

Computer Science Project: Cybersecurity Visualisations

Thanks: Many thanks to my supervisors, Louise Axon, Michael Goldsmith, and Ioannis Agraftotis, who have been enormously supportive in helping me complete this project

Declaration: I declare that this project I am submitting is entirely my own except where otherwise indicated

Word count: 8839

Total number of pages across the five appendices: 22

Link to online implementation: <https://emilyslade.co.uk/Personalised-Visualisation/>

Summary

There is a gap in the literature concerning cybersecurity tools for *non-expert users*, as well as a gap around *personalised cybersecurity tools*. To the best of this author's knowledge, this paper presents the first ever personalised cybersecurity visualisation aimed at non-expert users.

Gaps in the literature

Research has shown time and time again that humans are the weakest link in any cybersecurity system (1-6), with one study finding that human error accounts for nearly 25% of cybersecurity failures (7), and another study finding that cybercrime costs between \$375 billion and \$575 billion annually (8). Despite this, cybersecurity education aimed at non-expert users has been minimal. Two studies by NIST (National Institute of Standards and Technology) found that cybersecurity *definitions* alone were inconsistent (9) and unstandardised (10), and a literature review of cybersecurity visualisation objectives (11) found that there was 'an important gap in the existing literature regarding the application of security visualization for non-expert users.'

This project aims to address this gap, and to create a tool specifically designed to help educate non-expert users.

Within non-expert cybersecurity education, the importance of *tailoring* cybersecurity information to individuals has been well-documented (12-15). A 2018 literature review entitled 'Everyday Cyber Security in Organisations' (16) was submitted to the UK Cabinet Office and recommended:

'There is a need for more research on behavioural differences between types of employees, or within different organisational environments, as these may also display different behaviours towards cyber security issues.'

Similarly, a 2019 literature review of the impact of training on cybersecurity awareness (17) found:

'One of the main recommendations from studies carried out on cybersecurity awareness training is that individuals react differently to the same conditions.'

Despite this recognised need, to the best of the author's knowledge, a tailored cybersecurity education tool has never been developed.

Thus, to address these two known gaps in cybersecurity, this project aims to create a *tailored* education tool designed specifically for *non-expert users*.

The benefits of cybersecurity awareness

Recent research has shown that cybersecurity training can benefit individuals by providing awareness and knowledge of cybersecurity best practices (18, 19), and that cybersecurity awareness does improve users' cybersecurity behaviours (20). Thus, the education tool will provide users with *knowledge and awareness of cybersecurity best practices*, in line with existing research.

The three levels of cybersecurity awareness training

In McBride et al.'s 2012 paper 'Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies' (21), they concluded that customised training protocols that are based on personality would be more effective than generic cybersecurity training protocols. They investigated how situational factors (including self-efficacy, perceived certainty and severity of sanctions, vulnerability and severity of threats, effectiveness and cost of responses, and the realism of given scenarios) interacted with personality traits to predict the likelihood of an individual violating cybersecurity protocol.

McBride et al. (21) propose that there are three levels of cybersecurity training:

1. Non-personalised cybersecurity training (widely implemented)
2. Cybersecurity training that incorporates either personality factors or situational factors, but not the interaction between the two (not widely implemented)
3. Cybersecurity training protocol that incorporates the interaction between personality factors and situational factors (not widely implemented)

This project therefore aims to meet Level Two of McBride et al.'s cybersecurity levels, and to implement a visualisation-based cybersecurity awareness tool that is tailored to personality type. To the best of the author's knowledge, this is a *first-in-field personalised cybersecurity tool*. Further work in this area could expand this visualisation to also take into account situational factors, providing an even more bespoke experience for the user.

How to measure personality

There are various ways of describing and measuring personality. One of the most popular personality measures is the 'Big-Five,' which refers to the five personality traits: openness, conscientiousness, agreeableness, extraversion, and neuroticism. These personality traits are sometimes referred to as 'OCEAN', given their initial letters, or the FFM (Five Factor Model). These traits have been found to be stable throughout life (22) and universal (23).

This personality measure was first introduced by John and Srivastava in their 1999 paper 'The Big-Five Trait Taxonomy: History, Measurement and Theoretical Perspectives' (23), which has been highly influential in a range of cross-cutting fields, from psychology to sociology to education, and has amassed more than 15,000 citations to date.

The paper includes a 44-item list for evaluating personality traits based on various behaviours and tendencies (see Appendix 3 (Big-Five personality traits)). Later research has also produced shorter inventories (i.e. 5-item and 10-item) (24) for time-critical applications.

The personality traits can be broadly outlined as follows (25):

Openness: individuals who are imaginative, creative, and willing to try new things

Conscientiousness: individuals who are organised, dependable, and disciplined

Extraversion: individuals who are outgoing, energetic, and sociable

Agreeableness: individuals who are compassionate, cooperative, and trusting

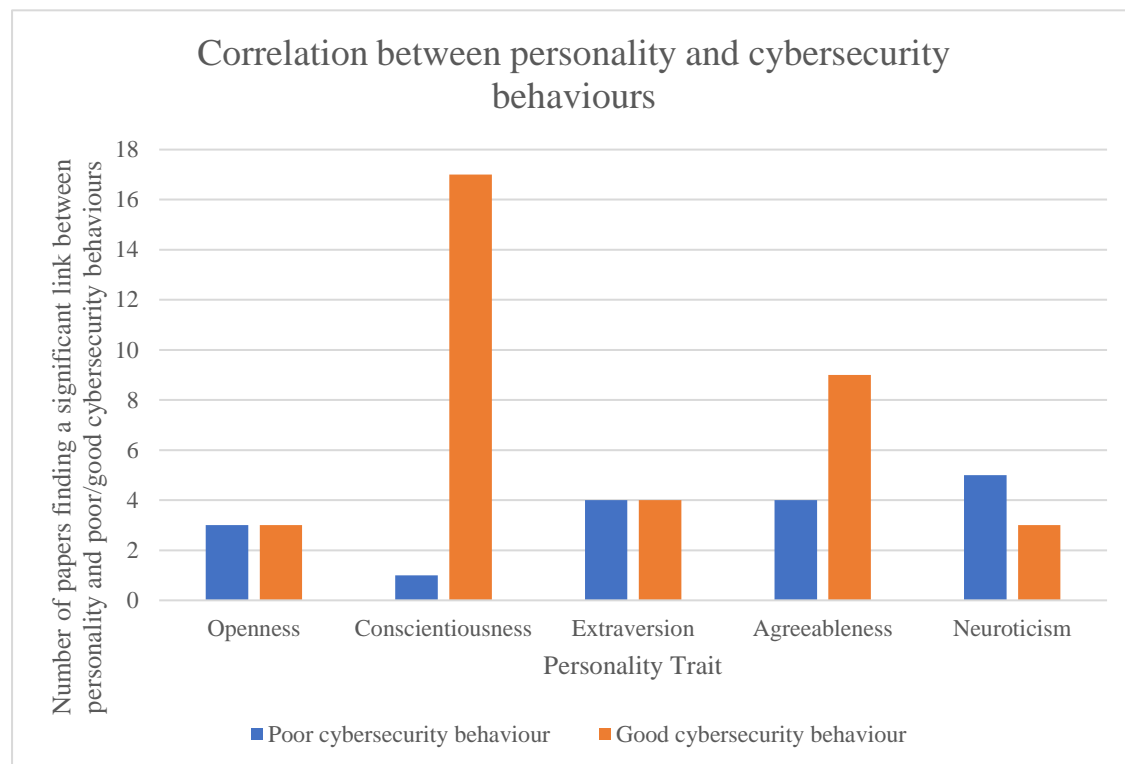
Neuroticism: individuals who are emotionally unstable, anxious, and irritable

How personality relates to cybersecurity

Personality is critically linked to how users perceive security messages. For example, a study by Kajzer et al. (26) found that some personality traits were not only *un-receptive* to certain message types, but were actively *dissuaded* by the message (i.e. would be more likely to perform the *opposite* of the suggested behaviour). They concluded that 'certain types of individuals are less receptive to certain message types and therefore security messages may backfire in terms of achieving their intended effect.' For example, openness was negatively associated with incentive-based messages, while agreeableness was positively associated with deterrence-based messages.

