

## DATA MAP for 'SurveyResponses\_DigitalSecurityAroundTheWorld.csv'

The data is presented in the same order as the columns in the dataset (which may differ from the order in the questionnaire).

### [ID] Consecutive numbering of participants

### [Country]

- China [1]
- Germany [2]
- India [3]
- Israel [4]
- Italy [5]
- Mexico [6]
- Poland [7]
- Saudi Arabia [8]
- South Africa [9]
- Sweden [10]
- UK [11]
- USA [12]

### [Gender] What is your gender?

- Answers
  - Male [1]
  - Female [2]
  - Non-binary [3]
  - Describe yourself: [4, free text answer, single line]
    - Answers in **[Gender\_SelfDescription]**
  - I prefer not to answer this question [9999]

### [Age] Age bins

- Answers:
  - 18-24 [1]
  - 25-39 [2]
  - 40-54 [3]
  - 55+ [4]

### [Education] Education bins

- Answers:
  - Low [1]
  - Medium [2]
  - High [3]
  - Other [4]

### [Ethnicity] What is your race? (only for the US data)

- Answers:
  - White [1]
  - African-American [2]

- Hispanic or Latino [3]
- Asian [4]
- Other [5]

**[Q1] Which of the following devices to you use in your daily life?**

- Answers – unchecked [0] – checked [1]:
  - [Q1r1] Smartphones
  - [Q1r2] Static PCs / Desktop PCs
  - [Q1r3] Laptops
  - [Q1r4] Tablets
  - [Q1r5] Voice assistants or smart speakers (e.g., Alexa, Amazon Echo)
  - [Q1r6] Wearables (e.g., fitness trackers, smartwatches or other computer technologies that are worn on the body)
  - [Q1r7] None of the listed devices

**[Q2] Do you have any smart home devices in your household? If yes, for what purpose?**

*The “smart home” area includes all networked devices that you use in your living space. For example, systems that automatically open or close windows, doors, and shutters - so-called home automation technology. But smart home also includes household appliances such as refrigerators that keep you informed about their contents or robotic vacuum cleaners. These devices can often be operated from anywhere and many of these devices are connected to the internet.*

- Subquestions
  - [Q2r1] Energy and climate (e.g., “intelligent” lights or radiators)
  - [Q2r2] Security (e.g., networked alarm systems or video monitoring)
  - [Q2r3] Home and garden (e.g., “intelligent” shutters, robotic vacuum cleaners)
- Answers:
  - Yes [1]
  - No [2]
  - I am not sure [3]

**[Q3] How often do you use the internet for the following purposes?**

- Subquestions
  - [Q3r1] Online shopping
  - [Q3r2] Ordering services (e.g., booking travel, ordering food, car sharing)
  - [Q3r3] Selling goods or services (e.g., through auctions)
  - [Q3r4] Researching information and forming opinions (e.g., reading online newspapers)
  - [Q3r5] Uploading and sharing personal content you have created yourself (texts, images, photos, videos, music, software)
  - [Q3r6] Expressing opinions (e.g., posts on social media, online comments)
  - [Q3r7] Online banking
  - [Q3r8] Communication (e-mail, chat, video conferences etc.)
  - [Q3r9] Entertainment (e.g., streaming films, music, online games)
  - [Q3r10] Official transactions (e.g., ordering an identity card, tax return)
  - [Q3r11] Health services (e.g., electronic patient record, virtual doctor appointment)

- [Q3r12] Map services / navigation
- [Q3r13] Data storage (cloud services)
- Answers:
  - Several times a day [8]
  - Every Day [7]
  - Several times a week [6]
  - Once a week [5]
  - Several times a month [4]
  - Once a month [3]
  - Less than once a month [2]
  - Never [1]

