The Myers-Briggs Company

Type and cyber-security

A research study from The Myers-Briggs Company

Contents

Research study conducted by: John Hackston, Head of Thought Leadership, The Myers-Briggs Company

Executive summary

Purpose and scope

Cyber-crime is a growing problem, and so cyber-security is of increasing importance. The 'human factor' is often seen as a weak link in cyber-security, and many organizations have gone to great lengths to help their employees become less susceptible to phishing and other cyber-attacks. This can involve putting in systems and processes, as well as staff training and education. However, a 'one size fits all' approach may not always be effective; individual differences exist in all aspects of human behavior, and cyber-security is unlikely to be an exception.

This study set out to examine the relationship between cyber-security behavior and personality type, as measured by the Myers-Briggs Type Indicator® (MBTI®) assessment. This is so that personality-based cyber-security guidelines could be developed. The MBTI model looks at four areas of personality type (Extraversion or Introversion, Sensing or Intuition, Thinking or Feeling and Judging or Perceiving) and at how these areas combine dynamically to describe the whole person.

By helping individuals become more aware of their strengths and blind spots, and by offering personality-based hints and tips, the intention is to improve the IT security behavior of individuals and thereby the safety of organizations.

Results

563 people completed an online survey, answering questions on their personality type, their background (gender, age, country, job role and level, organization size and type) and their cyber-security attitudes, behaviors and knowledge. The headline findings were as follows:

- Cyber-attacks are an issue. 64% said they had experienced cyber-attacks in the last year, 30% in the last month, 15% in the last week. Older respondents and those in management or sales jobs had experienced more attacks. Men were more likely to have experienced recent attacks than women.
- People are aware of the dangers of cyber-attacks. In general, survey respondents took cyber-security seriously. 82% agreed or strongly agreed that "A data breach would be disastrous for my organization" and only 13% agreed or strongly agreed that "If my organization did have a data breach, it would only be a public relations issue".
- Security behavior is mostly good. Most respondents reported good security behaviors (such as using a password) and were less likely to report having poor behaviors (such as leaving a note of the password next to their computer). On average, respondents scored above the mid-point on three scales of cyber-security attitude and behavior. The three scales were *Conscientiously follows rules* (3.74 on a 5-point scale), *Keeps passwords and devices secure* (4.00), and *Knowledge-informed carefulness* (3.44).
- Short versions of each of these scales have been produced and individuals can use them to assess their own cyber-security attitudes and behavior.
- There was a high general level of security knowledge among respondents, though a minority were unaware of some risks. For example, 10% thought it was OK to use a password-protected public Wi-Fi network for sensitive activities such as online banking. Almost all the group could distinguish between strong and weak passwords.
- There was a significant positive correlation between the cyber-security knowledge questions and scores on the scales of cyber-security attitude and behavior.

- Individuals working in computing or other IT roles were, as expected, higher than other job types on all three cyber-security attitude and behavior scales, on security knowledge, and on use of passwords. They were also higher on an overall cyber-security score that combined the attitude and behavior scales, security knowledge, and password use.
- The same pattern was seen for those working in organizations where the main function of the business was IT, compared with those working in other types of organization.
- Several personality differences were seen in relation to cyber-security attitudes, knowledge and password use:
  - Respondents with preferences for Introversion scored higher on Knowledge-informed carefulness than those with a preference for Extraversion and they had a higher knowledge score
  - Respondents with preferences for Sensing scored higher on Conscientiously follows rules than those with a preference for Intuition
  - Respondents with preferences for Thinking scored higher on Knowledge-informed carefulness and had a higher overall cyber-security score than those with a preference for Feeling
  - Respondents with preferences for Judging scored higher on Conscientiously follows rules and Keeps passwords and devices secure than those with a preference for Perceiving and had a higher overall cyber-security score.

  While these findings have informed the development of personality-specific guidelines for cyber-security, it is not the case that the MBTI assessment, or any other measure of psychological type, should be used in selection.
- Similar results are seen when looking at whole type preferences.
- One size does not fit all, and personality-specific advice can be useful. The data has been used to produce information and cyber-security guidelines for people of each MBTI type preference.

Introduction and methodology

Introduction

The World Economic Forum has identified data fraud and cyber-attack as major issues facing society (World Economic Forum, 2019). Cyber-crime is a growing problem and cyber-security is of increasing importance. Cyber-crimes may be 'syntactic' (exploiting technical weaknesses in software and systems to secure personal data), semantic (social engineering, exploiting the psychology of individuals) or a blend of both (Smith, 2010). In a 2019 survey of 1,700 IT professionals, 78% reported a successful cyber-attack within the last year (Cyberedge Group, 2019), and identified detection of rogue insiders and other insider attacks as one of the threats that organizations are least prepared for. Rogue insiders are current or former employees, contractors or others who can access an organization's IT network or systems and who have carried out malicious attacks.

While much research has focused on these rogue insiders (for example, Cappelli, Moore, & Trzeciak, 2012), less attention has been paid to the unintentional or accidental insider. These individuals do not have malicious intent but can still compromise an organization's IT network or systems via their accidental actions. They can be equally as damaging as malicious insiders, and many organizations have put much effort into staff training and education in order to mitigate this threat. Indeed, this 'human factor' is often seen as the weak link in information security (Metalidou, et al., 2014). However, a 'one size fits all' approach may not always be effective. Individual differences exist in all aspects of human behavior, and cyber-security is unlikely to be an exception. It would therefore be advantageous if employees could identify their individual susceptibility to different forms of cyber-threat.

Several specialized scales have been developed to examine the human factors influencing security behavior. They've been used to identify how likely an employee is to become an accidental insider, or how personality relates to the types of attack an individual is more susceptible to. These include 'SeBIS', the Security Behaviour Intention Scale (Egelman & Peer, 2015) and 'HAIS-Q', the Human Aspects of Information Security Questionnaire (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014). These are, however, for the most part, specialized research instruments, not widely used by organizations. Conversely, The Myers-Briggs Type Indicator (MBTI) model of personality (Myers, McCaulley, Quenk, & Hammer, 2018) is already widely used for self-development by organizations and individuals (Furnham, 2017). It therefore provides a useful starting point for personality-based guidelines for the many people who already know their MBTI personality type. The MBTI approach looks at four areas of personality type (Extraversion or Introversion, Sensing or Intuition, Thinking or Feeling and Judging or Perceiving) and at how these combine dynamically to describe the whole person. The model is described in detail in Appendix A.

This study set out to identify the relationship between the MBTI model and cyber-security behavior, and thereby develop personality-based guidelines. It is the first to look specifically at how MBTI type relates to cyber-security, and one of only a small number of studies to address the link between cyber-security behavior and personality.

Methodology

To carry out the study, we created an online survey. This was publicized via LinkedIn, Facebook, online forums, on The Myers-Briggs Company website (https://www.themyersbriggs.com) and by direct communication to individuals who had previously completed the MBTI assessment online.

Participants were asked to give their MBTI best-fit (validated) four-letter type, and for a range of background information including their gender, age, employment status, the country in which they worked, job role and level, the size and principal function of their organization, and what IT support they had available. They also completed 40 questions relating to their views on both cyber-security and their role, and they were asked how recently they had experienced phishing or other cyber-attacks. Finally, they answered a number of questions relating to their cyber-security knowledge, based in part on questions adapted from the Microsoft *Test your internet security* online quiz (Microsoft, 2019), but with a number of new items added.

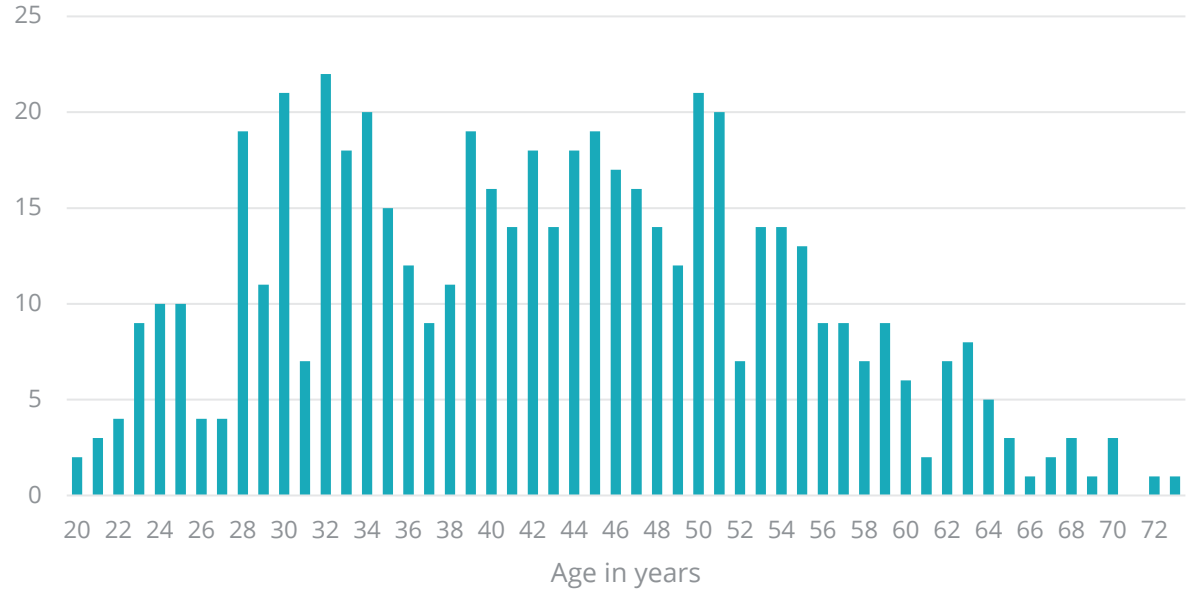
The analysis is based on data from 563 people who completed the online survey.

Results

Who took part? Description of the sample

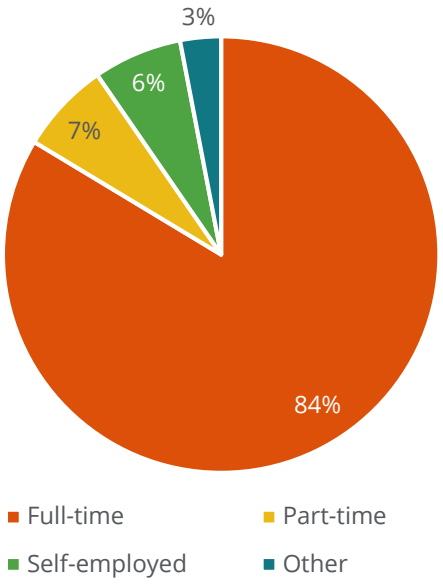
Group demographics

63% of the group were female, and 36% male, with 1% preferring not to say or to self-describe. Age ranged from 20 years to 73 years, with an average (mean) of 43 years:

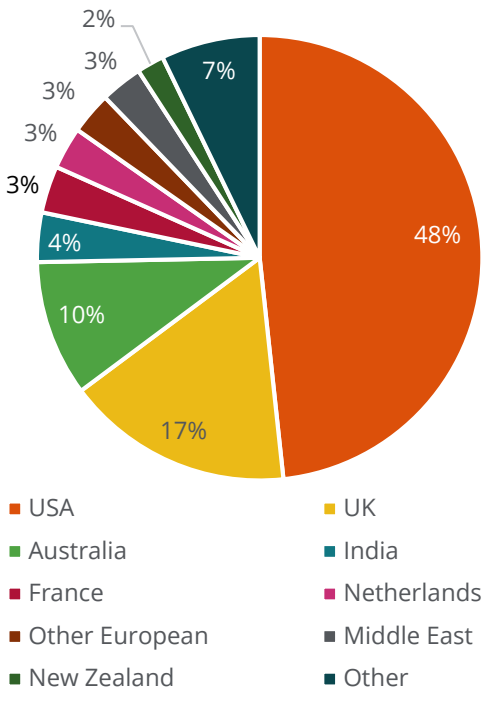


Most respondents (84%) were employed full-time by an organization. Just under half worked principally in the United States, though 40 different countries were represented in total.