There is an abundant literature on the link between personality and cybersecurity behaviours. A literature review was conducted to assess the cybersecurity behaviours associated with each personality trait. The full table of results is provided in Appendix 4 (Literature review).

The following graph summarises the results of the literature review, with the height of each bar showing the number of papers that found an association between each personality trait and either poor or good cybersecurity behaviours.



On the whole, conscientiousness strongly predicted positive cybersecurity behaviours, agreeableness weakly predicted positive cybersecurity behaviours, and neuroticism weakly predicted negative cybersecurity behaviours, though these are heavily mediated by context and sub-traits (27).

How personality is connected to learning approaches

Having shown the substantial link between personality traits and cybersecurity behaviours, we now need a way to implement the personalisation. Biggs' 1987 book 'Learning Process Questionnaire Manual. Student Approaches to Learning and Studying' (28) identified three distinct learning approaches: surface, deep, and achieving. These approaches are characterised by the use of different methods for engaging with new material (p. 10):

- 'Surface strategy (SS) is to limit target to bare essentials and reproduce them through rote learning.'
- 'Deep strategy (DS) is to discover meaning by reading widely, inter-relating with previous relevant knowledge, etc.'
- 'Achieving strategy (AS) is to organize one's time and working space; to follow up all suggested readings, schedule time, behave as 'model student'.'

Jensen's 2015 literature review (29) identified which personality traits are best suited to different learning approaches. The following tables are adapted from his paper and show the number of studies (out of a given total) that found significant positive or negative associations between each trait and learning approach:

Number of papers that found a positive association with each learning approach:

	Openness	Conscientiousness	Extraversion	Agreeableness	Neuroticism
Surface (out of 10)			1	1	6
Deep (out of 10)	9	7	5	3	
Achieving (out of 7)	3	6	3	2	1

Number of papers that found a negative association with each learning approach:

	Openness	Conscientiousness	Extraversion	Agreeableness	Neuroticism
Surface (out of 10)	8	4	2	5	
Deep (out of 10)				1	4
Achieving (out of 7)					2

Blanks = 0 (omitted for clarity)

The vast majority of education literature has focused on deep and surface learning (30-34), rather than achieving learning, due to the natural dichotomy between surface and deep learning (as evidenced by the above data showing their broad mutual exclusivity). However, 6 out of 7 studies found a significant positive association between conscientiousness and achieving learning. Since the achieving approach can complement both surface and deep learning, I propose the following approaches to be used in the visualisation:

- Openness: deep learning approach
- Conscientiousness: deep learning approach + achieving learning approach
- Extraversion: deep learning approach
- Agreeableness: deep learning approach
- Neuroticism: surface learning approach

As this is the first personalised cybersecurity visualisation, future refinements could include a more granular approach to different learning approaches (such as incorporating *varying proportions* of deep, surface, and achieving learning).

Visualisation theory

The use of visual communication, such as infographics, to convey information is an extremely effective method of education (35-38). Visual communication helps to explain complex topics (39), engage audiences (39), and enhance user understanding and learning (40).

There has been a lot of research on how to educate, persuade and influence people, both in general contexts and in cybersecurity-specific contexts. I will use the following papers to guide the visualisation creation, as they summarise the majority of cybersecurity education literature, have been widely cited, and (given the ever-evolving cybersecurity landscape) are relatively recent.

Bruijn and Janssen's 2017 paper 'Building cybersecurity awareness: The need for evidence-based framing strategies' (41) outlines how to effectively convey cybersecurity information:

1. **Do not exacerbate cybersecurity** (avoid exaggerated claims that can lead to feelings of nihilism and futility)
2. **Make it clear who the villains are** (clearly identify the threats)

3. **Give cybersecurity a face by putting the heroes in the spotlight** (highlight the heroes of cybersecurity)
4. **Show its importance for society** (emphasise benefits like economic growth and prosperity)
5. **Personalise for easy recognition by the public** (tailor messages to individuals)
6. **Connect to the undercurrent** (relate cybersecurity to broader cybersecurity issues)

Bada et al.'s 2019 paper 'Cyber security awareness campaigns: Why do they fail to change behaviour?' (42) proposed the following factors to improve the effectiveness of cybersecurity campaigns:

1. Campaigns need to be organised and prepared by professionals
2. Campaigns should not aim to invoke fear in people
3. Security education needs to be 'targeted, actionable, doable and provide feedback'
4. Users need continuous feedback and training to sustain change
5. Campaigns need to account for different characteristics and cultural contexts

The 2019 paper 'Design2Inform: Information Visualisation' (40) provides the latest UK guidelines for presenting complex information using visualisations, taking into account visual perception and cognition, to maximise user understanding.

Cognitive guidelines:

1. **Information chunking** (elements should be grouped together in meaningful units)
2. **Reminders** (use labels and visual cues to remind users about information they are seeing)
3. **Familiar elements** (build on knowledge the user already has about symbols and colours)
4. **A limit of choices** (limit the number of choices to avoid the user feeling overwhelmed)
5. **A limit of visuals** (limit the number of graphical elements to avoid the user needing to determine which are relevant)
6. **Order** (the most relevant information should come first)
7. **Hierarchy** (information should be presented in the order that the user will use it)
8. **Consistency** (constant information should be kept in the same position)
9. **Emphasis** (use colours or font sizes to emphasise important information)

Typography guidelines:

1. Text should be easy to read and self-explanatory
2. Typography should be appropriate to the message
3. There should be a maximum of two typefaces
4. Type size and line length should be coordinated
5. Bold, rather than italics, should be used for emphasis
6. Bolded text should be sufficiently contrasted from regular text
7. All-capitals should be avoided when rapid reading is required
8. Titles should be the most dominant element and should present the purpose and focus on the message
9. There should be sufficient contrast between the title and narrative text in terms of font size and bold
10. When typing white text on a black background, use a sans serif font in a larger size
11. Text and backgrounds should be sufficiently contrasted to be legible
12. Do not use multi-coloured or gradient backgrounds
13. Do not use black ink on dark red or dark purple paper
14. Large blocks of text should be left-aligned
15. Include orientating text to tell users about the relevance of the infographic
16. When embedding an infographic in another page, include the key message in large text

The 2022 book ‘Visual Communication for Cybersecurity’ (39) discusses how to use visualisation to enhance cybersecurity understanding among non-experts, and recommends using the Gestalt principles of visual perception (43):

1. **Simplicity** (present visuals in the simplest form possible)
2. **Proximity** (elements that are close together are perceived as being part of the same group)
3. **Similarity** (elements that are similar are perceived as being part of the same group)
4. **Enclosure** (elements that are enclosed by a border or background are perceived as being part of the same group)
5. **Closure** (elements that form a group do not need to be enclosed by borders)
6. **Continuity** (elements that are aligned are perceived as being part of the same group)
7. **Connection** (elements that are connected are perceived as being part of the same group)
8. **Figure-ground** (elements are perceived as either foreground ‘figures’ or background ‘ground’)
9. **Focal point** (elements that are emphasised or different are perceived as a focal point)
10. **Common fate** (lines moving in the same direction are perceived as being part of the same group)

Overall website design

The website can be viewed and interacted with at <https://tinyurl.com/2s3hktyr>.