**[Q4] How often do you use the following communication channels?**

- Subquestions
  - [Q4r1] Making telephone calls with a land line
  - [Q4r2] Making telephone calls with a smartphone / mobile telephone
  - [Q4r3] Video calls (e.g., Skype, Zoom, Microsoft Teams)
  - [Q4r4] Text messaging (SMS)
  - [Q4r5] Messenger services (e.g., WhatsApp, Signal)
  - [Q4r6] social media (e.g., Facebook, Twitter, Instagram)
  - [Q4r7] E-mail
  - [Q4r8] Online forums and communities
- Answers:
  - Several times a day [8]
  - Every Day [7]
  - Several times a week [6]
  - Once a week [5]
  - Several times a month [4]
  - Once a month [3]
  - Less than once a month [2]
  - Never [1]

Now we would like to ask you some questions on the subject of **digital security**.

**[Q6] How familiar are you with the following terms?**

For each of the following terms, please state how familiar you are with it.

- Subquestions
  - [Q6r1] Malware (viruses, worms, spyware, Trojans)
  - [Q6r2] Ransomware (extortion software)
  - [Q6r3] Phishing
  - [Q6r4] Spear phishing
  - [Q6r5] Two factor authentication (2FA)
  - [Q6r6] Biometric authentication process

- [Q6r7] Identity theft
- [Q6r8] Data leak / data theft
- [Q6r9] HTTPS
- [Q6r10] Hard drive encryption
- [Q6r11] End-to-end encryption
- [Q6r12] Transport encryption
- [Q6r13] Browser
- [Q6r14] Private browser mode (incognito mode)
- [Q6r15] IP address
- [Q6r16] URL
- [Q6r17] VPN (virtual private network)
- [Q6r18] Tor network
- [Q6r19] Ad blocker
- [Q6r20] (Love) scam / romance scam on the internet
- [Q6r21] Spam
- [Q6r22] Cloud
- 
- Answers
  - I've never heard of this [1]
  - I've heard of this but I don't know what it is [2]
  - I know what this is but I don't know how it works[3]
  - I know how this works[4]
  - I know very well how this works [5]

**[Q7] Have you personally been affected by cybercrime?**

For each of the following items please state if you have been affected.

- Question type:
- Subquestions
  - [Q7r1] Malware such as viruses or Trojans
  - [Q7r2] Phishing (spying on confidential data)
  - [Q7r3] Ransomware or extortion software
  - [Q7r4] Cyberbullying
  - [Q7r5] Fraud with online shopping
  - [Q7r6] External access to an online account
  - [Q7r7] Cyberstalking
  - [Q7r8] Data abuse (passing on or sale of personal data such as telephone number, address, bank details)
  - [Q7r9] Love scam / romance scam on the internet
- Answers:
  - Yes [1]
  - No [2]
  - I prefer not to answer this question [9999]

**[Q8] Where do you look for information on the topic of *digital security*?**

From the following information sources, please select all the ones that you use to inform yourself about digital security.

- Answers - unchecked [0] – checked [1]:
  - [Q8r1] I do not look for information on the topic of digital security
  - [Q8r2] Print media
  - [Q8r3] Online news
  - [Q8r4] social media
  - [Q8r5] Radio / podcasts
  - [Q8r6] Television
  - [Q8r7] Friends and family
  - [Q8r8] IT security experts
  - [Q8r9] Consumer centre, authorities
  - [Q8r10] Other: [free text answer]
    - Answers in: [Q8r10oer1]

Next you will see a number of statements on the topic of digital security. Please carefully read each statement and state how much you agree with the respective statement.

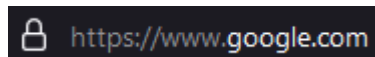
**[Q9] The following statements refer to communication with messengers that use end-to-end encryption (e.g., WhatsApp, Signal). Please read each statement carefully and indicate how much you agree with each statement.**