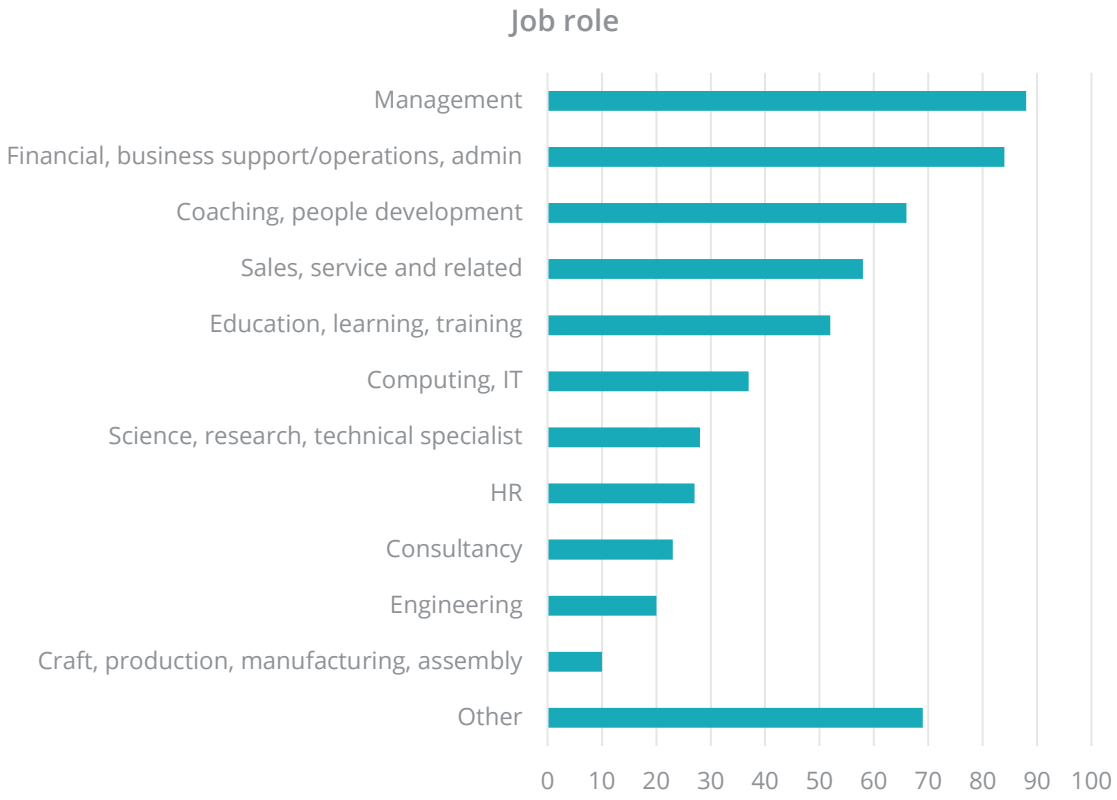
Employment status



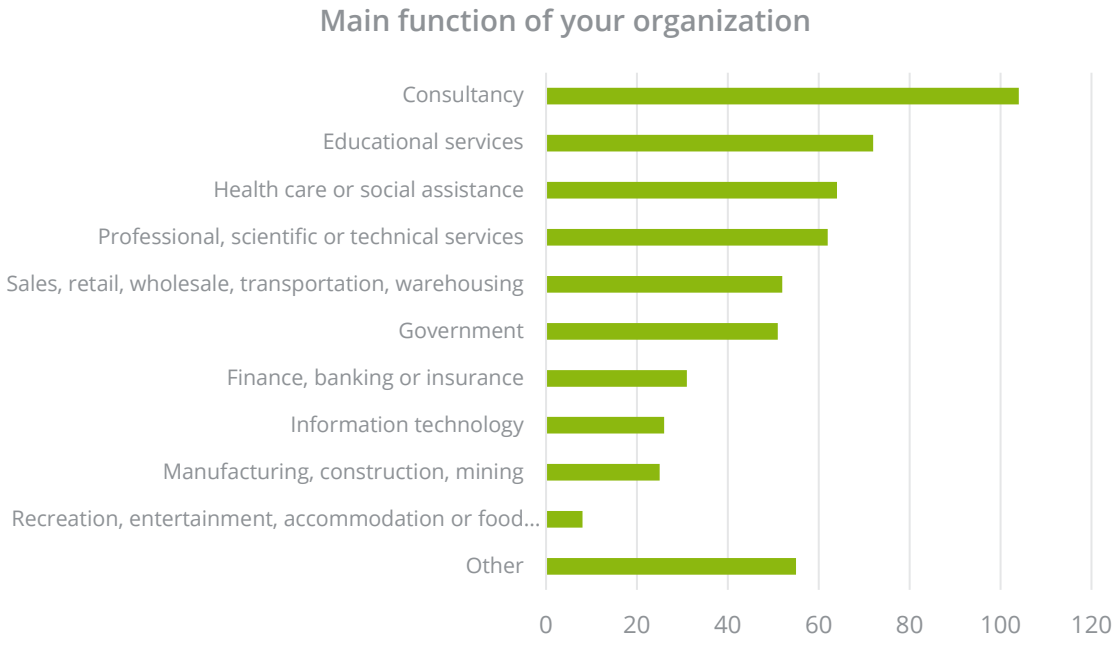
Country you principally work in

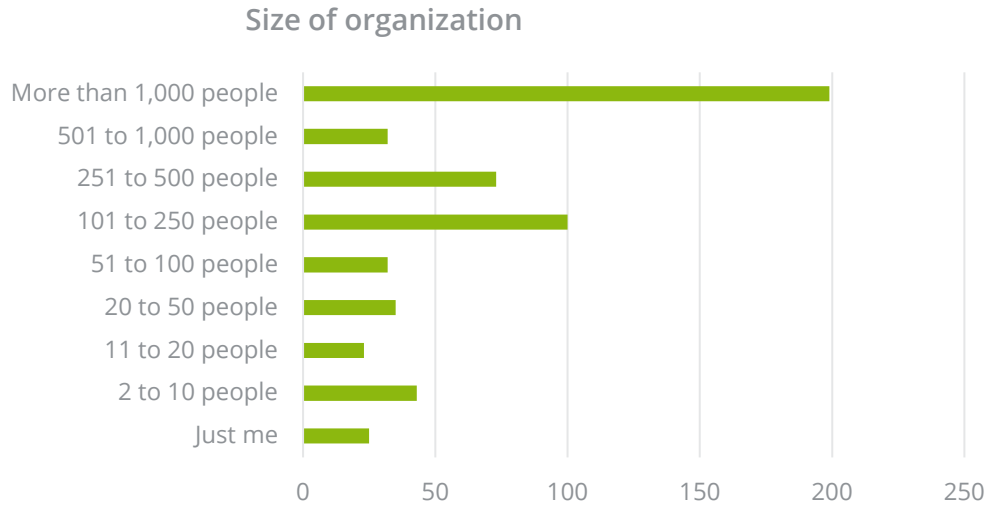


A range of job roles and levels were represented.

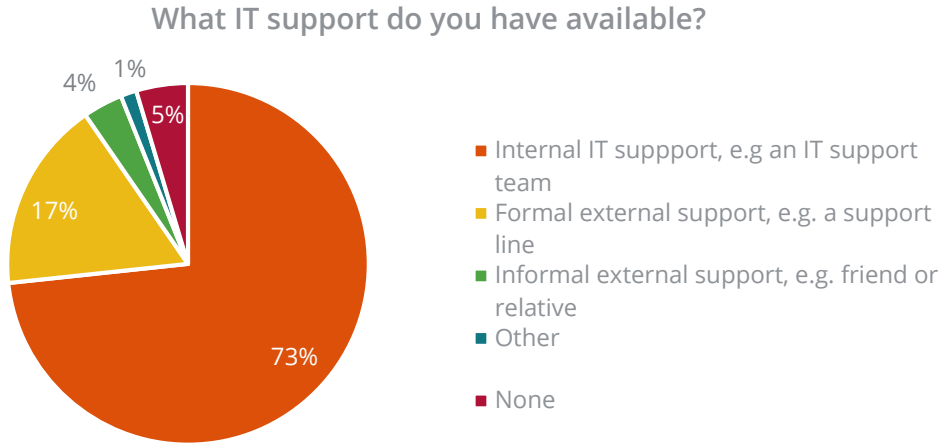


Survey respondents worked for a wide range of organizations, in terms of both function and size.



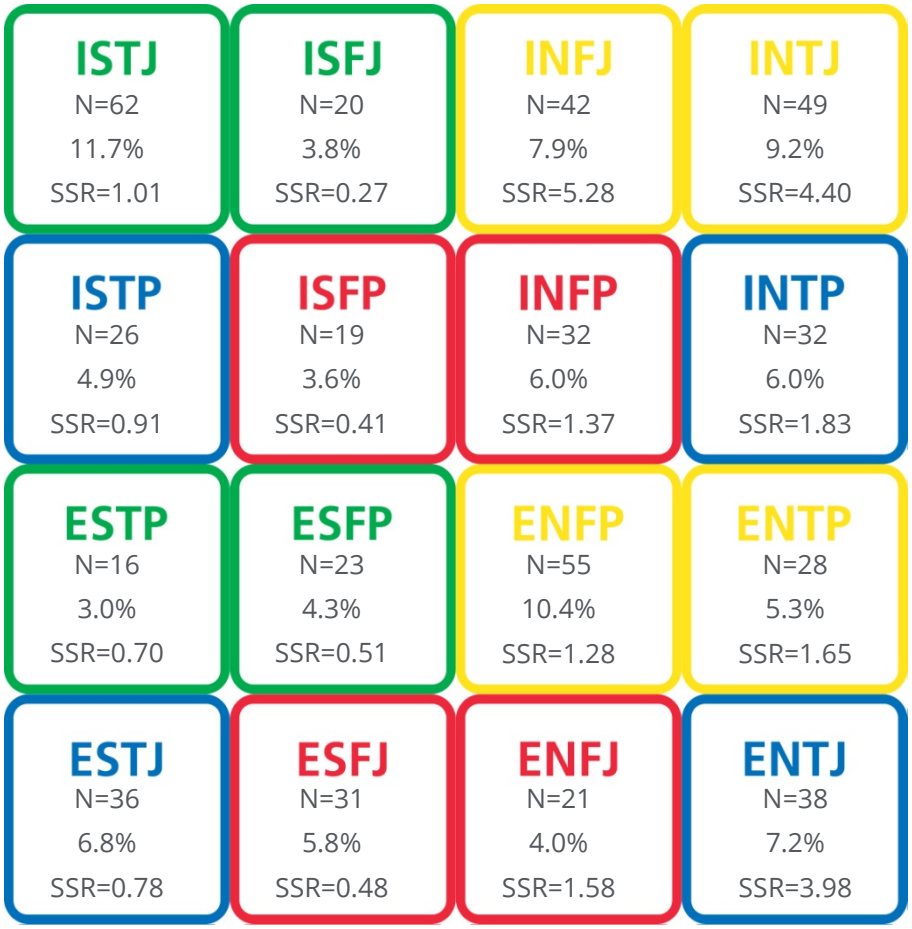


Most respondents had access to internal IT support within their organization.



Type distribution

Type data was available for 530 individuals. A type table for this group is shown below:



Type	N	%
E	248	46.8%
I	282	53.2%
S	233	44.0%
N	297	56.0%
T	287	54.2%
F	243	45.8%
J	299	56.4%
P	231	43.6%

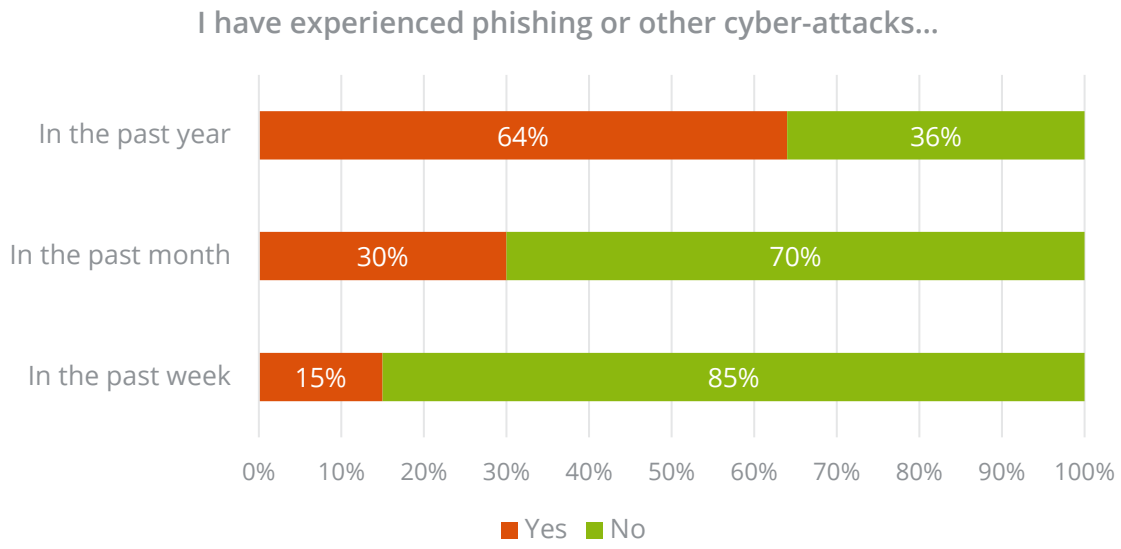
The SSR (Self-Selection Ratio) compares the sample to the general population. Types with an SSR greater than 1 are over-represented in this group compared with the general population.[1] All Intuition types are therefore over-represented, and most Sensing types under-represented. This is not uncommon in a group of people interested in personality type. However, there are sufficient numbers of each type in the sample to carry out meaningful analyses.