As recommended by the UK visualisation guidelines (40), the website has been designed to limit the number of options and the number of visuals presented to the user at any one time. Thus, to minimise the cognitive load, the website consists of a linear progression through four screens:

- The welcome screen
- The personality quiz
- The personality results
- The cybersecurity visualisation

I chose this four-screen structure to minimise the amount of information presented at once, while ensuring that connected information, such as the 44 personality questions, wasn’t unnecessarily split into different pages (to ensure that meaningful information is kept together, as per *information chunking* (40)).

Each page contains a single button to progress to the following page, located at the bottom of the page (as per the *consistency* guideline). Back buttons were not directly included in the interface (except for within the *cybersecurity visualisation* page) in order to minimise the number of visuals presented to the user (*limit of visuals*) and to encourage a linear progression through the site, but users had the option to use the browser navigation buttons to return to previous pages if wanted.

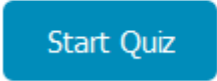
CSS was used to format all the buttons uniformly as blue with rounded edges and white text. This ensured there was sufficient contrast between the text and background (as per the typography guidelines in (40)), and that the colour scheme was ‘simple and elegant’ (i.e. blue, red or grey (40)) without distracting the user’s attention.

A set of screenshots showing the different web pages is available in Appendix 5 (Website screenshots).

The welcome screen

This screen was deliberately kept minimal, in order to not overwhelm the user when they first load the website. There is a simple user interface, with only one option for the user: to click the ‘Start Quiz’ button, styled using the consistent formatting described above.

Welcome to the Personality Quiz



The personality quiz

The personality questions from the original paper (23) were included verbatim in the training tool, with the only modification being the change from ‘disorganized’ to ‘disorganised’ to maintain consistency with UK spelling used throughout the rest of the tool.

However, the original wording does not fully adhere to the typography guidelines in (40). One guideline states ‘text in infographics should be easy to read and self-explanatory.’ The questions in the original paper are written as a continuation of the sentence ‘I see myself as someone who: ’, in the third person (such as, ‘is talkative,’ ‘is depressed, blue’). A clearer alternative would be to make each question self-contained and written in the first person, such as ‘I am talkative’ or ‘I am depressed and blue.’ Since such changes may alter the meaning and interpretation of the questions, future studies would need to validate these modifications to ensure the accuracy of responses.

The interface has been kept simple and minimal in order to focus the user’s attention on the questions. The full set of questions can be found in Appendix 3 (Big-Five Personality Traits). Each question is testing for a specific personality trait, and some of the questions are reverse scored. For example, ‘Is talkative’ is a measure of Extraversion and is *not* reverse scored (i.e. a higher answer indicates higher extraversion), and ‘Tends to find fault with others’ is a measure of Agreeableness and is reverse scored (i.e. a higher answer indicates lower agreeableness).

Personality Quiz

I see myself as someone who:

Is talkative

☐ Disagree Strongly ☐ Disagree a little ☐ Neither agree nor disagree ☐ Agree a little ☐ Agree strongly

Tends to find fault with others

☐ Disagree Strongly ☐ Disagree a little ☐ Neither agree nor disagree ☐ Agree a little ☐ Agree strongly

Does a thorough job

☐ Disagree Strongly ☐ Disagree a little ☐ Neither agree nor disagree ☐ Agree a little ☐ Agree strongly

Is depressed, blue

☐ Disagree Strongly ☐ Disagree a little ☐ Neither agree nor disagree ☐ Agree a little ☐ Agree strongly

Is original, comes up with new ideas

☐ Disagree Strongly ☐ Disagree a little ☐ Neither agree nor disagree ☐ Agree a little ☐ Agree strongly

Is reserved

☐ Disagree Strongly ☐ Disagree a little ☐ Neither agree nor disagree ☐ Agree a little ☐ Agree strongly

Is helpful and unselfish with others

☐ Disagree Strongly ☐ Disagree a little ☐ Neither agree nor disagree ☐ Agree a little ☐ Agree strongly

Can be somewhat careless

☐ Disagree Strongly ☐ Disagree a little ☐ Neither agree nor disagree ☐ Agree a little ☐ Agree strongly

The personality results

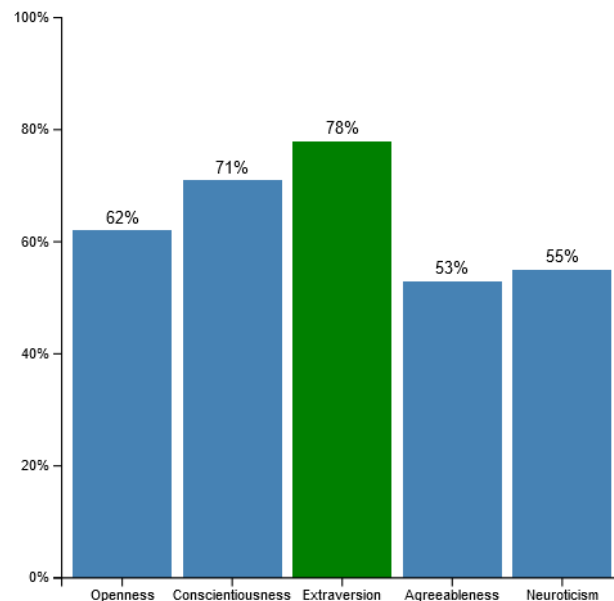
The scores are calculated by converting the five-point Likert scale of ‘Disagree Strongly’ to ‘Agree Strongly’ into a score out of five, with ‘Agree Strongly’ being five for non-reverse-scored questions and one for reverse-scored questions, as detailed in the original Big-Five Taxonomy paper (23).

There are 44 questions in total, meaning that are a different number of questions for each of the five personality traits. For example, a score of 20 for extraversion is not the same as a score of 20 for openness. Rather than present the absolute scores that a user received for each personality trait (which may be misleading), the scores are divided by the maximum possible score for each personality trait, converted into a percentage, and rounded to the nearest whole number.

The user is then presented with these results, displayed in a bar chart for easy comparison of heights, with the percentage displayed to allow accurate comparison of percentages, and with the highest trait displayed in green. The principle of *emphasis* is used to highlight the user’s highest trait: both by colouring the bar in a different yet neutral colour (i.e. green), and by reiterating the trait under the graph textually in bold.

The principle of closure (40) states that charts do not need borders around the entirety of the chart, as this creates a ‘boxed’ effect. Hence only the x and y axes have been included (since labels are needed on both axes to provide the percentages and personality traits).

Personality Test Results



Your highest personality trait is **Extraversion**
This trait is associated with a deep learning approach.

[See your personalised cybersecurity visualisation!](#)

The cybersecurity visualisation

As per the literature, openness, conscientiousness, extraversion, and agreeableness are associated with a deep learning approach (i.e. learning to *understand*), while neuroticism is associated with a surface learning approach (i.e. learning to *pass a test*). Additionally, conscientiousness is associated with an achieving learning approach (i.e. learning to *gain academic recognition*, such as by reading additional readings).

