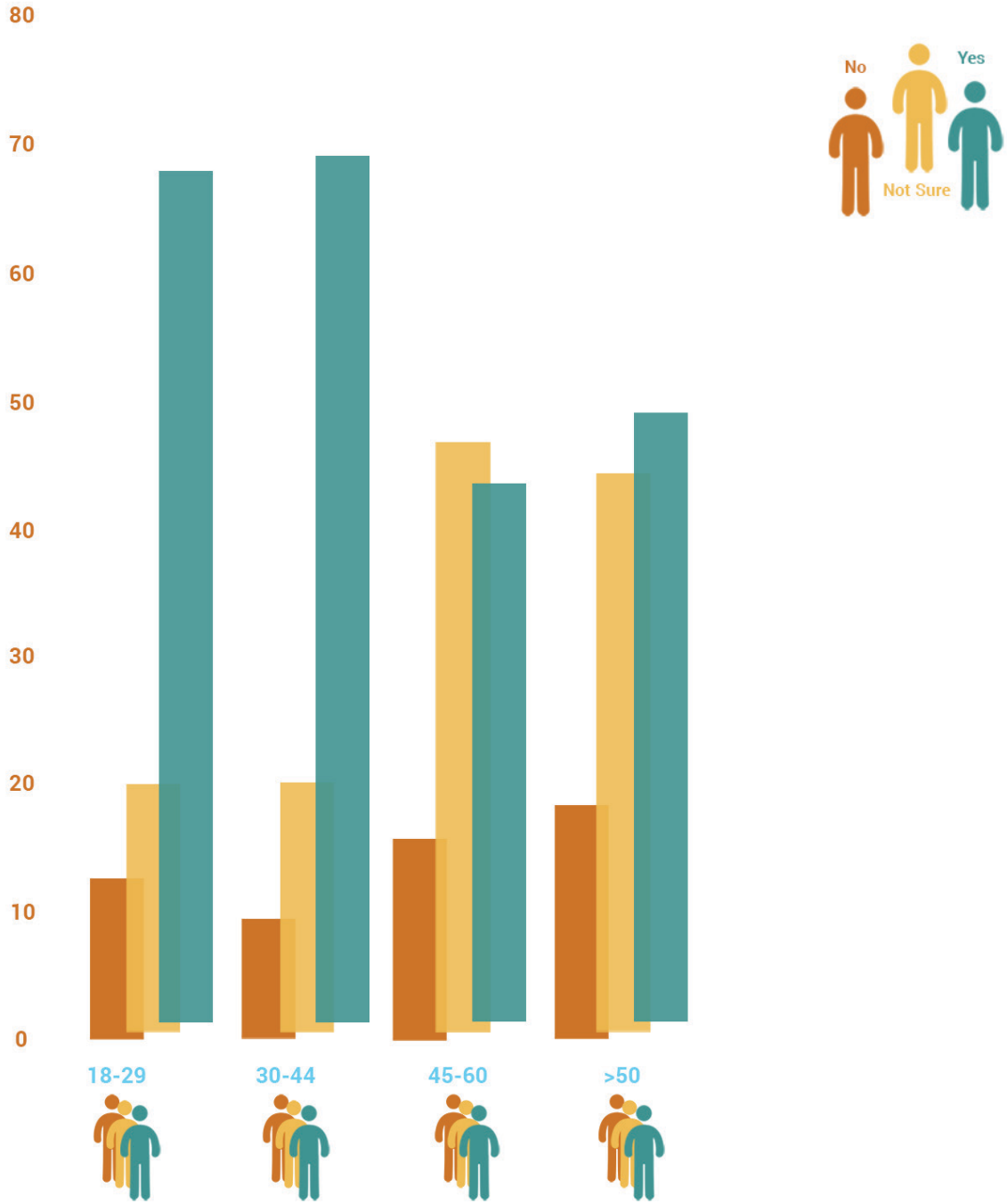



*Figure 15. Wanting to do more about one's cyber protection based on age groups*

After looking into the reasons for not willing to protect themselves online more, we discovered some differences corresponding to age.

For older respondents, cost and time were not significant barriers to doing more to protect themselves. While **36%** of 18-29-year olds said it is too expensive to protect themselves online, this decreased to **33.3%** for 30-44-year olds to, 29.8% for 45-60 year olds and finally to **24.1%** of those 60+.

As not knowing where to start was the most popular response, we looked into what age this concern corresponded with the most.

The 30-44-year old group was the most vocal about this issue with **43.3%** of them noting it as an issue while only **16%** of 18-29-year olds said so.