[1] The US national representative sample (Myers, McCaulley, Quenk, & Hammer, 1998) was used as a reference group

Experience of cyber-attacks

Overview

Survey respondents were asked whether they had experienced phishing or other cyber-attacks in the last year, the last month, and the last week. Just under two-thirds believed they had been the subject of a cyber-attack in the last year; 15% believed they had experienced such an attack in the past week.



Personality differences

It seems unlikely that an individual's personality type would influence how often they are subject to phishing or other cyber-attacks, and no links were hypothesized. Only one statistically significant personality difference was found between preference pairs[2]; respondents with a preference for Introversion were more likely to say they had experienced an attack in the past month than those with a preference for Extraversion. No statistically significant differences were found with whole type.

Group differences

Some targets may be more attractive for cyber-criminals than others. Existing research suggests that the frequency of successful cyber-attacks varies from country to country (Cyberedge Group, 2019), that larger organizations are targeted more often than smaller ones, and that some types of organization (e.g. national security) are targeted more often than others (e.g. agricultural services) (Thonnard, Bilge, Kashyap, & Lee, 2015). On an individual basis, older people, and especially the elderly, may be targets (James, Boyle, & Bennett, 2014). Women may be more likely to respond to 'spear-fishing' attacks, which utilize personal information about their intended victim (Halevi, Memon, & Oded, 2013).

[2] Based on chi-squared analysis

Some statistically significant[3] group differences were found in our data:

- Men are significantly more likely than women to say that they have experienced cyber-attacks in the last month and the last week. This contrasts with the findings of Halevi et al., though other research by some of the same authors (Halevi, Lewis, & Memon, 2013) suggests that there may be only a limited correlation between the perception and the reality of being phished.
- Those employed full-time were significantly more likely than those employed part-time to say that they have experienced cyber-attacks in the last week.
- Those in management roles, and in sales, service and related jobs, are more likely than others to say they have experienced cyber-attacks in the last year. Those in sales are also more likely to have experienced such attacks in the last week.
- People based in the USA and UK are more likely than others to say that they have experienced cyber-attacks in the last year, week and month.
- Older respondents were more likely to have experienced cyber-attacks. The average ages of those who said they had experienced cyber-attacks in the last year, month and week were all significantly higher than those who had not[4].

In contrast to the work of Thonnard et al., no statistically significant relationship was found between frequency of cyber-attacks and organization type or organization size.

[3] Based on chi-squared analysis
[4] Based on independent-samples t-tests

Views on cyber-security and job role

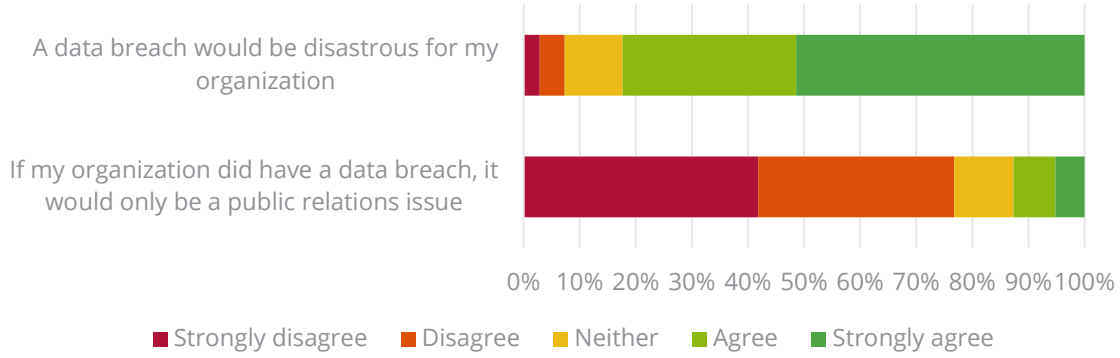
Overview

Survey respondents were asked 40 questions about their views on cyber-security and on their job role, using a scale from strongly disagree to strongly agree. The average (mean) score on each question is shown below.

The overall data do suggest that in general, respondents did have good security behaviors (such as using a password) and were less likely to have poor behaviors (such as leaving a note of the password next to their computer).

The importance of cyber-security

The data suggest that most respondents took cyber-security seriously. 82% agreed or strongly agreed that "A data breach would be disastrous for my organization" and only 13% agreed or strongly agreed that "If my organization did have a data breach, it would only be a public relations issue".



For the first statement, those working in large organizations were most likely to agree, as were those with formal IT support (especially internal support) and those whose role was as a first line manager or supervisor. Owners and CEOs were the least likely to agree [5].

Those working in medium-sized organizations of between 11 and 50 people were the most likely to see a data breach as only a PR issue. Those who were self-employed or in larger organizations saw this as more important[6], as did those with personality preferences for Extraversion[7].

Cyber-security dimensions

Previous researchers have investigated cybersecurity attitudes and behaviors and proposed several possible dimensions or scales. For example, Kelley (2018) distinguished between *cyber hygiene* (proactively minimizing vulnerabilities to maintain system security) and *threat response* (the ability to prevent an attack from occurring by responding to a specific threat and being able to stop an occurring attack). Others have developed specific scales or questionnaires, such as the Cybersecurity Attitudes Scale (Howard, 2018), HAIS-Q, the Human Aspects of Information Security Questionnaire (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014) or SeBis, the Security Behavior Intentions Scale (Egelman & Peer, 2015).

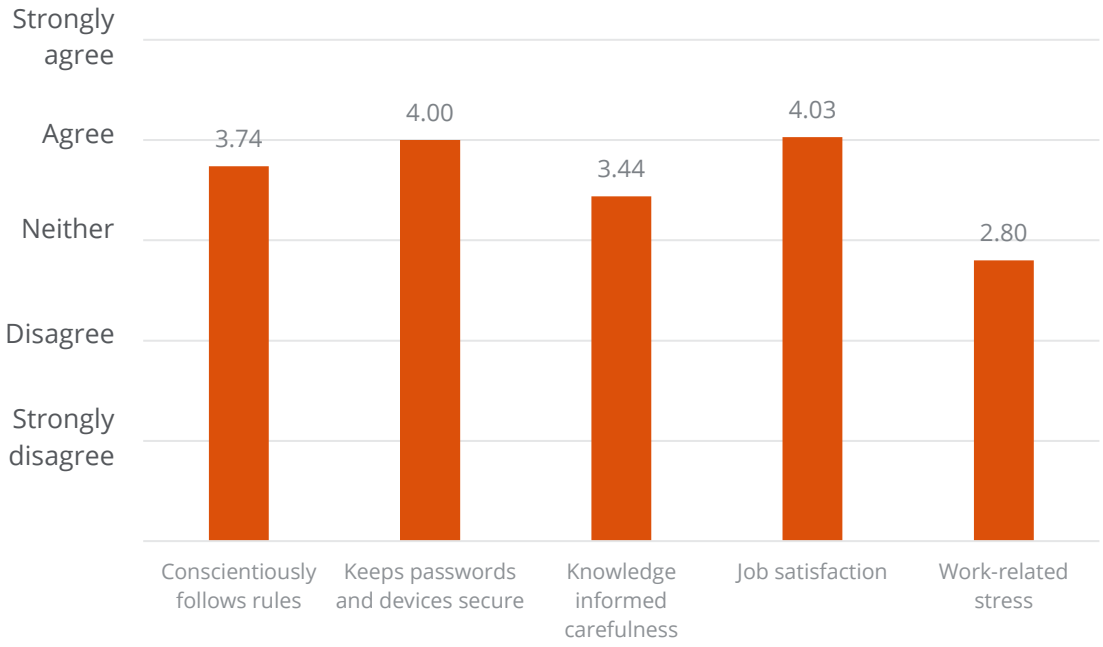
Informed by previous research but derived from factor and item analysis of the dataset, three scales of cyber-security attitudes and behaviors were derived from the 40 items. In addition, short scales of job-satisfaction and work-related stress were produced. All had acceptable to

[5] Based on one-way analyses of variance.
[6] Based on one-way analyses of variance.
[7] Based on an independent-samples t-test.

good internal consistency reliability (coefficient alpha). A shorter self-scorable version of the cyber-security scales can be found in Appendix B.

Scale	Items	Alpha
Conscientiously follows rules	Everyone in my organization has a role to play in IT security I always follow all the IT security rules and procedures in my organization (-) I can't be bothered to read security briefings or emails (-) I do things in my own way I have never ignored or contravened any of the IT security rules in my organization (-) I have not always reported phishing attempts or other cyber-attacks (-) If I discover a security problem, I continue what I was doing; someone else will fix it In my organization there are clear rules and procedures on cyber-security (-) Many of the rules about IT security don't really apply to me (-) My organization's rules cyber-security rules and procedures get in the way of productivity (-) There are a lot of stupid rules about IT security in my organization	0.773
Keeps passwords and devices secure	(-) I am often one of the last to realize that a new process or protocol has been put into place I manually lock my computer screen when I step away from it (-) I only use a password because my IT administrator makes me do so I set my computer screen to automatically lock if I don't use it for a prolonged period I use a password or passcode to unlock my laptop or tablet (-) I write down my password (-) Occasionally I will write down a password and leave this note next to my computer	0.651
Knowledge-informed carefulness	I know the difference between websites that have a "http" address and a "https" address (-) I submit information to websites without first checking that it will be sent securely (e.g. SSL, https: or a 'lock' icon (-) I use the same password for most accounts and apps If I am browsing a website, I mouseover (hover over) links to see where they go, before clicking on them (-) If I can, I will re-use the same password (-) If I get an email from someone I know personally, it's OK to open any attachments (-) When someone sends me a link, I usually open it without first checking where it goes	0.757
Job satisfaction	I enjoy my work I have a great deal of job satisfaction My work is interesting	0.883
Work-related stress	I'm having a hard time at work at the moment My job is often stressful Work is quite stressful at the moment	0.752

Each individual question was scored on a scale from strongly disagree to strongly agree, 1 to 5. The chart below shows the average (mean) score for the items in each scale.



On average, respondents tended to have high levels of job satisfaction and to believe that they keep passwords and devices secure.

There are some inter-correlations between the security scales, but these are small enough to allow the scales to be treated as separate dimensions.

	Follows rules	Keeps secure	Carefulness	Job satisfaction	Work-related stress
Follows rules	1	.470**	.421**	.141**	-.197**
Keeps secure		1	.483**	.202**	-.100*
Carefulness			1	.129**	.109*
Job satisfaction				1	-.289**
Stress					1

Personality differences in cyber-security and job scales

Four scales – *Conscientiously follows rules*, *Keeps passwords and devices secure*, *Knowledge-informed carefulness* and *Job satisfaction* – show significant differences with one or more of the MBTI preference pairs[8]:

- Those with a preference for Sensing, and those with a preference for Judging, score significantly higher on *Conscientiously follows rules*
- Those with a preference for Judging score significantly higher on *Keeps passwords and devices secure*
- Those with a preference for Introversion, and those with a preference for Thinking, score significantly higher on *Knowledge-informed carefulness*
- Those with a preference for Extraversion, and those with a preference for Intuition, score significantly higher on *Job satisfaction*.

These differences are summarized in the table below, where 'd' refers to Cohen's d, a statistic used to describe the size of the difference between any two preferences. These differences are statistically significant but relatively small.