The user was presented with one of two pages, depending on their personality trait. If the user's highest trait was neuroticism (or neuroticism was *one of* their highest traits, if there were multiple highest traits), then the user was presented with a visual password generation mechanism. Otherwise, the user was presented with a visual story of the 23andMe data breach in 2023.

The surface learning approach

Users who adopt a surface learning approach are extrinsically motivated, and will often perform the minimum required to pass, through rote learning and memorisation without properly engaging with the material. As a result, providing surface learners with cybersecurity information followed by a test is ineffective, as they are unlikely to retain the information long-term and will view the test as a hurdle to pass rather than an opportunity to learn.

Given that these users often want to do the minimum amount of work, the aim of this visualisation is to provide them with a mechanism to perform cybersecure behaviours with the minimum overhead. This visualisation provides users with a password generation mechanism, based on the most recent

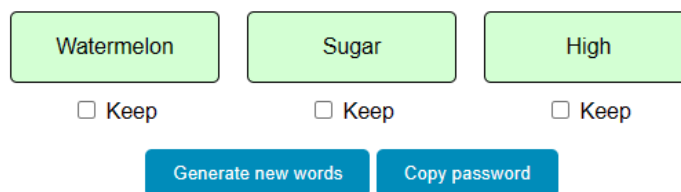
advice from the NCSC (National Cyber Security Centre) (44). This advice is the ‘three word approach’, in which users concatenate three unrelated words to form a secure password, such as ‘CoffeeTrainFish’.

The visualisation provides users with a graphical interface for creating such passwords, as shown below:

Personalised Cyber Security Visualisation (Surface Learning Approach)

The NCSC recommends using [the three word approach](#) to create strong passwords. This is where you put three random words together to create a password, such as ‘CoffeeTrainFish’ or ‘WallTinShirt’.

Click the button below to generate three random words for your password.



Watermelon	Sugar	High
<input type="checkbox"/> Keep	<input type="checkbox"/> Keep	<input type="checkbox"/> Keep
Generate new words		Copy password

The page is kept uncluttered, as per the *limit of visuals* guideline, with a short explanation given at the top, and an intuitive graphical interface taking up around half of the page. The three words are each presented on a light green background, to subconsciously signal to the user the idea of the password being ‘good’ or ‘correct’ (as per the *familiar elements* guideline), while also maintaining contrast with the black text.

When the page initially loads, the site automatically generates and displays three random words as an example, to save the user having to click the Generate button. The user can check and uncheck each of the three checkboxes underneath the words to keep one or more of the words. This allows the user to create a more memorable password (since they will keep words they like or recognise) while maintaining the element of randomness and unpredictability that a strong password needs.

The buttons use the same formatting (i.e. blue with rounded edges and white text) as previous pages to maintain consistency, and only two buttons are provided: one to ‘Generate new words’ and one to ‘Copy password’.

Clicking the *generate* button replaces the existing words with three other random words. The generation process uses [random-word-api.herokuapp.com](#), which is an API for requesting random English words.

Clicking the *copy* button concatenates the three words and copies them to the device’s clipboard and presents a temporary message to the user signalling that the action has been successfully performed. After five seconds, the message disappears and the interface is reset (i.e. the three ‘Keep’ options are set to unchecked, and three new words are generated):

Personalised Cyber Security Visualisation (Surface Learning Approach)

The NCSC recommends using [the three word approach](#) to create strong passwords. This is where you put three random words together to create a password, such as 'CoffeeTrainFish' or 'WallTinShirt'.

Click the button below to generate three random words for your password.

Watermelon	Sugar	High
<input type="checkbox"/> Keep	<input type="checkbox"/> Keep	<input type="checkbox"/> Keep
Generate new words		Copy password

Copied **WatermelonSugarHigh** to clipboard

Theoretical underpinnings for the surface learning approach

Since users high in neuroticism are more likely to engage in insecure cyber behaviours (see Appendix 4 (Literature Review)), they may be less concerned with potential risks on this site, such as:

- The URL hyperlinked to 'the three word approach' may be malicious since the link address is not shown directly
- The API providing the words might track which words are accessed
- The website itself might track accessed words to guess passwords

Thus, the tradeoff was made in favour of a visually appealing site (such as not showing the full URL to keep the text concise), and not providing the source code since the user is unlikely to verify it.

As this is a standalone page, users can bookmark the page to use in the future for password generation. Since surface learning is associated with having a minimal cognitive overhead, this page allows users to quickly generate memorable passwords, improving their cyber behaviours.

Since there is no method to manually type in words to any of the three boxes (without inspecting and editing the raw HTML), the easiest way to create a password is to repeatedly generate words, keeping favourable words and re-generating unfavourable words, until a satisfactory combination is found. The user can then click the copy button and paste it into the desired application. This mitigates the risks associated with users choosing part or all of the password, since the most secure path (i.e. relying solely on automated generation and avoiding keyboard input) is also the path of least resistance, and hence is the path most likely to be chosen by users with a surface learning approach.

Potential risks:

It is possible that an attacker may intercept the traffic to and from this site (or that the site owner is malicious and is tracking requests), which does present a security risk. However, the alternative to this approach is either user-generated passwords (which are predictable, weak, and often reused) or automatically-generated passwords (which are unmemorable and often written down in insecure places). Thus, while some risk remains with this method, it is still relatively secure compared to the alternatives (and the user is unlikely to be concerned by these risks if they are willing to use a web-based password generation mechanism).

In addition, after the password has been copied, the site automatically resets the interface and generates three new words so that the password is no longer displayed on the screen, and removes the

message from the screen. The message text is deleted from the HTML (and not simply hidden from the user), ensuring there is no trace of the password left in the site after the five seconds have elapsed. This ensures the maximum amount of security is given to potentially-insecure users who may not proactively take secure steps such as re-generating new words to flush the password from the screen.

Deep learning approach

Users who adopt a deep learning approach are intrinsically motivated, and want to understand and connect with ideas presented to them by looking for the underlying principles. Thus, the aim of this visualisation was to walk users through a recent case study of a data breach to illustrate the importance of not reusing passwords and using Two-Factor Authentication.

I chose to use the 23andMe data breach for the following reasons:

- It is recent (October 2023)
- It is directly relevant to members of the public (since it involved the exposure of sensitive personal and genetic information, rather than just the exposure of confidential company information)
- It connects to broader issues about the protection and regulation of sensitive data
- The cyber attacker is 'known' (i.e. has an online pseudonym that we can refer to)

The 23andMe case study is presented over 6 frames, followed by a summary screen. The frames are viewed one at a time by clicking on forwards and backwards buttons at the bottom of the screen. Each frame explains one part of the 23andMe breach timeline, ranging from April 2023 to October 2023. The frames contain two main components: a textual description and a visualisation.

Some frames contain extra information, which is only accessible to users with an achieving learning approach (as part of the personalisation aspect). Each frame also includes a URL for further reading and/or verification of the information.

Appendix 1 (23andMe timeline) presents a table shows the date, description, URL and extra information (if applicable) shown on each frame. Appendix 2 (23andMe visualisations) shows the visualisations in each frame. An example of how the information is put together in the final webpage is shown below.