- Subquestions
  - [Q9r1] If my chat messages are protected by end-to-end encryption, then my messages can only be read on my device and by the recipient; nobody else can access and read them in transit.
  - [Q9r2] Not even the communication service provider that I use can read my messages if they are protected by end-to-end encryption.
  - [Q9r3] If someone has access to my smartphone, then this person can read my messages in the messenger app, despite end-to-end encryption.
  - [Q9r4] Because the developers of the messenger service know how the encryption works, they can also read my messages despite end-to-end encryption.
  - [Q9r5] The end-to-end encryption in messenger services is not secure because any encryption can be broken.
  - [Q9r6] If messages are end-to-end encrypted, they are sent directly from my device to the recipient's device, without any intermediate steps.
  - [Q9r7] If messages are end-to-end encrypted, they can also be read by third parties during transmission.
  - [Q9r8] If I send messages with end-to-end encryption, nobody knows when and with whom I am communicating.
  - [Q9r9] Messages that are sent over the internet are easier to read than text messages that are sent via the telephone network.
- Answers:
  - 5 fully agree [5]
  - 4 mainly agree [4]
  - 3 neutral [3]

- 2 mainly disagree [2]
- 1 fully disagree [1]
- I don't understand the statement [9999]

**[Q10] Next you will see some statements about digital security when surfing on the internet. Generally, an internet browser (e.g. Firefox, Chrome, Edge, Internet Explorer) is used for this. Please carefully read each statement and indicate how much you agree with the respective statement.**

If we mention "https" for websites, we mean websites that show a lock symbol in the address bar of your internet browser, like in this illustration:



- Subquestions
  - [Q10r1] I can identify a fraudulent website (e.g., a fake online shop that wants to capture my data), because no lock symbol is shown in the address bar of the internet browser.
  - [Q10r2] If https is used on a website, my internet provider does not know what I am clicking on the website.
  - [Q10r3] Https prevents the website operator from seeing what I am clicking on and viewing on the website.
  - [Q10r4] Websites that use https are trustworthy.
  - [Q10r5] If I visit websites that use https then other people that use my computer cannot see where I have been on the internet.
- Answers:
  - 5 fully agree [5]
  - 4 mainly agree [4]
  - 3 neutral [3]
  - 2 mainly disagree [2]
  - 1 fully disagree [1]
  - I don't understand the statement [9999]

**[Q11] Next you will see some statements about digital security when surfing on WLAN networks. Please carefully read each statement and state how much you agree with the respective statement.**

- Subquestions
  - [Q11r1] When I use a public WLAN, other devices that are also using this WLAN (e.g., laptops of other visitors in an internet café) can see what websites I am visiting.
  - [Q11r2] When I use a public WLAN, other devices that are also using this WLAN can generally see what data (e.g., passwords, credit card information) that I enter on websites.
  - [Q11r3] When I am connected to a public WLAN, it is easy to infect my device with malware.
  - [Q11r4] On a public WLAN, attackers can redirect me to specifically prepared websites and record the data that I enter there.
  - [Q11r5] When I use a public WLAN, other devices that are also using this WLAN can also read and change my emails.

- Answers:
  - 5 fully agree [5]
  - 4 mainly agree [4]
  - 3 neutral [3]
  - 2 mainly disagree [2]
  - 1 fully disagree [1]
  - I don't understand the statement [9999]

**[Q12] Next you will see some messages about digital security when surfing on the internet with a VPN (virtual private network). Please carefully read each statement and state how much you agree with the respective statement.**

- Subquestions
  - [Q12r1] When I use a VPN, my internet provider can no longer see what websites I visit.
  - [Q12r2] A VPN prevents malware from reaching my device.
  - [Q12r3] A VPN protects me from entering my passwords or credit card information on dangerous websites.
  - [Q12r4] A VPN protects me from unauthorized persons getting access to my device.
  - [Q12r5] A VPN is like end-to-end encryption between the website and my device.
  - [Q12r6] When I use a VPN, the VPN provider can see what websites I visit.
  - [Q12r7] When I use a VPN, the VPN provider can see in principle what data I enter on a website (e.g., passwords, credit card information).
  - [Q12r8] Surfing via the Tor network prevents my internet provider from seeing what websites I visit.
- Answers:
  - 5 fully agree [5]
  - 4 mainly agree [4]
  - 3 neutral [3]
  - 2 mainly disagree [2]
  - 1 fully disagree [1]
  - I don't understand the statement [9999]