Cybersecurity scale	E–I	d	S–N	d	T–F	d	J–P	d
Conscientiously follows rules	-	-	S	0.18	-	-	J	0.29
Keeps passwords and devices secure	-	-	-	-	-	-	J	0.23
Knowledge-informed carefulness	I	0.18	-	-	T	0.25	-	-
Job satisfaction	E	0.26	N	0.18	-	-	-	-

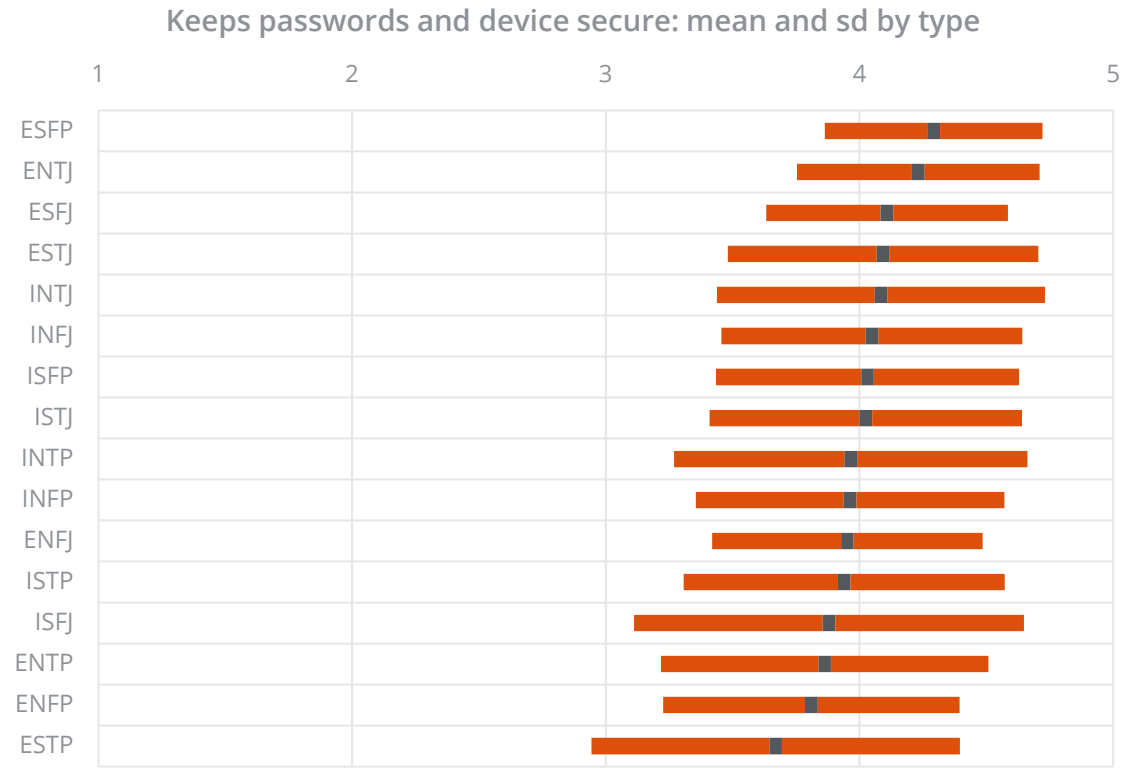
At preference pair level, there were no significant differences in *Work-related stress*.

These findings are broadly in agreement with previous research using the Five Factor Model of personality. The research found that Extraversion and Conscientiousness related to a lower likelihood to violate cybersecurity policies (McBride, Carter, & Warkentin, 2012), and Conscientiousness to a lower likelihood to take risks and a greater likelihood to follow the rules (McCormac, et al., 2017).

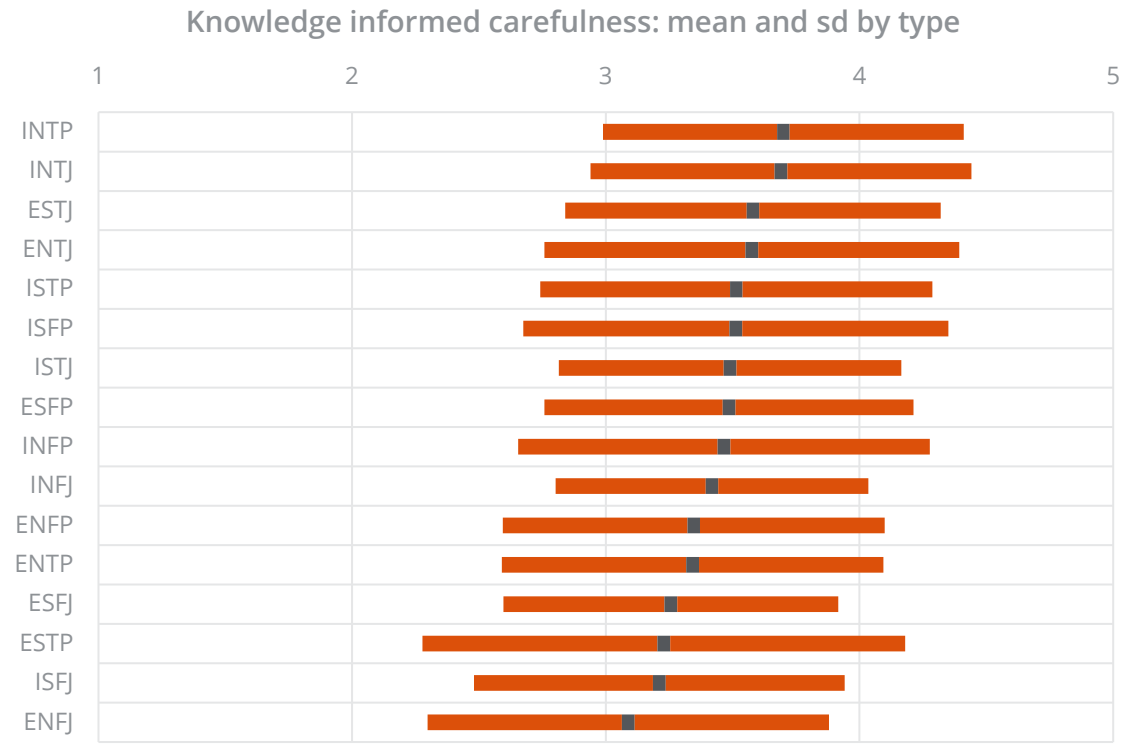
Each of these scales also showed a statistically significant relationship with whole type[9]. As with the preference pairs, there was no significant relationship with stress. The charts on the following pages show the mean (indicated by the black square) and standard deviation (orange bars) of each scale for each type. Note that though there are significant differences between types, no type has an average score below the mid-point of 3 for any scale. On the whole, the sample were conscious of and careful with cyber-security.

[8] Based on independent-samples t-tests.
[9] Based on one-way analyses of variance.

Those with ES_J preferences are the most likely to conscientiously follow the rules; those with E_TP the least likely.



Those with ESFP and ENTJ preferences are the most likely to say that they keep devices and passwords secure; those with ESTP preferences are the least likely.



In general, those with a Thinking preference score higher on this scale, in particular INTP and INTJ. Those with a preference for ENFJ have the lowest score.

Although INTP is the type with the highest level of job satisfaction, in general those with preferences for Extraversion tend to be higher here. These results are consistent with other research. For example, a large-scale study by Boult, Thompson, & Schaubhut (2019) found that those with preferences for ISTP had, on average, the lowest overall levels of well-being.

Group differences

There were several demographic differences[10]:

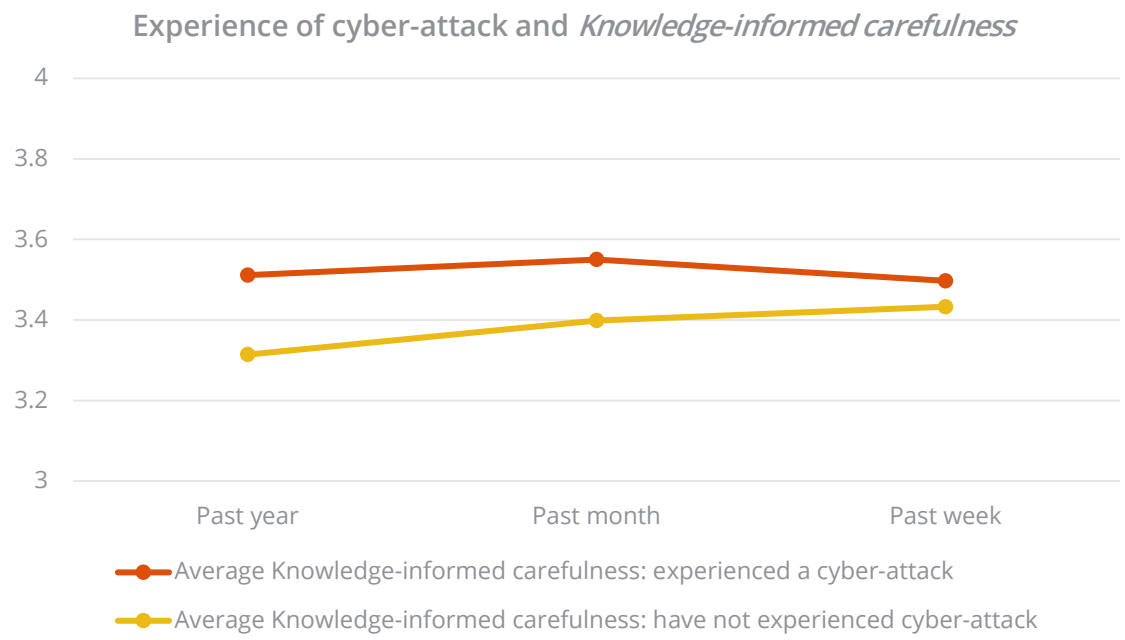
- On average, men scored more highly than women on Keeps passwords and devices secure and Knowledge-informed carefulness[11].
- Older respondents tended to score higher on Conscientiously follows rules, Knowledge-informed carefulness and Job satisfaction[12].
- Those who were self-employed reported higher levels of *Job satisfaction* than other groups.
- Those working in the United States were on average the highest on *Conscientiously follows rules*, significantly more so than those working in India, who were the lowest. UK and Australian respondents also scored significantly higher than Indian workers.
- Individuals working in computing or other IT roles were, on average, the highest on *Conscientiously follows rules*, *Keeps passwords and devices secure* and *Knowledge Informed carefulness*. They were significantly higher:
  - On *Conscientiously follows rules* than those in consultancy, education, engineering or scientific jobs
  - On *Keeps passwords and devices secure* than those in all other job categories
  - On *Knowledge-informed carefulness* than those in coaching, education, engineering, financial/business, HR, sales, scientific or management jobs
- A similar pattern was seen when looking at the whole organization. Individuals working in organizations where the main function of the business was IT were, on average, the highest on *Conscientiously follows rules*, *Keeps passwords and devices secure* and *Knowledge Informed carefulness*. They were significantly higher:
  - On *Conscientiously follows rules* than those in consultancy, educational, professional services or sales organizations
  - On *Keeps passwords and devices secure* than those in all other types of organization except manufacturing
  - On *Knowledge-informed carefulness* than those in all other types of organization except manufacturing and recreation, accommodation and food services.
- Owners or CEOs of organizations showed the highest level of *Job satisfaction*, significantly higher than all other levels except executive management. There was a steady reduction in average job satisfaction from Owner/CEO, through levels of managers, to employee level. Those at employee level showed significantly lower levels of job satisfaction than all other levels.
- Organization size did not show a consistent relationship with the three cyber-security scales, though the self-employed showed the highest level of job satisfaction.
- Respondents with access to internal IT support were the most likely to *Conscientiously follows rules* and to exhibit *Knowledge-informed carefulness.*

[10] Unless stated otherwise, all significant differences quoted on this page are based on one-way analyses of variance.
[11] Based on independent-samples t-tests.
[12] Based on bivariate correlations of .169, .174 and .255 respectively, all significant at the 1% level.

Relationship with experience of cyber-attack

It was hypothesized that individuals with a higher score on *Knowledge-informed carefulness* would be more likely to realize that they had experienced a cyber-attack, and hence would be more likely to say that they had experienced such an attack. It was also hypothesized that those who had experienced an attack might have a higher degree of *Work-related stress*.

A significant relationship[13] was found with *Knowledge-informed carefulness.* Those who had experienced cyber-attacks in the last year or last month were significantly higher on this scale. No significant relationship was found with *Work-related stress* or any scale other than *Knowledge-informed carefulness*.