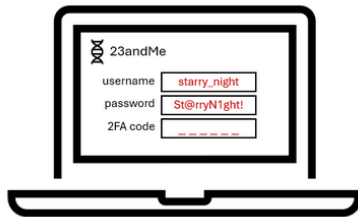
For example, the following shows two screenshots of Frame 5, before and after the user clicks on ‘Click to reveal more information!’:

23andMe Data Breach

November 2023

23andMe resets everyone's passwords, and implements mandatory Two-Factor Authentication (2FA) on all accounts, to prevent further unauthorised access to user data.

[Click to reveal more information!](#)



For more information, visit: <https://blog.23andme.com/articles/addressing-data-security-concerns>



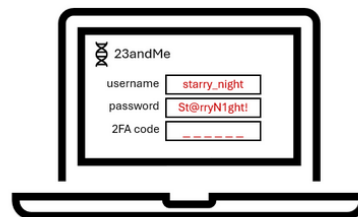
23andMe Data Breach

November 2023

23andMe resets everyone's passwords, and implements mandatory Two-Factor Authentication (2FA) on all accounts, to prevent further unauthorised access to user data.

[Click to reveal more information!](#)

Two-Factor Authentication is a type of Multi-Factor Authentication (MFA), and requires users to provide extra authentication for added security



For more information, visit: <https://blog.23andme.com/articles/addressing-data-security-concerns>



Adhering to the typography guidelines

1. Text should be easy to read and self-explanatory	Technical terms were removed, and text was written to be easily understood without prior knowledge. Multiple short sentences were used instead of one long sentence, where applicable
2. Typography should be appropriate to the message	Sans serif was used throughout the site, as this has been found to be more readable than serif fonts (45), and is recommended for people with dyslexia (46)
3. There should be a maximum of two typefaces	Monospace font was used in the visualisations to highlight ‘computerised’ text, such as text in a database. All other font was sans serif
4. Type size and line length should be coordinated	A minimum font size of 12pt was used throughout the site, as per web readability guidelines (47)
5. Bold, rather than italics, should be used for emphasis	Only bold was used for emphasis (such as on the final frame to emphasise the security measures users should implement)
6. Bolded text should be sufficiently contrasted from regular text	Emphasised text is implemented with the HTML ‘strong’ tag
7. All-capitals should be avoided when rapid reading is required	All-capitals have been avoided, except in two of the infographics, which do not require rapid reading
8. Titles should be the most dominant element and should	Titles are displayed with the HTML heading tag at the top of the page, above all page content, and summarise the purpose of the page

present the purpose and focus on the message	
9. There should be sufficient contrast between the title and narrative text in terms of font size and bold	The title is displayed in a larger font size
10. When typing white text on a black background, use a sans serif font in a larger size	Not applicable (only white, grey, light red and green backgrounds were used)
11. Text and backgrounds should be sufficiently contrasted to be legible	Black text is presented on either a light grey or white background in the web page. Within the visualisations, black text is presented either on a light red background, or a white background, white text is presented either on a light green or dark green background, or red text is presented on a white background
12. Do not use multi-coloured or gradient backgrounds	Only white or light grey backgrounds were used
13. Do not use black ink on dark red or dark purple paper	Not applicable (the visualisations are only presented on a screen, rather than printed)
14. Large blocks of text should be left-aligned	All blocks of text and titles have been left-aligned
15. Include orientating text to tell users about the relevance of the infographic	A description is provided prior to each visualisation
16. When embedding an infographic in another page, include the key message in large text	Not applicable (the web page is a standalone item and is not being embedded into anything else)

Frame sections

Each frame is split into four sections:

- Heading
- Description
- Image
- URL

The description block contains the extra information (if present). There are forwards and backwards buttons at the bottom of the screen to navigate between the frames.

Per typography guideline 8, the heading is placed prominently at the top of the screen. The order of the Description, Image, and URL was chosen to adhere to the principles of *order* and *hierarchy* (40). The Description provides textual information about the data breach, then the Image supplements the text and provides a visual representation of the data breach to aid understanding (but is not intended as a standalone image), and the URL provides a link to a reputable source that can be optionally accessed if wished. The URL is placed last as it is the least important of the three sections. Placing the Image between the Description and the URL also splits the text sections up so there is not one long block of text, which would be visually unappealing.

The two textual sections (Description and URL) are displayed on a light grey background. The use of light grey is intended to not draw attention to itself per se (since light grey is a neutral colour (40) but maintains enough contrast to the text to ensure readability, as per typography guideline 11). This background uses the Gestalt principle *enclosure*, where elements that are enclosed by a border or

common field of colour are seen as connected. This ensures the information is *chunked* (40) and is meaningfully grouped together, without explicitly introducing section headings (which may clutter the interface and introduce unnecessary text).

The webpage is rescalable, so users could zoom in for larger text if wanted. The HTML was also designed to be responsive and to adapt to different screen sizes and browser dimensions while preserving the readability of the text and the overall structure of the page.

Heading

The heading is constant across all the frames, and is '23andMe Data Breach'. The heading is formatted using the CSS heading styles to ensure the website is accessible to screen readers. Typography guideline 8 states that titles should be the most dominant element of an infographic, and guideline 9 states that there should be sufficient contrast between the title and narrative text. These guidelines are achieved by putting the title at the top of the screen in a larger font size and in bold, and putting the text sections on a light grey background underneath to visually distinguish it from the heading.

Description

For a full list of dates, source URLs, descriptions and extra information, see Appendix 1 (23andMe timeline). The following shows the six text descriptions that are presented over the six frames.

1. A cyber attacker called 'Golem' obtains a database of stolen usernames and passwords.

Frame 1 sets the scene for the data breach, and introduces the person 'Golem'. This is in accordance with Framing Principle 2: 'Make it clear who the villains are' (41).

2. Golem tries to log in to 23andMe using each of the stolen usernames and passwords, hoping that people have reused their passwords for the 23andMe site.

Frame 2 explains in plain English how a credential stuffing attack works. The frame also uses language that non-technical users would be more familiar with, such as 'stolen usernames and passwords' rather than 'compromised credential pairs.' In order to maintain understandability and simplicity, some of the details of how this would have worked in practice have been skipped. For example, Golem likely used an automated tool to try each of the credentials, but an explanation of an automated credential stuffing tool (such as Metasploit (48)) is not crucial to understanding the timeline of the data breach, and would overcomplicate the frame.

3. Golem accesses 14,000 user accounts using this method, and then uses the 'DNA Relatives' feature to connect to 6.9 million linked accounts

Frame 3 explains the extent of the data breach. Exact numbers are provided to the user as part of Framing Principle 1: 'Do not exacerbate cybersecurity' (41), while also emphasising the magnitude of the impact.

4. Each of the 6.9 million profiles contains: the display name, when you last logged in, your relationship labels (masculine, feminine, neutral), your predicted relationship and DNA percentage match, your ancestry reports, your location, your ancestors' birth locations and family names, your profile picture, birth year, and family tree.

Frame 4 continues to explain the effect of the data breach, highlighting the types of sensitive information that were stolen

5. 23andMe resets everyone's passwords, and implements mandatory Two-Factor Authentication (2FA) on all accounts, to prevent further unauthorised access to user data.

Frame 5 follows Framing Principle 3: ‘Give cybersecurity a face by putting the heroes in the spotlight’, and emphasises the actions that 23andMe took to prevent further unauthorised access.

6. Golem sells the data they have already collected on the dark web. They sell the data in batches, with one batch containing data specifically on people with Chinese ancestry, and another batch containing only data on Ashkenazi Jews.