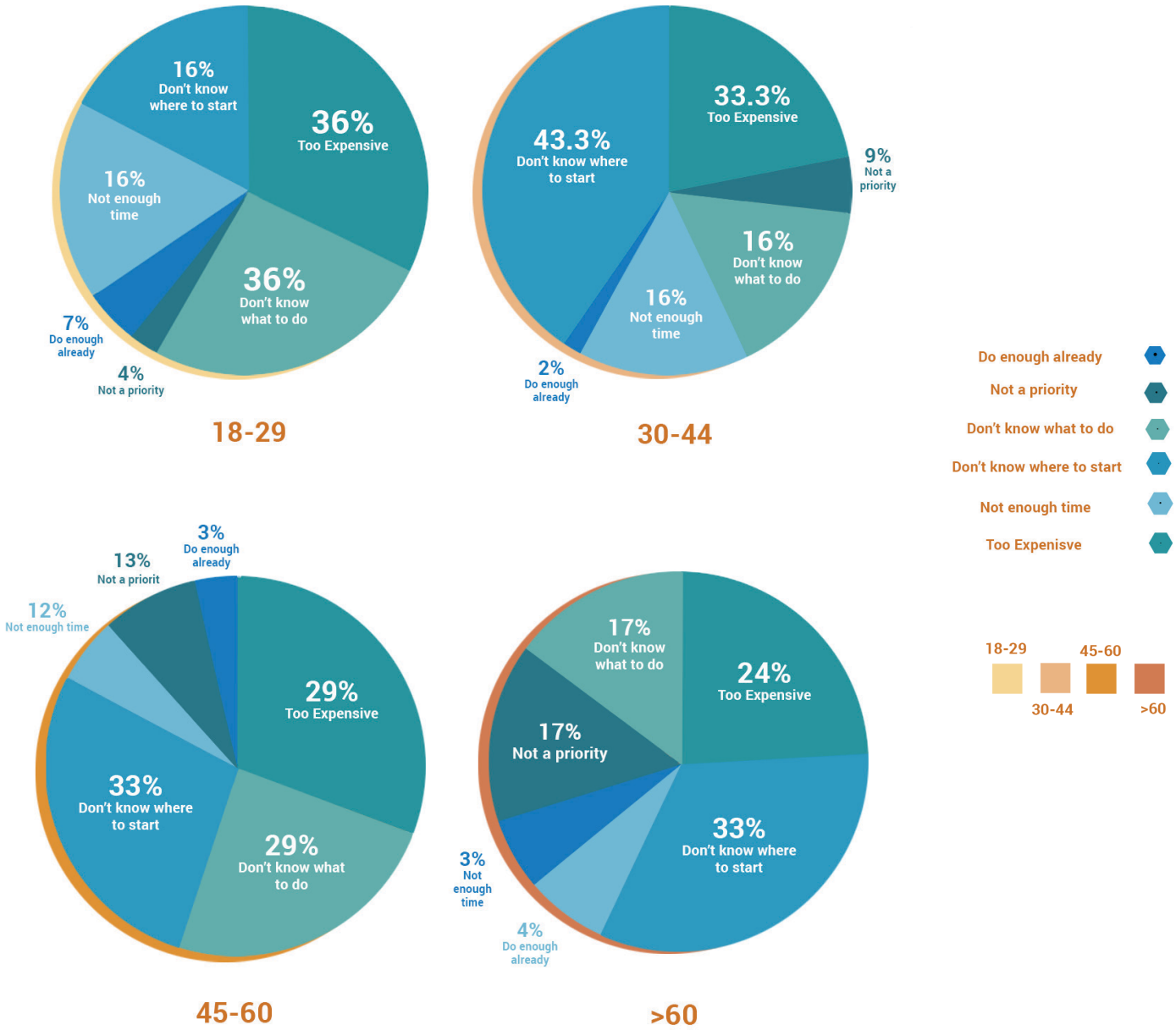



*Figure 16. Reasons for not wanting to do more about one's cyber protection based on age groups.*

# Appendix A. Methodology

## Time frame and sources

*The findings were collected by merging the data from two studies.*

**Study I** was being conducted from the 10th of October, 2017 to the 18th of December, 2017. The responses were collected in three ways:

**1.** The study was posted on an online survey platform
**2.** The study was available to fill in on the DynaRisk blog https://blog.dynarisk.com/.
**3.** The study was conducted in person, surveying people at work spaces.

**Study II** was conducted on the 7th of December, 2017. The responses were collected on an online survey platform.

## Respondents

**Study I** had 111 respondents, out of which 60.6% were female and 39.4% were male. The age distribution was the following:

18-24 – 44.5%
25-34 – 31.8%
35-45 – 10.9%
46-59 – 9.1%
older than 60 – 3.6%

The respondents came from 17 countries. Most of them were from the UK (54.1%), the US (US 15.3%) and the Netherlands (13.5%).

**Study II** had 203 respondents, out of which 57.21% were female and 42.79% were male. The age distribution was the following:

18-29 - 12.44%
30-44 - 44.78%
45-60 - 28.36%
older than 60 - 14.43%

All of the respondents resided in the United Kingdom.

There were 314 overall answers in both studies that were combined to formulate this report.