**[Q13] Next you will see some statements on the topic of passwords and login processes. Please carefully read each statement and indicate how much you agree with the respective statement.**

- Subquestions
  - [Q13r1] The security of a password is higher if it includes numbers or special characters as well as letters.
  - [Q13r2] To increase the security of a password, it is sufficient to replace letters by numbers, for example to replace an "i" with a "1".
  - [Q13r3] To increase the security of a password, it is sufficient to use a word from a different language.
  - [Q13r4] A date of birth is a secure password as long as it isn't my own date of birth.
  - [Q13r5] The security of a password only depends on the length of the password.
  - [Q13r6] It is important for the security of my user accounts to regularly change the password.
  - [Q13r7] Attackers try to guess my password and enter a lot of different passwords manually.

- ⊖ [Q13r8] Using one strong password to log into different user accounts is perfectly safe.
- [Q13r9] Password managers generate secure passwords that cannot be guessed, even with technical assistance.
- [Q13r10] It is more secure to choose a weaker password that is easy to remember, than to write a strong password down (e.g., a note).
- [Q13r11] This is a control question. Please click on the second selection option from the right / from the bottom.
- [Q13r12] A password manager that I can use to and store all my accounts and passwords is not secure.
- [Q13r13] I have to log in to online banking with two processes so that the connection is encrypted, for example, with a password and TAN (transaction number).
- [Q13r14] If, in addition to entering my password, I have to confirm that I want to login into my email mailbox by mobile phone, it is harder for attackers to get into my email mailbox.
- [Q13r15] Facial recognition to log into my user account is very easy to trick, for example with a photo.
- [Q13r16] If I use, my fingerprint to log in to an Apple or Android smartphone, this is stored with the provider and can be stolen from there.
- [Q13r17] It is easier to steal my fingerprint and use it for authentication on my device than it is to guess my password.
- [Q13r18] Login processes such as fingerprints or facial recognition are imprecise and therefore less secure than passwords.
- Answers:
  - 5 fully agree [5]
  - 4 mainly agree [4]
  - 3 neutral [3]
  - 2 mainly disagree [2]
  - 1 fully disagree [1]
  - I don't understand the statement [9999]

**[Q14] Next you will see some statements on the topic of digital security of end devices. Please carefully read each statement and state how much you agree with the respective statement.**

- Subquestions
  - [Q14r1] When I enter my laptop password in public, somebody could look over my shoulder and read the password.
  - [Q14r2] To protect the data on my laptop even if it is stolen, a hard drive encryption must be used.
  - [Q14r3] Even if my laptop is stolen, my data is secure because my user account is protected by a password.
  - [Q14r4] Anti-virus software doesn't only protect my PC from viruses but also protects my online user accounts from attacks.
  - [Q14r5] Regular updates are sufficient to protect my device and my data from attacks.
  - [Q14r6] I don't need to lock devices such as my laptop, PC, smartphone etc. -when I am not using them, because the screen is dark anyway and nobody can read it.
  - [Q14r7] It is safer to send sensitive data via a computer than via a smartphone.
  - [Q14r8] The PIN for the SIM card is sufficient to protect the data on my smartphone.



- [Q14r9] Strangers cannot access my smart home devices as long as I use a secure password for them.
- Answers:
  - 5 fully agree [5]
  - 4 mainly agree [4]
  - 3 neutral [3]
  - 2 mainly disagree [2]
  - 1 fully disagree [1]
  - I don't understand the statement [9999]

**[Q15] Next you will see some statements on the topic of malware and deception on the internet. Please carefully read each statement and state how much you agree with the respective statement.**