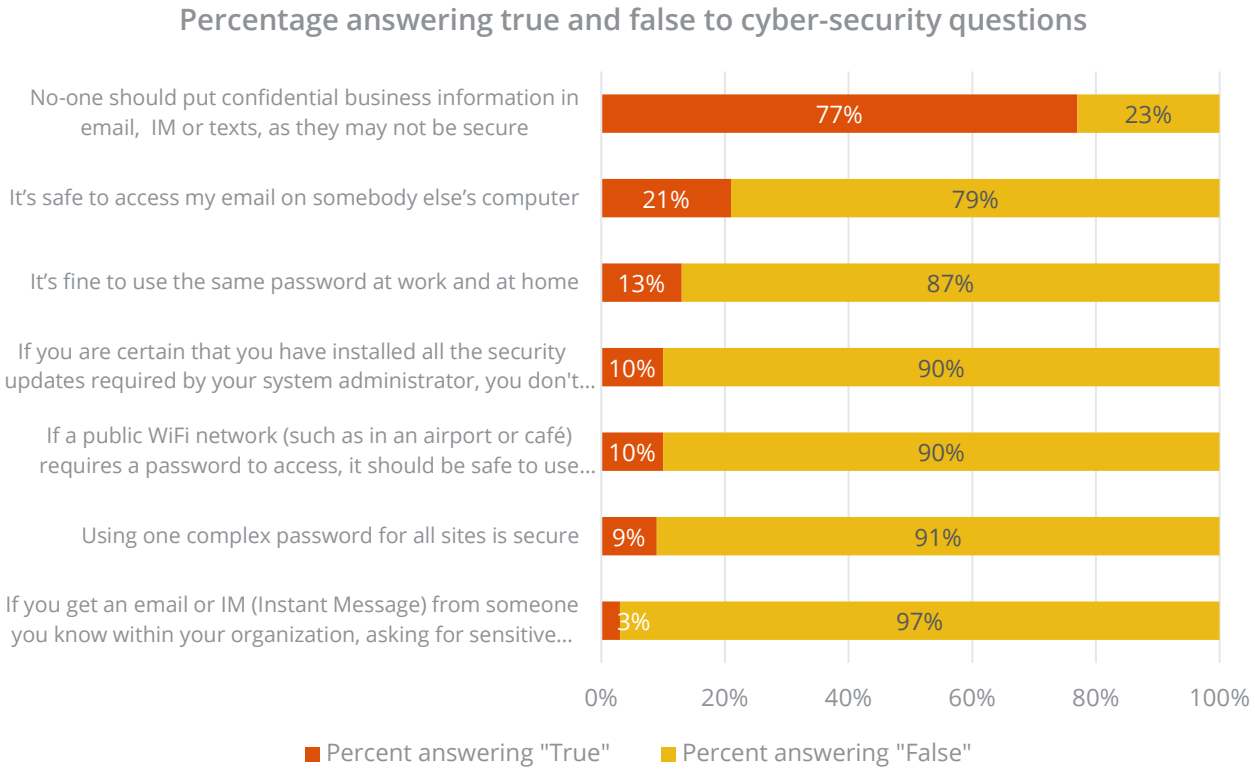


[13] Based on an independent-samples t-test

Cyber-security knowledge

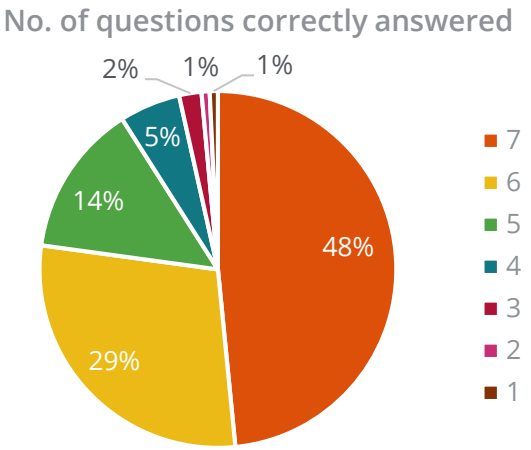
Overview

The cyber-security knowledge of survey respondents was assessed using a combination of questions adapted from the Microsoft *Test your internet security IQ* online quiz (Microsoft, 2019) and new items. Seven true/false questions measured general cyber-security knowledge. In each case, most respondents chose the correct answer. In the chart below, the questions have been re-ordered according to the percentage of respondents who answered 'true'.



Only the first question has 'true' as a correct answer. While some questions were seen by almost everyone as examples of poor cyber-security, others were seen as OK by a significant minority of respondents.

Overall, just under half of respondents answered every question correctly and no-one chose the wrong answer for every single question. The number of correct answers achieved by each respondent was summed to give an overall knowledge score.



Relationship with personality, cyber-security scales, and other factors

There were no personality differences in overall knowledge score between Sensing and Intuition, Thinking and Feeling, or Judging and Perceiving, but those with a preference for Introversion on average achieved a significantly higher score than those with a preference for Extraversion[14]. Further analysis shows that this difference comes principally from three questions. Extraverts are more likely than Introverts to agree that "if you get an email or IM (Instant Message) from someone you know within your organization, asking for sensitive personal information, it's OK to supply this" and that "if you are certain that you've installed all the security updates required by your system administrator, you don't need to worry about computer viruses". Introverts are more likely than Extraverts to agree that "No-one should put confidential business information in email, IM or texts, as they may not be secure".

Overall knowledge score showed statistically significant correlations (at the 1% level) with *Knowledge-informed carefulness* (r=0.389), *Conscientiously follows rules* (r=0.295) and *Keeps passwords and devices secure* (r=0.184). Correlations with Job satisfaction and Work-related stress were nonsignificant and close to zero. These results demonstrate that there is a relationship between views on and attitudes towards cyber-security and cyber-security knowledge.

Those who had experienced phishing or cyber-attacks in the last year had a significantly higher overall knowledge score than those who had not[15]. No significant difference was found between those who had or had not experienced an attack in the last month, or the last week. It may be that, following an attack, it takes time for an individual to build up their cyber-security knowledge. Alternatively, the key difference may be between those who have never experienced a cyber-attack, and those who have. These results mirror the relationship between experience of cyber-attack and the scale of *Knowledge-informed carefulness*.

There was no significant difference in overall cyber-security score between men and women, or by employment type, job level, organization size or type of IT support available. However, two group differences were found:

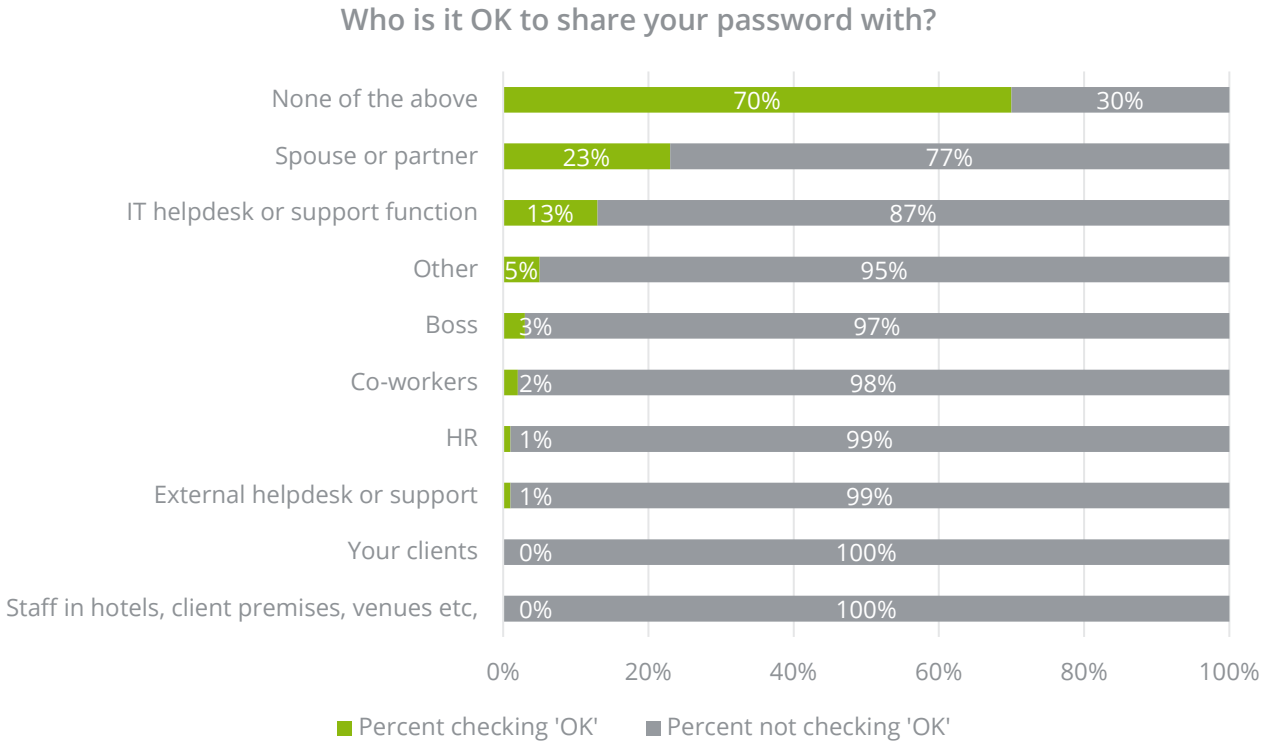
- Those working in computing or IT jobs showed the highest score on average (6.47 out of a maximum possible of 7) and those working in HR the lowest (5.63)
- Similarly, those working in IT sector organizations showed the highest average score (6.46), with those in the recreation, entertainment, accommodation and food sectors the lowest (5.75)

[14] Based on an independent-samples t-test
[15] Based on an independent-samples t-test

Use of passwords

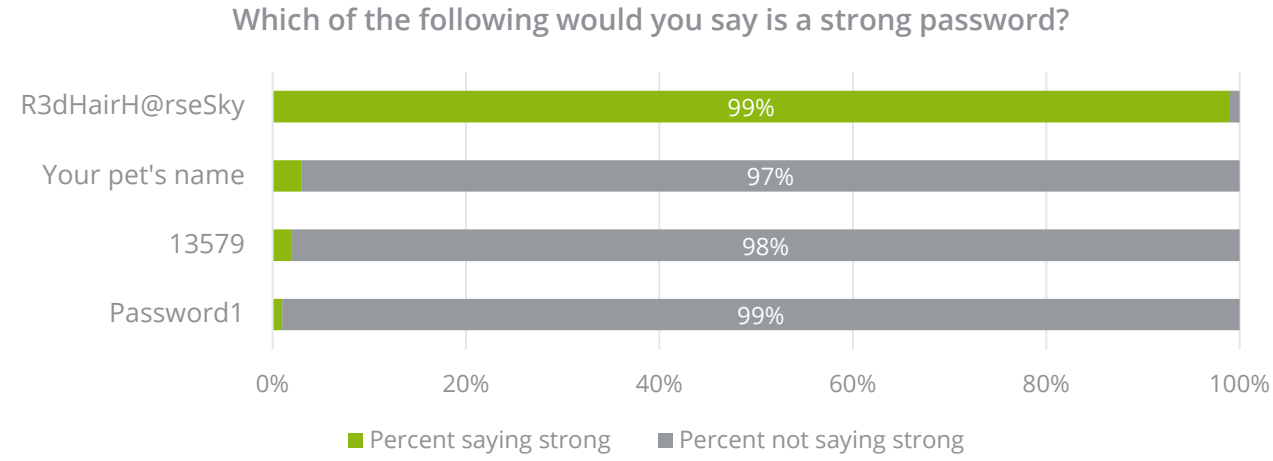
Overview

Respondents were also asked, “who is it OK to share your passwords with? Please check all that apply”. In the chart below, the questions have been re-ordered according to the percentage of respondents who checked each option.



Strictly, ‘none of the above’ is the only safe option. However, almost a quarter of respondents would share their password with their spouse or partner, and over 10% would share their password with their IT helpdesk or support function.

They were also given examples of possible passwords, and asked “which of the following would you say is a strong password?”

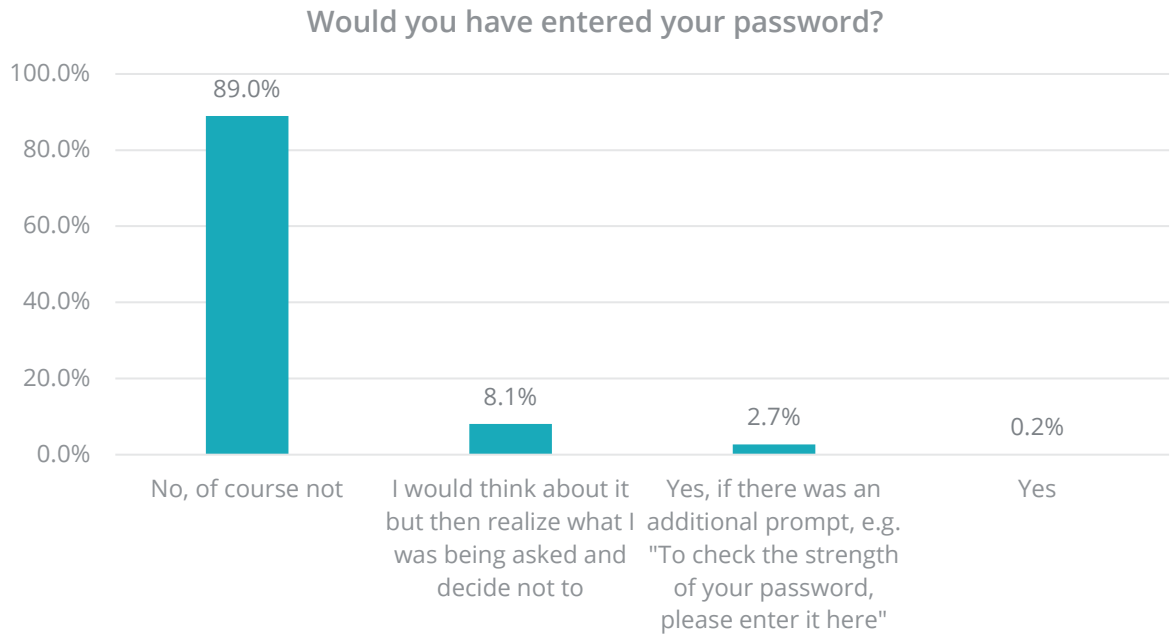


In this list, 'R3dHairH@rseSky' is the only strong password, and almost all respondents recognized it as such. 'Password1' is a very common business password, at the top of most cyber-criminals' lists to try; nevertheless, a small number of respondents identified it as strong.

The final question in the online survey, just after the question "which of the following would you say is a strong password", was this:

- If at this point, we had asked "and what is your password", would you have entered your password? Please answer this question honestly.