Frame 6 follows Framing Principle 6: ‘Connect to the undercurrent’, and links the data breach to wider societal issues about racism and the targeting of ethnic minorities (49). This point is further emphasised by the extra information ‘The fact that Golem is selling data by ethnicity implies that they are targeting minority groups. This could be used for identity theft or personalised phishing attacks,’ which was only available to users with an achieving learning approach (i.e. high in conscientiousness), and further connected the data breach to the undercurrent of data protection concerns.

Image

The images were embedded in the page as SVG (scalable vector graphics) files. Since these are scalable, the user could zoom in on the images without losing image quality. This format also enables future iterations of the web page to incorporate these visualisations as interactive elements with clickable components.

URL

Users with a deep or achieving learning approach (i.e. who are high in openness, conscientiousness, agreeableness, or extraversion), are more likely to practice good cybersecurity behaviours (see Appendix 4 (Literature review)). Thus, users may be concerned about clicking unknown hyperlinks that may redirect to a malicious site. The source section therefore included the URL in hyperlinked text, so that a meticulous user could copy and paste the URL directly into their browser instead of clicking the hyperlink.

The URLs also linked to a range of news sites (rather than re-linking to the same two or three sites), to provide a breadth of information if the user wanted to follow up on the sources.

The sites referenced were:

1. engadget
2. Cyber Management Alliance
3. BBC News
4. 23andMe (Customer Care)
5. 23andMe (Blog)
6. Health IT Target

Extra information

The extra information was only displayed for users with an *achieving learning approach* (i.e., whose highest trait was conscientiousness), to allow them to strategically learn more information about the case study and understand the wider context in which the data breach happened.

The extra information was only displayed if the user chose to click on the ‘click to reveal’ text, in order to allow the user to proactively search and discover information, rather than be passively presented with all the information. This gives the user a sense of autonomy, and a chance to extend their learning in a non-compulsory manner (since the extra information was not crucial to know in order to understand the case study). This also kept the screen from being too cluttered and overwhelming when initially presented to the user.

Users with an achieving learning approach may not always want to seek out extra information, since there may be other external factors at play, such as time pressure.

For users with only a deep learning approach, the extra information was not displayed, but the source URLs were (if the user still wanted to proactively find more information about the incident).

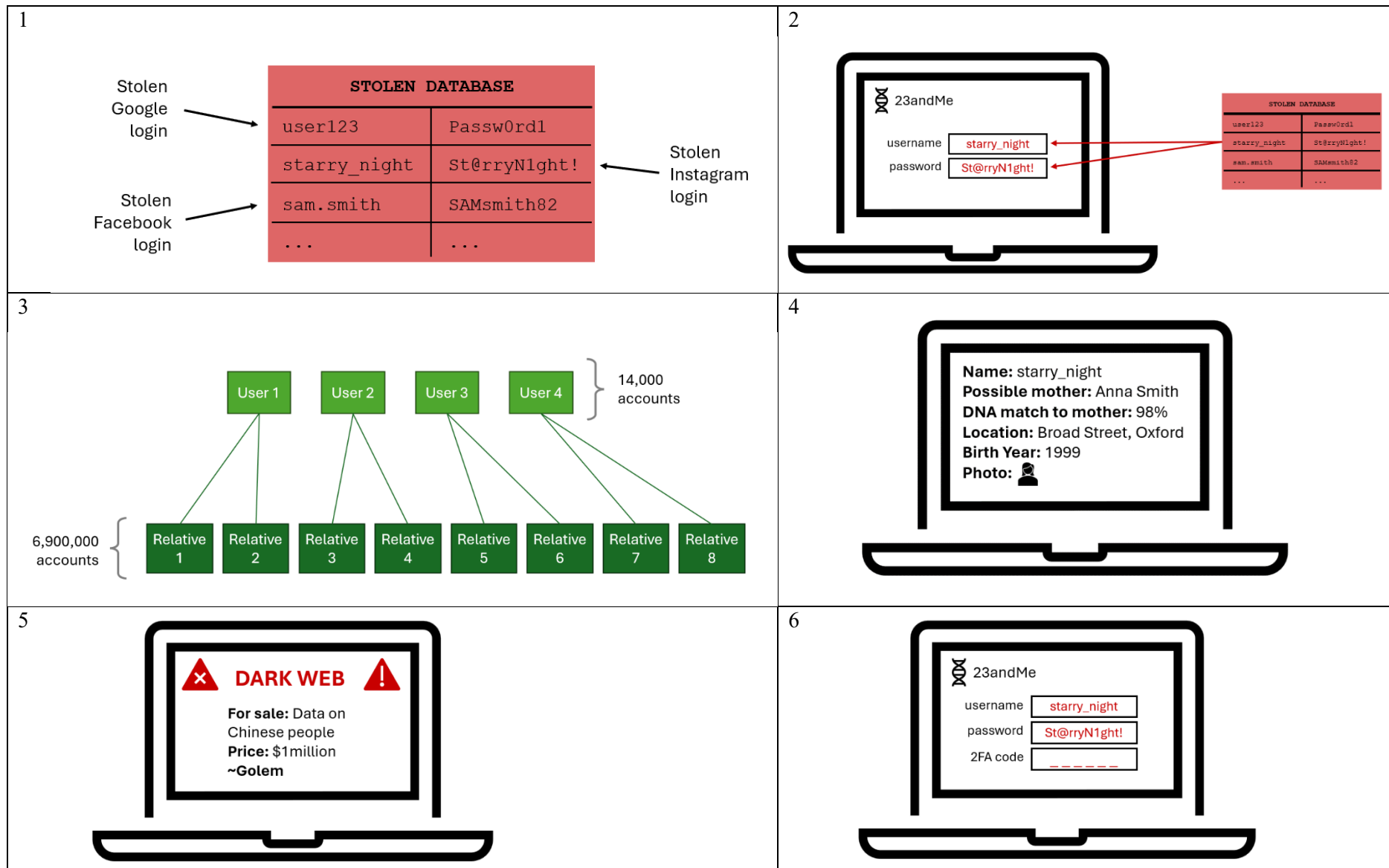
The interface was designed to be as intuitive as possible (rather than needing extensive instructions in order to interact with it). Thus, CSS was used to turn the cursor into a pointer when hovering over the ‘Click to reveal more information,’ to indicate to the user that it contained an interactive clickable component. The user could also re-hide the information by clicking on the text again in order to de-clutter the page.

Arrow buttons

The arrow buttons are styled with CSS to provide consistent formatting with the other buttons on the website (i.e. blue with rounded edges and white text). They are also displayed in a fixed position on the page (20 pixels above the bottom of the screen) to ensure they remain fixed while users navigate through frames. These CSS techniques ensure the buttons adhere to the principle of *consistency* (40). When the user hovers over the button, the opacity decreases slightly to indicate to the user that the button is clickable.

When the user is viewing the first frame, the ‘back’ button is disabled and coloured grey to indicate that the user cannot go back any further, and the hover effect is disabled. The same technique is applied on the final frame to the ‘forward’ button. When the button is clicked, the colour changes to dark blue to provide immediate feedback to the user that the button has been clicked, since there is a slight delay between the button being clicked and the next image and text block being displayed on the screen. These techniques provide the user with immediate and intuitive feedback, helping users easily interact with the page.

To allow the user to navigate the pages in the most intuitive way, an additional navigation mechanism was added to the web page to allow users to use the left and right arrow keys on the keyboard instead of the on-screen forwards and backwards buttons.



Visual principles

The six visualisations are provided above for easy reference, and are provided in greater resolution in Appendix 2 (23andMe Visualisations).