- Subquestions
  - [Q15r1] If I don't discover anything suspect on my computer, then it is not infected with malware.
  - [Q15r2] As long as I don't download anything, my PC cannot be infected with malware (even if I visit a risky website).
  - [Q15r3] Is it more likely to pick up malware from visiting a porn website than visiting a website on the topic of sport.
  - [Q15r4] As long as I don't open a file infected with malware, it can't do any damage.
  - [Q15r5] Malware is mostly distributed via USB sticks.
  - [Q15r6] If Windows is not installed on my PC, it is more secure from attacks, because attackers do not bother to attack operating systems few people use.
  - [Q15r7] Malware can be installed on my device (Laptop/PC) without me noticing it directly.
  - [Q15r8] Malware can cause me no longer being able to view my data and having to pay the attackers money to release it.
  - [Q15r9] It is sufficient to look at the sender to check the security of emails before opening.
  - [Q15r10] My PC can get infected with malware by clicking on a link.
  - [Q15r11] I can click on attached files without concern for an email that is addressed to be directly.
  - [Q15r12] As long as a website looks official, I can enter my login data without concern.
  - [Q15r13] The email could be risky if the sender's name and email address are not the same.
  - [Q15r14] The text on a link shows me what site you will end up on if you click on it.
  - [Q15r15] As long as I know the sender of an email then I don't have to worry about the email containing viruses.
  - [Q15r16] Links in emails can lead to fake websites to gather my login data.
- Answers:
  - 5 fully agree [5]
  - 4 mainly agree [4]
  - 3 neutral [3]
  - 2 mainly disagree [2]
  - 1 fully disagree [1]

- I don't understand the statement [9999]

**[Q16] Next you will see some statements about digital security when surfing in private browsing mode (also called *incognito* mode). Please carefully read each statement and state how much you agree with the respective statement.**

- Subquestions
  - [Q16r1] The private browser mode encrypts my data.
  - [Q16r2] The private browser mode prevents my internet provider from seeing what websites I visit.
  - [Q16r3] The private browser mode protects me from other people using my device from being able to track my activities.
  - [Q16r4] The private browser mode prevents malware from reaching my device.
  - [Q16r5] The private browser mode has the same protective effect as an ad blocker, that is, advertising is blocked on a website.
  - [Q16r6] The private browser mode does not prevent website operators from being able to see my IP address.
- Answers:
  - 5 fully agree [5]
  - 4 mainly agree[4]
  - 3 neutral [3]
  - 2 mainly disagree [2]
  - 1 fully disagree [1]
  - I don't understand the statement [9999]

Next you will see a number of statements-relating to digital security. Please carefully read each statement and state how much you agree with the respective statement.

**[Q17] How important is it to you to prevent ...**

- Subquestions
  - [Q17r1] malware such as viruses or Trojans from reaching your devices (PC, laptop, smartphone)?
  - [Q17r2] your data (such as login data) from being spied on?
  - [Q17r3] you from no longer being able to view your data and having to pay blackmailers money to view your data?
  - [Q17r4] you from being insulted online (cyberbullying)?
  - [Q17r5] you from being a victim of fraud, for example, when shopping online?
  - [Q17r6] unauthorised persons from having access to your online accounts?
  - [Q17r7] unauthorised persons from gaining access to your personal data?
  - [Q17r8] your digital messages, such as emails, being accessed and read by third parties?
  - [Q17r9] you becoming a victim of cyberstalking?
  - [Q17r10] your passwords from being guessed by unauthorised persons?
  - [Q17r11] your devices (PC, laptop, smartphone) from being spied on?
  - [Q17r12] you from entering your login data on fraudulent websites?
  - [Q17r13] friends or family with access to your devices (PC, laptop, smartphone) being able to see your browser history?