The responses to the four answer options to this question were as follows:



While most respondents would not have entered their password, around 3%, in the right circumstances, would have done so.

Relationship with personality, cyber-security scales, and other factors

For many of the password-related questions, almost everyone chose the 'correct', more security-conscious answer. Therefore, group differences were only investigated for the four questions where there was some variability in responding, specifically:

- Sharing passwords with 'none of the above'
- Sharing passwords with spouse or partner
- Sharing passwords with IT helpdesk or support function
- Would you have answered the question, 'if at this point, we had asked, what is your password, would you have entered your password'?

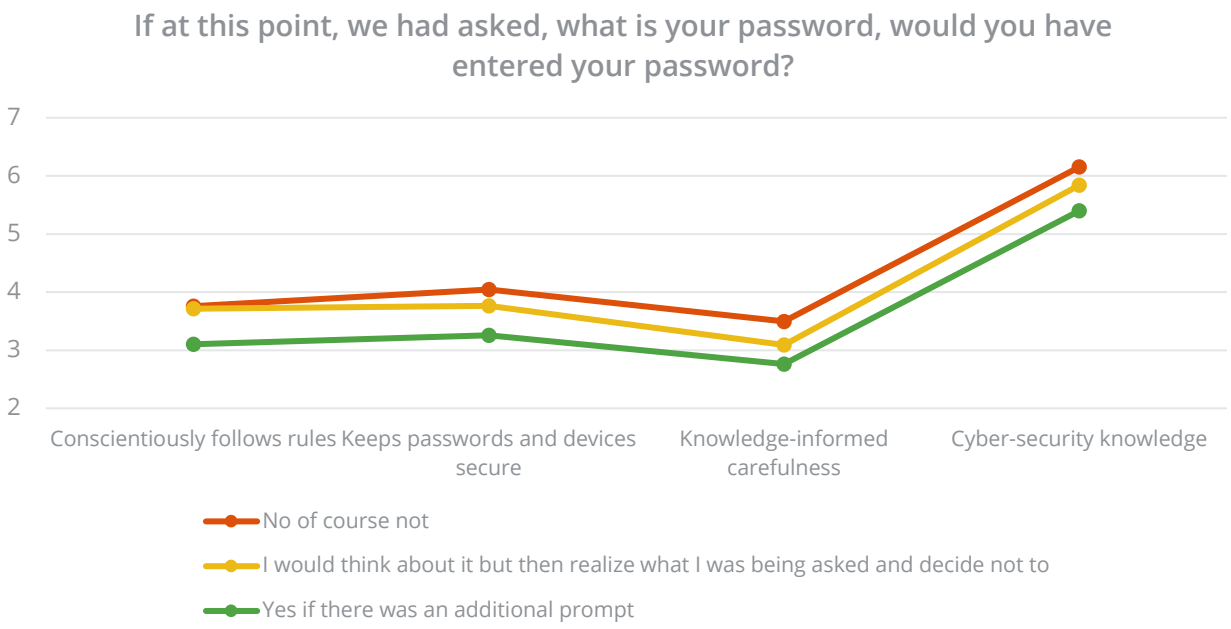
Only one personality-related difference was found. Those with a Sensing preference were more likely to choose 'none of the above' than those with an Intuition preference[16].

As expected, password use was related to the cyber-security scales and to cyber-security knowledge. Those who chose 'none of the above' scored higher on *Conscientiously follows rules*,

[16] Based on chi-square analysis

Keeps passwords and devices secure and *Knowledge-informed carefulness*, and had a higher knowledge score. Those who said they would share their password with their IT support function had a lower score on *Keeps passwords and devices secure* and *Knowledge-informed carefulness,* and had a lower knowledge score. The same applied for those who would share their password with their spouse or partner. This group also had a lower score on *Conscientiously follows rules*[17].

When asked, 'if at this point, we had asked, what is your password, would you have entered your password', those who chose 'No of course not' had significantly higher scores on all three cyber-security scales and on cyber-security knowledge[18].



There were several demographic differences[19]:

- Those who had experienced phishing or other cyber-attacks in the past year were more likely to share their password with 'none of the above' and less likely to share with their spouse or partner or with IT support
- Respondents working in the UK were less likely than others to share their password with their spouse or partner; those working in the USA were more likely
- Those working in computing or IT were more likely than others to share their password with 'none of the above' and to choose "No of course not", and less likely to share with their spouse or partner or with IT support
- Those working in larger organizations (501+) were more likely to share their password with 'none of the above' and less likely to share with IT support.
- Older respondents were more likely to share passwords with their spouse or partner (of course, they may be more likely to have a spouse or partner to share their password with) and less likely to share with IT support[20].

[17] All results based on independent t-tests
[18] Based on one-way analyses of variance
[19] Based on chi-square analysis, unless otherwise noted
[20] Based on independent-samples t-tests

Overall cyber-security score

Overview

An overall cyber-security attitude and behaviors score was computed by standardizing each of the three cyber-security scales, adding these together and standardizing the total. An overall cyber-security knowledge score was computed by totalling the true/false questions and adding a weighted total of the password questions (so as not to make the overall score overly weighted towards use of passwords). This score was then standardized. Details of these calculations are given in Appendix C.

There was a correlation of 0.425, significant at the 1% level, between these two scores. Those with a high score on overall cyber-security attitude also tend to have a high overall knowledge score.

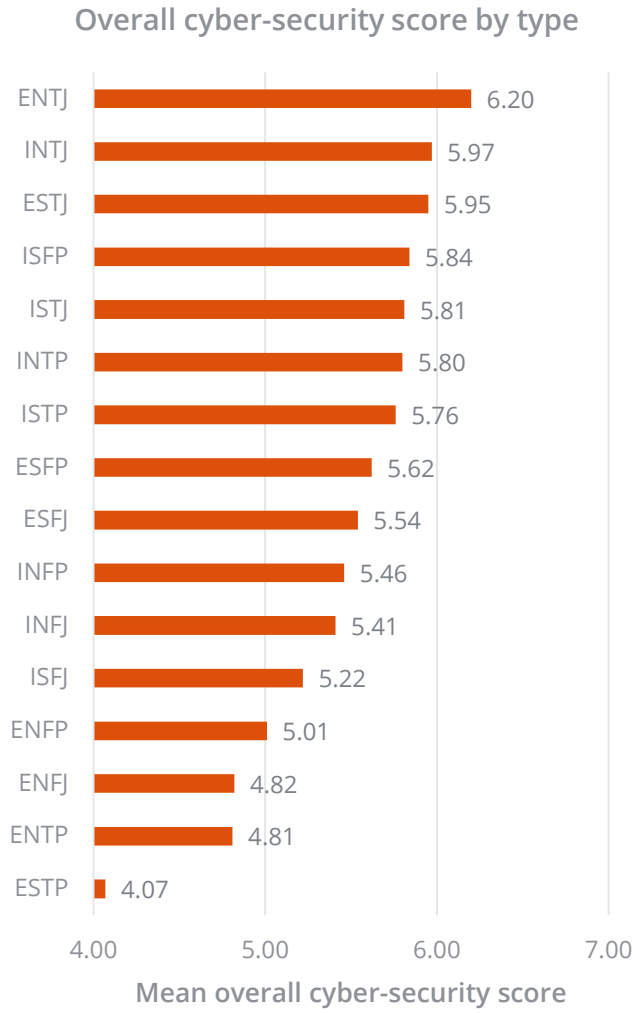
The two scores were added together and re-standardized as a 1–10 scale for each respondent. Details of this calculation are given in Appendix C. The distribution of the overall score is shown below.

Relationship with personality and other factors

Respondents with preferences for Thinking and for Judging had a significantly higher overall score than those with preferences for Feeling and for Perceiving[21]. However, these differences were small in absolute terms (Cohen's d of 0.27 and 0.30 respectively), as illustrated on the next page.

[21] Based on independent-samples t-tests

These relationships were reflected in statistically significant differences in overall score[22] between whole types and between favorite processes (dominant functions).



[22] Based on one-way analyses of variance

While these differences are interesting, it is not the case that the MBTI assessment, or any other measure of psychological type, should be used in selection. Rather, a detailed analysis of the likely strengths and possible vulnerabilities of each type can be used to produce personality-specific cyber-security guidelines. These are described in the next section.

There were no significant differences in overall cyber-security score[23] between men and women[24], by employment status, job level, or organization size, or in terms of which country respondents worked in. However, the following significant relationships were seen:

- Older respondents tended to have a higher score than younger respondents[25]
- Those working in computing or IT roles had on average the highest score (by some distance). Those working in education, training or learning roles had the lowest score, and those in HR the second lowest
- Those working in IT companies had, by some distance, the highest score on average
- Those with access to IT support had a higher score on average than those with no support
- Those who had experienced phishing or other cyber-attacks in the last year had a higher score on average than those who had not.

There were small but statistically significant (at the 0.1% level) correlations between overall cyber-security score, job satisfaction and work-related stress. Those with higher scores on cyber-security tended to have a higher degree of *Job satisfaction* (r=0.142) and a lower level *of Work-related stress* (r=-0.139).

[23] All significance testing based on one-way analyses of variance unless otherwise noted.
[24] Based on an independent-samples t-test.
[25] Correlation of 0.251, sig at 0.1% level, between age and overall cyber-security score.

Cyber-security guidelines

General guidelines

General guidelines on cyber-security are available from many sources. They include government-sponsored certification schemes such as the UK government 'cyber-essentials' programme (National Cyber Security Centre, 2019), academic papers (for example, Sotira, 2018), and a wealth of guidelines and suggestions from commercial organizations. This study set out to develop personality-specific guidelines rather than general ones, and it is not the intention to produce a set of general guidelines here. Nevertheless, the data suggest that some poor cyber-security behaviours are carried out more frequently than others. These more common security mistakes are listed below.

- Submitting information to websites without first checking that it will be sent securely (e.g. SSL, https: or a 'lock' icon)
- Assuming that it is safe to access one's email on someone else's computer
- Re-using the same password where one can
- Using the same password at work and at home
- Using the same password for most accounts and apps
- Sharing passwords with one's spouse or partner
- Over-confidence that one won't be caught out by cyber-attacks
- Assuming that if you have installed all the security updates required by your system administrator, you are 100% safe and don't need to worry about viruses
- Assuming that if a public network is passworded, it is safe enough to use for sensitive activities (such as online banking).

Type-based advice

Overview

People of each type preference will have their own particular strengths when it comes to cyber-security, but also things that they should look out for. The following pages present information and advice for each type. This can be used by individuals looking for hints and tips about their own cyber-security behaviour, and by cyber-security professionals who need to work with and communicate to people of every MBTI type.

ISTJ

People with ISTJ preferences typically put a great deal of trust in their detailed memories of past experiences and facts. As such, they are less likely than most to be caught out twice by the same cyber-attack. They are also less likely than others to be susceptible to emotional appeals in phishing emails, and more likely to spot the sort of discrepancies and errors that sometimes give away phishing attacks. They are likely to know rules and policies around IT security, and to be careful with sensitive or confidential information. They were also less likely than most to think it was OK to use the same password at work as at home.

However, while ISTJs are keen to follow the rules, they can become frustrated when these seem illogical, outdated or inefficient. This may, for example, extend to the use of passwords; some ISTJs will find it irritating if they must change their passwords frequently or are forced to have different passwords for different applications. ISTJs may be less quick than others to find out that a new phishing scheme is circulating, or to find out from others that a cyber-attack is under way. Some ISTJs may over-rely on past experience, which may lay them open to new forms of cyber-attack.

ISFJ

ISFJs typically put a great deal of trust in their memories of past experiences and how these felt and are therefore less likely than most to be caught out twice by the same cyber-attack (though our data suggests that this knowledge may lead to a degree of over-confidence for some ISFJs).

ISFJs tend to put their trust in people and value being treated as an individual. In terms of cyber-security, this may open them up to social engineering attacks where a malicious agent masquerades as a trusted acquaintance. Less skilful attacks will however fail; an ISFJ is likely to notice details such as a different email address or unusual wording.

In general, ISFJs can be quite trusting. A quarter of ISFJ respondents in our survey agreed that if a public Wi-Fi network requires a password to access, it should be safe to use this network for sensitive activities such as online banking (compared with 10% of total respondents). ISFJs were more likely than most to think it OK to use the same password at work as at home, and less likely to set their computer screen to automatically lock if they don't use it for a prolonged period. As a group, ISFJs may take cyber-security less seriously than other MBTI types. However, when they, or someone they know, have experienced a cyber-attack, this is likely to change.

For those with ISFJ preferences, it may be useful to remember that public networks can never be considered secure, and that even if a message seems to come from a close friend, it could be a from a malicious (and not necessarily human) agent. For those working with ISFJs, it may be especially important to demonstrate how IT security is relevant to their specific personal circumstances.