Visualisation 1:

This visualisation depicts a database of stolen credential pairs. It emphasises the varying origins of the stolen credentials with well-known social media websites, like ‘Facebook’, ‘Instagram’ and ‘Google’. The database text is displayed in a monospace font to highlight the digital nature of the data. The first two credential examples are designed to be simplistic and representative of a generic username and password (*user123* and *Passw0rd1*), allowing the user to infer the data type without explicit labelling. The light red background draws on users’ pre-existing notions of danger, and emphasising that this database contains ‘dangerous’ information.

Visualisation 2:

This visualisation shows a cyber attacker inputting the stolen credentials into the 23andMe login page. As discussed earlier, this image abstracts away the details of automated credential stuffing tools. The text, arrows, and database are all coloured with the same hue of red (with the database having increased transparency for legibility) to appeal to the Gestalt principle of *similarity*, where similar elements are perceived as related. This emphasises how the username-password pairs have been taken from the stolen database.

Visualisation 3:

This visualisation uses a hierarchical flow diagram (39) to depict the flow of compromise from the initial 14,000 accounts to the further 6,900,000 accounts (via the ‘DNA Relatives’ feature). This highlights how even accounts with secure passwords can be compromised through connections to insecure accounts. The use of green draws on users’ pre-existing notions of ‘good’ and ‘safe’ to show that these accounts were created by non-malicious users. The use of the arrows also draws on the Gestalt principle of *connectedness*, linking the two types of accounts.

Visualisation 4:

This visualisation uses the Gestalt principle of *similarity* by employing the same laptop shape as visualisation 2, indicating that all these activities are occurring on a computer/the Internet. The use of sensitive information (such as ‘DNA match to mother’) highlights the personal nature of the compromised data.

Visualisation 5:

This visualisation uses the same hue of red as visualisations 1 and 2 to signify its connection with the initial compromised database. It also uses the same laptop shape as visualisations 2 and 4 to maintain the computer/Internet theme. The use of whitespace and underscores indicates missing elements, emphasising the incompleteness of the image and illustrating the importance of 2FA in preventing cyber attackers from having the complete login.

Visualisation 6:

This final image ties together all the connected components from the previous frames, using the common shape of the laptop and the common hue of red. The cross symbol and exclamation mark in red immediately signal danger to the user the idea, reinforced by the text ‘DARK WEB’. Since this text is not meant for rapid reading, the typography guideline recommending minimal use of all-caps text is still met.

The final frame

The final frame was presented after the first six frames, and did not contain an image as it was not part of the 23andMe data breach case study. The final frame explained what lessons users should learn from the 23andMe data breach, and why these measures are important for users to implement.

Text in the final frame (with bold text formatted using HTML strong tags):

What can we learn from the 23andMe data breach?

You should **use Two-Factor Authentication** whenever possible. This means that even if attackers have your password, they will still need another form of verification to access your account. This is often a code sent to your phone or email.

It is also important to **use unique passwords** for each of your accounts. If one account is compromised, attackers will not be able to access your other accounts with the same password.

Finally, you should consider **using a password manager** to generate and store complex passwords. This can help you keep track of your passwords and ensure they are strong and unique.

Extra information in the final frame (only visible to users high in conscientiousness):

As of 2018, the NCSC (National Cyber Security Centre) no longer recommends regularly changing passwords, and instead to only change them if there is a suspicion or indication of a breach. This is because users often choose new passwords that are only a minor variation of the old one, which can be easily guessed by attackers.

Source URL in the final frame:

<https://www.ncsc.gov.uk/collection/passwords/updating-your-approach>

23andMe Data Breach

What can we learn from the 23andMe data breach?

You should **use Two-Factor Authentication** whenever possible. This means that even if attackers have your password, they will still need another form of verification to access your account. This is often a code sent to your phone or email.

It is also important to **use unique passwords** for each of your accounts. If one account is compromised, attackers will not be able to access your other accounts with the same password.

Finally, you should consider **using a password manager** to generate and store complex passwords. This can help you keep track of your passwords and ensure they are strong and unique.

[Click to reveal more information!](#)

As of 2018, the NCSC (National Cyber Security Centre) no longer recommends regularly changing passwords, and instead to only change them if there is a suspicion or indication of a breach. This is because users often choose new passwords that are only a minor variation of the old one, which can be easily guessed by attackers.

For more information, visit: <https://www.ncsc.gov.uk/collection/passwords/updating-your-approach>



Adhering to the cybersecurity awareness campaign guidelines

Bada et al's paper (42) recommended the following five principles to enhance cybersecurity awareness campaigns:

1. Campaigns need to be organised and prepared by professionals
2. Campaigns should not aim to invoke fear in people
3. Security education needs to be 'targeted, actionable, doable and provide feedback'
4. Users need continuous feedback and training to sustain change
5. Campaigns need to account for different characteristics and cultural contexts

This final frame ties all the previous frames together and uses these principles to provide a final message:

1. The case study was organised and prepared to the best of the author's ability, aiming to provide clear, factual information in a structured way.
2. The 23andMe data breach case study was not presented to invoke fear in people, and instead aimed to neutrally present the facts about what happened, and provide some lessons that users can learn from the event.
3. The final three suggestions for the user (using 2FA, using unique passwords, and using a password manager) are both actionable and doable (rather than vague advice like 'use better passwords' or 'don't get hacked'). The case study was also targeted, since only users with a certain personality type and learning approach were presented with this information, and within that group, the presentation was further tailored (to either show or not show the extra information) depending on whether the user had an achieving learning approach.
4. The case study is currently designed as a one-off training material, but could be adapted to visualise future data breaches to show the user the importance of staying up to date with best cybersecurity practices, since threats are constantly present and ever-changing.
5. Similar to point 3, this campaign explicitly accounted for different user characteristics by providing a personalised cybersecurity visualisation depending on the results of the user's personality quiz.

Discussion

While every effort was made to create a well-developed, theory-driven cybersecurity visualisation tool, future iterations of this tool could improve on certain aspects. For example, when neuroticism is the joint-highest personality trait (along with another personality trait), the web page treats this as though it were neuroticism alone, and provides the user with a surface learning approach. Future studies may be needed to validate the accuracy of this assumption.

Similarly, when users have conscientiousness as a joint-highest personality trait, the web page treats this as conscientiousness alone, and provides the user with the joint deep learning and achieving learning version of the 23andMe case study, but this should ideally be empirically validated.

The random words API did not allow parameters to specify the type of word, and sometimes resulted in complex words being presented (such as 'carceral,' 'entente', or 'coxswained'). Future versions could use a more advanced API that allows users to specify the desired complexity of words.

In terms of next steps for future research, this tool could be evaluated in practice to test whether it has a positive effect on participants' cybersecurity behaviours. Post-use interviews could also be used to refine the acceptability and usability of the platform interface.

Bibliography

1. Denno J. Attacking the human-the weakest link in cybersecurity: Utica College; 2016.
2. Daudi M. Trust Framework on Exploitation of Humans as the Weakest Link in Cybersecurity. *Applied Cybersecurity & Internet Governance*. 2023;2(1):1-26.
3. Rahman T, Rohan R, Pal D, Kanthamanon P, editors. Human factors in cybersecurity: a scoping review. *Proceedings of the 12th International Conference on Advances in Information Technology*; 2021.
4. Zhu F, Carpenter S, Kulkarni A, Kolimi S. Reciprocity attacks. *Proceedings of the Seventh Symposium on Usable Privacy and Security*; Pittsburgh, Pennsylvania: Association for Computing Machinery; 2011. p. Article 9.
5. Ncubukezi T, editor Human errors: A cybersecurity concern and the weakest link to small businesses. *Proceedings of the 17th International Conference on Information Warfare and Security*; 2022.
6. Kadena E, Gupi M. Human factors in cybersecurity: Risks and impacts. *Security science journal*. 2021;2(2):51-64.
7. Waldrop MM. How to hack the hackers: The human side of cybercrime. *Nature*. 2016;533(7602).
8. McAfee C. Net losses: estimating the global cost of cybercrime. McAfee, Centre for Strategic & International Studies. 2014.
9. Lorenzo N, Julie H, Kerrianne B, editors. Analyzing Cybersecurity Definitions for Non-experts2023 2023-07-04 04:07:00: IFIP International Symposium on Human Aspects of Information Security & Assurance (HAISA 2023), Kent, GB; IFIP International Symposium on Human Aspects of Information Security & Assurance (HAISA 2023), Kent, GB.
10. Lorenzo N, Julie H, Kerrianne B, Charlotte H, editors. Cybersecurity Definitions for Non-Experts2023 2023-08-06 04:08:00: Poster session at the Symposium on Usable Privacy and Security, Anaheim, CA, US; Poster session at the Symposium on Usable Privacy and Security, Anaheim, CA, US.
11. Cavallo S. Visualizing Cybersecurity-a comparative study toward a security visualization methodology: Politecnico di Torino; 2023.
12. Pattinson M, Jerram C, Parsons K, McCormac A, Butavicius M. Why do some people manage phishing e-mails better than others? *Information Management & Computer Security*. 2012;20:18-28.
13. Conetta C. Individual differences in cyber security. *McNair Research Journal SJSU*. 2019;15(1):4.
14. Mersinas K, Bada M, editors. Behavior Change Approaches for Cyber Security and the Need for Ethics. *The International Conference on Cybersecurity, Situational Awareness and Social Media*; 2023: Springer.
15. Egelman S, Peer E. Scaling the Security Wall Developing a Security Behavior Intentions Scale (SeBIS)2015.
16. Ertan A, Crossland G, Heath C, Denny D, Jensen R. Cyber security behaviour in organisations. *arXiv preprint arXiv:200411768*. 2020.
17. Alruwaili A. A REVIEW OF THE IMPACT OF TRAINING ON CYBERSECURITY AWARENESS. *International Journal of Advanced Research in Computer Science*. 2019;10(5).
18. McCrohan K, Engel K, Harvey J. Influence of Awareness and Training on Cyber Security. *Journal of Internet Commerce*. 2010;9:23-41.
19. Peker YK, Ray L, Da Silva S, Gibson N, Lamberson C, editors. Raising cybersecurity awareness among college students. *Journal of The Colloquium for Information Systems Security Education*; 2016.
20. Muhirwe J, White N. CYBERSECURITY AWARENESS AND PRACTICE OF NEXT GENERATION CORPORATE TECHNOLOGY USERS. *Issues in Information Systems*. 2016;17(2).
21. McBride M, Carter L, Warkentin M. Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. 2012.
22. Cobb-Clark DA, Schurer S. The stability of big-five personality traits. *Economics Letters*. 2012;115(1):11-5.

23. John OP, Srivastava S. The Big-Five trait taxonomy: History, measurement, and theoretical perspectives. 1999.
24. Gosling SD, Rentfrow PJ, Swann WB. A very brief measure of the Big-Five personality domains. *Journal of Research in Personality*. 2003;37(6):504-28.
25. McCrae RR, John OP. An introduction to the five-factor model and its applications. *Journal of personality*. 1992;60(2):175-215.
26. Kajzer M, D'Arcy J, Crowell CR, Striegel A, Van Bruggen D. An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers & security*. 2014;43:64-76.
27. Uebelacker S, Quiel S, editors. The Social Engineering Personality Framework. 2014 Workshop on Socio-Technical Aspects in Security and Trust; 2014 18-18 July 2014.
28. Biggs JB. Learning Process Questionnaire Manual. Student Approaches to Learning and Studying; ERIC; 1987.
29. Jensen M. Personality traits, learning and academic achievements. *Journal of Education and Learning*. 2015;4(4):91-118.
30. Asikainen H, Gijbels D. Do students develop towards more deep approaches to learning during studies? A systematic review on the development of students' deep and surface approaches to learning in higher education. *Educational Psychology Review*. 2017;29:205-34.
31. Chin C, Brown DE. Learning in Science: A Comparison of Deep and Surface Approaches. *Journal of Research in Science Teaching*. 2000;37(2):109-38.
32. Dolmans DH, Loyens SM, Marcq H, Gijbels D. Deep and surface learning in problem-based learning: a review of the literature. *Advances in health sciences education*. 2016;21:1087-112.
33. Hussin F, Hamed S, Jam SM. Approaches to learning of engineering students: Deep or surface. *International Academic Research Journal of Social Science*. 2017;3(1):122-7.
34. English L, Luckett P, Mladenovic* R. Encouraging a deep approach to learning through curriculum design. *Accounting Education*. 2004;13(4):461-88.
35. Adi D, Ariesta I, editors. Infographic in relation to the human information-processing system and its effectiveness to deliver complex information. *Journal of Physics: Conference Series*; 2019: IOP Publishing.
36. Bystrova T, editor Infographics as a tool for improving effectiveness of education. Convention 2019 "Modernization and Multiple Modernities"—Ekaterinburg, 2020; 2020: Knowledge E.
37. Çaka C, Dursun Ö. Evaluation of the effectiveness of different infographic designs. *Journal of Educational Technology and Online Learning*. 2022;5(3):519-34.
38. Elaldi S, Çifçi T. The Effectiveness of Using Infographics on Academic Achievement: A Meta-Analysis and a Meta-Thematic Analysis. *Journal of Pedagogical Research*. 2021;5(4):92-118.
39. Van Deursen N. Visual Communication for Cybersecurity: Beyond Awareness to Advocacy: River Publishers; 2022.
40. Lonsdale MdS, Lonsdale D. Design2Inform: Information visualisation. 2019.
41. de Bruijn H, Janssen M. Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*. 2017;34(1):1-7.
42. Bada M, Sasse AM, Nurse JR. Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:190102672. 2019.
43. Todorovic D. Gestalt principles. *Scholarpedia*. 2008;3(12):5345.
44. McCormack I. NCSC. 2016. Available from: <https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0>.
45. Josephson S. Keeping Your Readers' Eyes on the Screen: An Eye-Tracking Study Comparing Sans Serif and Serif Typefaces. *Visual Communication Quarterly*. 2008;15(1-2):67-79.
46. Association BD. Dyslexia Style Guide 2023 2023 [Available from: <https://cdn.bdadyslexia.org.uk/uploads/documents/Advice/style-guide/BDA-Style-Guide-2023.pdf?v=1680514568>].
47. Miniukovich A, De Angeli A, Sulpizio S, Venuti P, editors. Design guidelines for web readability. *Proceedings of the 2017 Conference on Designing Interactive Systems*; 2017.
48. Rapid7. Metasploit [Available from: <https://www.metasploit.com/>].

49. Ajanovic E, Sauer B. The rise of racism across Europe. *Children's Voices: Studies of interethnic conflict and violence in European schools*: Routledge; 2014. p. 17-32.