INFJ

People with preferences for INFJ seek meaning and they may sometimes over-complicate things. From a cyber-security point of view, this may in some ways be an asset. In our survey, they were among the least likely to agree that "If you are certain that you've installed all the security updates required by your system administrator, you don't need to worry about computer viruses", or that "If you get an email or IM from someone you know within your organization, asking for sensitive personal information, it's okay to supply this", or that "if you are certain that you have installed all the security updates required you don't need to worry".

Set against this, INFJs do not always pay attention to detail, especially when it is not relevant to their view of the world, and therefore they may miss some of the cues in poorly spelled or constructed phishing emails. They often have a deep insight into people, but when it comes to cyber-security this can be a double-edged sword. They may spot that something does not seem right but may also rely too much on their gut feel and not check the detail. For an INFJ, if they have any hint that something does not feel right, it pays to remember to check, check and check again.

INFJs may sometimes be internally focused. In our survey, they were a little more likely than most to say that if they discovered a security problem, someone else would fix it.

INTJ

INTJs value knowledge and strive to be capable and competent. In our survey, they were one of the highest-scoring groups on the *Knowledge-informed carefulness* scale (recognising secure sites, checking links, verifying attachments etc). They were particularly unlikely to re-use the same password, even when they could, and were very unlikely to say that the rules did not apply to them. However, where IT policies and rules are not logical or do not make sense, they may be tempted to do things in their own way; INTJs often trust their own opinions more than those of others. As a tip, INTJs may need to remind themselves that they don't necessarily know best.

People with INTJ preferences do not always pay attention to detail, especially when it is not relevant to their view of the world, and therefore may miss some of the cues in poorly spelled or constructed phishing emails. If, however, an INTJ sees IT security as a core part of their job, or as an area of competence that they should be able to demonstrate to themselves, this is much less likely. For a manager, encouraging INTJs to connect cyber-security awareness with their sense of self-competence is likely to be worthwhile. Some INTJs may not take data security as seriously as other MBTI types; in our survey, they were less likely than most to agree that a data breach would be disastrous for their organization.

ISTP

In our survey, respondents with preferences for ISTP were very aware of the policies and procedures on cyber-security in their organization and knew that these rules did apply to them. However, they may not always follow all of these rules, or may find a way to bend them. For ISTPs, it will be important that cyber-security rules and procedures make logical sense and are efficient. If this is not the case, or if the reasons for the rule are not explained or presented in a clear and logical way, there is a danger that ISTPs may take shortcuts – possibly risky ones.

ISTP respondents were generally careful in their online behavior and were less likely than most others to trust the security of public Wi-Fi networks, or to feel entirely safe if they have installed all security updates, or to supply sensitive personal information. They were however more likely than most to share their password with their spouse or partner. Many ISTPs are naturally cautious, even at times cynical, about the intentions of others and the claims made for systems and processes. This can work to their advantage when it comes to cyber-security.

ISFP

ISFPs were the most likely group to say they follow all the security rules and procedures in their organization, and they agreed that these rules applied to them. They generally took cyber-security seriously and most were careful in their online behavior, for example manually locking their computer when they step away from it, not assuming that installing security updates made them safe from viruses, or that using one password for all sites is secure.

However, ISFPs may be more easily caught out than most by cyber-attacks where a malicious agent masquerades as a trusted acquaintance, especially if a quick or automatic response is required. They can be quite spontaneous, even impulsive at times. In the survey, after a question about passwords, we asked, “If at this point, we had asked ‘and what is your password’, would you have entered your password?”. ISFPs were more likely than others to think about doing so, or, if there was an additional and apparently reasonable prompt, to say yes. ‘Pause before you click’ can be a useful mantra for ISFPs.

INFP

People with preferences for INFP are not natural followers of externally imposed rules, preferring instead to be guided by their inner values. In our survey, many did not agree that there were clear policies on cyber-security in their organization, and they were less likely than most to follow such processes, often feeling that many of the rules did not really apply to them. Indeed, many agreed that were a lot of stupid rules on IT security in their organization. Where INFPs have not internalized IT security as part of their value system, they may not always take personal responsibility for it. INFP survey respondents were less likely than most to think that everyone in the organization has a role to play in IT security, and some would leave it to someone else to fix security problems.

As a positive, INFPs are unlikely to make sudden, risky choices. If they are made aware of the importance of cyber-security, and in particular of the negative effects that security breaches may have on people they know, they are likely to become more invested in the importance of IT security rules.

INTP

Across all the respondents to our survey, those with preferences for INTP achieved the highest average score on the scale of *Knowledge-informed carefulness* (recognizing secure sites, checking links, verifying attachments etc). Many consider themselves to be knowledgeable about cyber-security issues. In our survey, INTPs were the least likely group to agree that "if a public Wi-Fi network requires a password to access it should be safe to use this network for sensitive activities" and did not agree that "If you get an email or IM from someone you know within your organization, asking for sensitive personal information it's okay to supply this". INTPs are likely to use different passwords for different accounts and apps.

However, INTPs are the type least likely to always follow the IT security rules and procedures in their organization, which could result in a security breach. Although they are very aware that anyone may be caught out by cyber-attacks, some INTPs may over-estimate their own competence and knowledge to deal with or prevent such attacks. Where INTPS are not knowledgeable about cyber-security, not seeing this as a lack of competence, they may be especially lax about following procedures.

A tip for all INTPs may be to remember that they don't always know best and to stick to the rules. They are there for a reason.

ESTP

People with preferences for ESTP enjoy living in the moment and typically find rules and standard procedures constricting. This is reflected in the way that ESTP respondents answered our survey. These individuals agreed that they do not always follow all the IT security rules and procedures in their organization. They are likely to have at some point contravened these rules. They do things in their own way and will ignore the rules in order to get things done. Indeed, ESTPs are the most likely MBTI type to agree that many IT security rules don't really apply to them, and that there are a lot of stupid rules about IT security in their organization. They are among those most likely to think it is OK to use the same password at work and at home, to share a password with their spouse or partner and, if they can, will re-use the same password for different accounts and apps. Not surprisingly, ESTPs have on average the lowest scores on the scales of *Conscientiously follows rules* and *Keeps passwords and devices secure*.

A challenge for those working with ESTPs may be to get them to take IT security seriously. Although ESTPS are the least certain that they won't be caught out by cyber-attacks, they are also the least concerned about this. ESTPs can see any data breach as only a PR issue, are less likely than others to agree that everyone in the organization has a role to play in IT security and are more likely to agree that if they discover a security problem someone else will fix it. To help ESTPs improve their cyber-security behavior, give specific examples of what they can do and illustrate with realistic accounts of the results when things go wrong, presented in as engaging a way as you can. If possible, offer specific cyber-security hints and tips at the point of use.

ESFP

ESFP survey respondents were the type most certain that they would not be caught out by cyber-attacks. They were also generally happy to follow IT security rules, and did not agree that there are a lot of stupid rules about IT security in their organization. Across all types, they had the highest average score on *Keeps passwords and device secure*. However, ESFPs may be overly trusting. A quarter of ESFPs believed that if a public Wi-Fi requires a password to access, it should be safe to use for sensitive activities. The same number believed that if they had installed all the security updates required, they didn't need to worry.

Most ESFPs will have good intentions regarding cyber-security, and see themselves as following the rules, but there may be a degree of complacency or lack of attention to detail when IT security is not seen as sufficiently important. To help ESFPs be more aware of the importance of cyber-security give specific examples of what they can do and illustrate by showing the negative effects of breaches on people. If possible, offer specific cyber-security hints and tips at the point of use.

ENFP

People with preferences for ENFP are usually gregarious and sociable and are typically one of the first to realize when a new cyber-security process or protocol has been put in place, especially if it has impacted on their circle of friends and acquaintances. This does not of course mean that they will then follow this process rigidly; ENFPs dislike structure and routine and are less concerned with detail. In our survey they were less likely than most MBTI types to take care to ensure their computer is locked, either manually or automatically, when they step away from it, and were less concerned with keeping their passwords secure.

ENFPs are also the group most likely than others to be susceptible to social engineering attacks that have an emotional appeal to their values, or which purport to come from a worthy cause that is congruent with these values. They may need to be reminded to pause before clicking on that link. However, where an ENFP has internalized the importance of cyber security, this may itself become one of their values and they will treat anything that comes into their inbox unexpectedly with a degree of suspicion. Describing the potential people impacts of not taking cyber-security seriously may help with this process.

ENTP

ENTPs are independent and autonomous and like to do things in their own way. This can mean that they ignore rules or IT security procedures in order to get things done. In our survey, they were more likely than most others to say that many of the rules about IT security didn't really apply to them. They also had one of the lowest average scores on the scale of *Conscientiously follows rules*. ENTPs may not always take the time to be knowledgeable about cyber-security unless this is central to their role or to their sense of competence. In our survey, they were more likely than most to agree that if they received an email or IM from someone they knew in their organization asking for sensitive information, then it was okay to supply this. They tended to agree that using one complex password for all sites is secure and were the most likely MBTI type to see "password1" as a secure password (though even for ENTPs, this was a minority).

Where ENTPs have an interest in technology, or this is central to their role, they are likely to see cyber-security as an area in which they should be competent. These ENTPs will seek to demonstrate this competence and build their credibility by avoiding what they would describe as 'stupid' mistakes.

ENTPs see themselves as innovative and can be easily bored. Imposing IT security processes without explanation will not work well. An ENTP may just find a creative way to circumvent the rules, or just go ahead and do things in their own way. It is, however, important to ENTPs to be competent, so if it is possible to give them options and make choices so that they can take responsibility for their own cyber-security (and thereby demonstrate their competence), this is likely to be more successful. A tip for ENTPS would be to consciously slow down before reading emails so as to spot anything unusual.

ESTJ

People with preferences for ESTJ like to be organized, follow efficient processes, and get things done. In a cyber-security context, they are likely to follow all the IT security rules and processes in their organization. If they consider a process to be inefficient, they will push to have it changed rather than ignoring the rule and just doing things in their own way. In our survey, they were on average one of the highest types on the scale of *Conscientiously follows rules*. However, some ESTJs may place too much faith in systems and processes. They were more likely than most to agree that if a public Wi-Fi network requires a password to access, it should be safe to use this network for sensitive activities, and to agree that if you are certain that you have installed all the security updates required you don't need to worry.

ESTJs generally take cyber-security seriously; they were the most likely type to say that a data breach would be disastrous for their organization. Some do, however, become very frustrated when IT security processes get in the way – for example, when passwords are required to be very complex. ESTJs are typically very organized in carrying out day-to-day IT security behaviors such as locking their computer screen, or not supplying sensitive information to a possibly compromised source, but may occasionally cut corners in order to save time or be more efficient. If they see others being less careful or systematic, some (not all) ESTJs may react in a dogmatic and overly forceful way, which would not be helpful in motivating others to change their behavior.

ESFJ

People with preferences for ESFJ are organized, conscientious, and people focused. In terms of cyber-security, they are likely to be aware of the polices and processes used in their organization, and to follow these conscientiously; they are unlikely to ignore the rules or seek to do things in their own way. In our survey, ESFJs had the highest average score on the scale of *Conscientiously follows rules*. However, if IT policies change in a way that adversely affects others, ESFJs may find this difficult to deal with. They will still want to comply with the rules, but also want to help their colleagues. Some ESFJs may be vocal in voicing their frustration.

ESFJs like to be appreciated for who they are, and they show loyalty to others. This may sometimes mean that they are overly trusting. In our survey, a third of ESFJs said that they would share their password with a spouse or partner – the highest percentage for any type. They were also more likely than most to agree that if you are certain that you have installed all the security updates required, you don't need to worry.

ESFJs enjoy having clear processes and rules and are happy to follow them. They also rely on experience and form habits to follow these rules efficiently. For organizations, this means that it is not a good idea to introduce new IT security rules and processes at times of high pressure, or multiple deadlines, as ESFJs may then accidentally forget new procedures which have not yet become habitual.

ENFJ

People with ENFJ preferences are people-focused and like to base decisions on their personal values. As such, cyber-security may not be at the top of their list of concerns. Indeed in our survey they were less likely than most to agree that a data breach would be disastrous for their organization, and slightly more likely than most to agree that if they discovered a security problem, they would leave it and let someone else fix it. Demonstrating their competence in and knowledge of cyber-security issues may be less important for ENFJs than for some other types, and as a group they had the lowest average score on the scale of *Knowledge-informed carefulness* (recognizing secure sites, checking links, verifying attachments etc). They are the most likely MBTI type to use the same password for most accounts and apps, re-use the same password if they can, and think that it is OK to use the same password at work as at home.

ENFJs do like to be organized and will follow the rules where these are clear. They will, however, find it difficult where people's needs conflict with cyber-security processes and will be tempted to put people first. They may take quick and decisive action to break the rules to help others.

ENTJ

ENTJs see themselves as analytical, logical and decisive. Being competent (or more than competent) is important to them and they try to be aware of the bigger picture of what is happening in their organization. Most ENTJs in our survey said they were one of the first to realize when a new process or protocol had been put in place, and several commented on how important it was to keep up to date and to be questioning about IT issues in order to understand these more fully. As a group, ENTJs scored highly on the scale of *Keeps passwords and devices secure*.

ENTJs like things to be clear and organized and will in general be willing to follow IT security rules and processes. If, however, these are not clear and logical, or do not fit with the wider strategy of the organization, ENTJs will seek to change them. This may improve the situation or may result in them over-ruling others who have a more detailed knowledge of cyber-security. It will be important for ENTJs to allow themselves to pause before forcing any changes through.

References

Boult, M., Thompson, R., & Schaubhut, N. (2019). *Well-being in the workplace: Why it matters for organizational performance and how to improve it.* Sunnyvale, CA: The Myers-Briggs Company.

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT Guide to Insider Threats.* Addison-Wesley.

Cyberedge Group. (2019). *2019 Cyberthreat Defense Report.* Annapolis, MD: Cyberedge Group.

Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a Security Behavior Intentions Scale (SeBIS). *Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems*, *1*, pp. 2873-2882. Seoul.

Furnham, A. (2017). Myers-Briggs Type Indicator. In V. Zeigler-Hill, & T. K. Shackleford, *The Sage Handbook of Personality and Individual Differences.* New York: Sage.

Halevi, T., Lewis, J., & Memon, N. (2013). Phishing, personality traits and Facebook. *ArXiv*.

Halevi, T., Memon, N., & Oded, N. (2013). Spear-fishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. In D. Schwabe, V. Almedia, & H. Glaser, *Proceedings of the 22nd International Conference on World Wide Web.* New York: ACM.

Howard, D. J. (2018). Development of the Cybersecurity Attitudes Scale and modeling cybersecurity behavior and its antecedents. *Graduate Theses and Dissertations*.

James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Correlates of susceptibility to scams in older adults without dementia. *Journal of Elder Abuse & Neglect, 26*(2), 107-122.

Kelley, D. (2018). Investigation of attitudes towards security behaviors. *McNair Research Journal SJSU, 14*, 123-139.

McBride, M., Carter, L., & Warkentin, M. (2012). *Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies.* RTI International - Institute of Homeland Security Solutions.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*(C), 151-156.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia - Social and Behavioral Sciences*, 424-428.

Microsoft. (2019, October 18). *Test Your Internet Security IQ.* Retrieved from go.microsoft.com: http://go.microsoft.com/?linkid=9713967

Myers, I. B., McCaulley, M. H., Quenk, N. L., & Hammer, A. L. (1998). *MBTI Manual: A Guide to the Development and Use of the Myers-Briggs Type Indicator (3rd Ed).* Palo Alto, CA: Consulting Psychologists Press, Inc.

Myers, I. B., McCaulley, M. H., Quenk, N. L., & Hammer, A. L. (2018). *MBTI Manual for the Global Step I and Step II Assessments* (4th ed.). Sunnyvale: The Myers-Briggs Company.

National Cyber Security Centre. (2019, November 18). *Cyber Essentials Homepage*. Retrieved from Cyber Essentials: https://www.cyberessentials.ncsc.gov.uk/

Parsons, K., McCormac, A., Butavicius, M. A., Pattinson, M. R., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176.

Smith, R. G. (2010). Indentity theft and fraud. In Y. Jewkes, & M. Yar, *Handbook of Internet Crime* (pp. 273-301). Cullompton: Wiley.

Sotira, N. (2018). The human factor in cyber security. *Cyber Security: A Peer-Reviewed Journal, 1*(4), 326-330.

Thonnard, O., Bilge, L., Kashyap, A., & Lee, M. (2015). Are you at risk? Profiling organizations and individuals subject to targetted attacks. *International Conference on Cryptography and Data Security* (pp. 13-31). Berlin Heidelberg: Springer-Verlag.

World Economic Forum. (2019). *The Global Risks Report 2019 (14th Edition).* Geneva: World Economic Forum.

Appendices

Appendix A: Psychological type and the MBTI® assessment

The Myers-Briggs Type Indicator® (MBTI®) assessment is probably the most widely used personality questionnaire in the world. It does not measure our ability or skill, or how much of a particular personality trait we have. It looks at whether we have an in-built preference to do things in one way or in another way. It looks at four pairs of preferences:

Opposite ways to direct and receive energy	
Extraversion (E)	**Introversion (I)**
Gets energy from the outer world of people and experiences	Gets energy from the inner world of reflections and thoughts
Focuses energy and attention outwards in action	Focuses energy and attention inwards in reflection

Opposite ways to take in information	
Sensing (S)	**Intuition (N)**
Prefers real information coming from five senses	Prefers information coming from associations
Focuses on what is real	Focuses on possibilities and what might be

Opposite ways to decide and come to conclusions	
Thinking (T)	**Feeling (F)**
Steps out of situations to analyze them dispassionately	Steps into situations to weigh human values and motives
Prefers to make decisions on the basis of objective logic	Prefers to make decisions on the basis of values

Opposite ways to approach the outside world	
Judging (J)	**Perceiving (P)**
Prefers to live life in a planned and organized manner	Prefers to live life in a spontaneous and adaptable way
Enjoys coming to closure and making a decision	Enjoys keeping options open

For convenience, these pairs of preferences, or pairs of opposites, are often called type preference pairs. So, we might talk about the E–I preference pair, the S–N preference pair, the T–F preference pair or the J–P preference pair.

In each pair, we will have a preference for one type. So, for example, we might prefer E rather than I, and spend much more of our time and energy doing things typical of Extraverts, and little of our time or attention on activities and ways of doing things typical of Introverts. Or we might

prefer I rather than E. Whatever our preference, however, we will spend some time and carry out some activities associated with the other side. The same applies to S–N, T–F and J–P – in each case we will have a preference, but we will visit the other side from time to time. We will use all eight modes at least some of the time.

The MBTI assessment is a method for helping individuals to work out what their type preferences are, so you may hear people say things like "I'm an ESTJ" or "I've got preferences for INFP" or "I'm definitely a Perceiving type". They can then use this knowledge in all sorts of ways to help them with their development as human beings. The four letters can be combined to give 16 different types, but this four-letter type formula should not be used to 'put people in a box'.; The MBTI instrument is used to open up possibilities, not to limit individuals.

The 16 types are often illustrated using a *type table*, as shown here.

Each of these 16 types has a particular characteristic taking the lead in directing their personality – what's often called their favorite process.

So, for ISTJ and ISFJ for example, Introverted Sensing (S^i) leads. Central to their personality is the importance of lived experience and drawing on their rich store of memories.

For ESTP and ESFP, it is Extraverted Sensing (S^e) – experiencing the moment and the here and now with all their senses – that leads, and so on for all 16 types. See the table below.

Types	Favourite process
ISTJ, ISFJ	Introverted Sensing (S^i)
ESTP, ESFP	Extraverted Sensing (S^e)
INFJ, INTJ	Introverted Intuition (N^i)
ENTP, ENFP	Extraverted Intuition (N^e)
ISTP, INTP	Introverted Thinking (T^i)
ESTJ, ENTJ	Extraverted Thinking (T^e)
ISFP, INFP	Introverted Feeling (F^i)
ESFJ, ENFJ	Extraverted Feeling (F^e)

Appendix B: What are your cyber-security attitudes?

This short quiz asks you about your cyber-security attitudes and behavior. For each block of statements below, answer each individual statement in terms of whether you strongly disagree, disagree, neither agree nor disagree, agree, or strongly agree. For each statement, you will have a score of 1, 2, 3, 4 or 5, depending on which option you chose. Make sure you note the numbers correctly; some run 1 to 5, others run 5 to 1. Add up the numbers in each block to get the total raw score for each block.

Conscientiously follows rules	Strongly disagree	Disagree	Neither	Agree	Strongly agree
Everyone in my organization has a role to play in IT security	1	2	3	4	5
I always follow all the IT security rules and procedures in my organization	1	2	3	4	5
I can't be bothered to read security briefings or emails	5	4	3	2	1
If I discover a security problem, I continue what I was doing; someone else will fix it	5	4	4	2	1
Many of the rules about IT security don't really apply to me	5	4	3	2	1
My organization's cyber-security procedures and rules get in the way of productivity	5	4	3	2	1
There are a lot of stupid rules about IT security in my organization	5	4	3	2	1

Conscientiously follows rules total (NOTE scoring for the last five questions is reversed):

Keeps passwords and devices secure	Strongly disagree	Disagree	Neither	Agree	Strongly agree
I manually lock my computer screen when I step away from it	1	2	3	4	5
I use a password or passcode to unlock my laptop or tablet	1	2	3	4	5
I set my computer screen to automatically lock if I don't use it for a prolonged period	1	2	3	4	5
I am often one of the last to realize that a new process or protocol has been put in place	5	4	4	2	1
I only use a password because my IT administrator makes me do so	5	4	3	2	1
I write down my password	5	4	3	2	1
Occasionally I will write down a password and leave this note next to my computer	5	4	3	2	1

Keeps passwords and devices secure total (NOTE scoring for the last five questions is reversed):

Knowledge-informed carefulness	Strongly disagree	Disagree	Neither	Agree	Strongly agree
I know the difference between websites that have a "http" address and a "https" address	1	2	3	4	5
If I am browsing a website, I mouseover (hover over) links to see where they go, before clicking on them	1	2	3	4	5
I submit information to websites without first checking that it will be sent securely (e.g. SSL, 'https' or a 'lock' icon	5	4	3	2	1
I use the same password for most accounts and apps	5	4	4	2	1
If I can, I will re-use the same password	5	4	3	2	1
If I get an email from someone I know personally, it's OK to open any attachments	5	4	3	2	1
When someone sends me a link, I usually open it without first checking where it goes	5	4	3	2	1

Knowledge-informed carefulness total (NOTE scoring for the last five questions is reversed):

Now compare the total raw score from each block to the norm table below to see your standard score on each scale:

	1	2	3	4	5	
Does not follow all IT security rules; may pick which apply to them. Thinks many rules stupid or obstructive. Leaves IT security to others.	*Conscientiously follows rules*					Follows IT security rules and procedures, takes responsibility, takes rules seriously, reads briefings, knows that the rules apply to them.
	7-23	24-27	28-31	32-34	35	
Only uses passwords/ codes because they have to, writes down password and may leave next to computer, unaware of new IT security protocols.	*Keeps passwords and devices secure*					Uses passwords willingly, locks computer screen when away, does not write down password, keeps up to date with IT security protocols.
	7-17	18-22	23-28	29-33	34-35	
Does not identify secure sites or check sites are secure, opens links and attachments without checking if secure, re-uses passwords.	*Knowledge-informed carefulness*					Can identify secure sites, checks sites are secure before using, does not trust attachments or links, varies passwords.
	7-22	23-26	27-31	32-34	35	
	1	2	3	4	5	

Appendix C: Calculation of the overall cyber-security score

Step 1 Calculate z-scores for each of the cyber-security attitude and behavior scales

Zrules=(*Conscientiously follows rules* – 41.1386)/5.14950

Zpassword=(*Keeps passwords and devices secure* – 27.9758/4.27645)

Zinformed=(*Knowledge-informed carefulness* – 24.1029)/5.24013

Step 2 Calculate and norm overall cyber-security and behavior scale

Cyberatt=zrules+zpassword+zinformed

Zcyberatt=(cyberatt –(-0.0101))/2.42296

Step 3 Calculate an overall score for the knowledge items in question 13, scoring each item positively or negatively as appropriate

Q13know = (2-q13_1)+(2-q13_2)+(2-q13_3)+ (2-q13_4)+(2-q13_5)+q13_6-1+(2-q13_7)

Step 4 Calculate an overall score for question 14 ("who is it OK to share your passwords with"). Only one option ("None of the above") is a strictly correct answer. Sum the number of wrong answers and subtract from 9, giving a score between 0 (no incorrect options chosen) and 9 (every correct option chosen). Award 1 point for choosing the correct option, then calculate total score for question 14:

Q14tot = (reversed wrong score/9)+correct option score.

Step 5 Calculate a total score for question 15 ("which of the following would you say is a strong password"). Award 1 point for each correct answer and divide total by 4 to give total score (Q15tot)

Step 6 Recode question 16 ("If at this point, we had asked, "what is your password", would you have entered your password"). Award 1 point for "No" and 0.25 of a point for "I would think about it but then realize what I was being asked and decide not to" and 0 points for other answers.

Step 7 Calculate and norm total knowledge score

Knowledge score=Q13know+Q14tot+Q15tot+Q16score

Zknowledge=(knowledge score – 9.6515/1.146878

Step 8 Compute overall cyber-security score as a Sten

Overall score = ((((Zknowledge+Zcyberatt)-(-0.116))/1.70359) x 2)+5.5