- [Q17r14] advertisers from being able to see what websites you visit?
- [Q17r15] the contents of your messages from being read by communication service providers, e.g., the messenger service?
- Answers:
  - 5 very important [5]
  - 4 quite a bit important [4]
  - 3 moderately important [3]
  - 2 a little important [2]
  - 1 not important [1]
  - I don't understand the question [9999]

**[Q18A] For each of the following statements, please state how concerned you are.**

**How concerned are you...**

- Subquestions
  - [Q18r1] that when using messenger services your messages could also be read by unauthorised persons?
  - [Q18r2] that the messenger service provider has access to your message contents, such as sent texts or images?
  - [Q18r3] that other people could read your messages despite end-to-end encryption?
  - [Q18r4] that a website could use an illegal mechanism to collect personal information about you?
  - [Q18r5] that when using a public Wi-Fi other devices could see what data (e.g., passwords, credit card information) you enter on websites?
  - [Q18r6] that somebody could track you based on your location?
  - [Q18r7] that somebody could steal your passwords?
  - [Q18r8] that your biometric data could be abused, e.g., my fingerprint to unlock the mobile phone?
- Answers
  - 5 very concerned [5]
  - 4 quite a bit concerned [4]
  - 3 moderately concerned [3]
  - 2 a little concerned [2]
  - 1 not concerned [1]
  - I don't understand the question [9999]

**[Q18B] For each of the following statements, please state how concerned you are.**

**How concerned are you...**

- Subquestions
  - [Q18r9] that one of your passwords is easy to crack or guess?
  - [Q18r10] that sensitive data on your computer is not secure enough (e.g., through backups or firewalls)?
  - [Q18r11] that someone could get the password for your computer by watching you enter it?
  - [Q18r12] that, if your computer is stolen, unauthorised persons could have access to your sensitive data and passwords?

- [Q18r13] that your computer could be affected by malware, and you would no longer be able to open your files because of it?
- [Q18r14] that your computer could be affected by malware and is therefore no longer usable?
- [Q18r15] that your computer could be affected by malware and therefore unauthorised persons have access to your data?
- [Q18r16] that your computer could have a virus that you don't know about?
- [Q18r17] that unauthorised third parties could have access to your data?
- [Q18r18] that networked devices such as voice assistants (e.g., Alexa, Siri) inadvertently gather, store and forward personal data?
- [Q18r19] that voice assistants, such as Alexa or Siri, inadvertently listen to everything you say?
- Answers
  - 5 very concerned [5]
  - 4 quite a bit concerned [4]
  - 3 moderately concerned [3]
  - 2 a little concerned [2]
  - 1 not concerned [1]
  - I don't understand the question [9999]

**[Q19A] For each of the following statements, please state how much you agree.**

- Subquestions
  - [Q19r1] I am not rich or famous, so nobody is interested in accessing my personal data.
  - [Q19r2] I do not believe that anyone is interested in reading my messages (e.g. emails, chats).
  - [Q19r3] I have nothing to hide, therefore it is not important to me whether my messages are encrypted or not.
  - [Q19r4] I consciously use communication services (e.g., messenger services) that use end-to-end encryption, because I don't want unauthorised persons to be able to read my messages.
  - [Q19r5] I don't need strong passwords because my data is not interesting to attackers.
  - [Q19r6] People who use the private browser mode have something to hide.
  - [Q19r7] WLAN at home is more secure than public WLAN.
  - [Q19r8] Encryption is only for people who are paranoid.
- Answers:
  - 5 fully agree [5]
  - 4 mainly agree [4]
  - 3 neutral [3]
  - 2 mainly disagree [2]
  - 1 fully disagree [1]
  - I don't understand the statement [9999]

**[Q19B] For each of the following statements, please state how much you agree.**

- Subquestions
  - [Q19r9] Encryption has more advantages than disadvantages.
  - [Q19r10] Encryption is dangerous, because I can irretrievably lose my data.
  - [Q19r11] Encryption is bad because it is used by hackers and criminals, e.g., for illegal activities.
  - [Q19r12] Encryption is useful to ensure protection of personal data.
  - [Q19r13] Digital security is complicated.
  - [Q19r14] Products with a high level of security are often difficult to use.
  - [Q19r15] Secure programs or applications are often difficult to use.
  - [Q19r16] Programs and services should be secure. It is not my job to take care of security.
  - [Q19r17] Regardless of what I do, I am powerless against skilled attackers and hackers.
  - [Q19r18] I don't want to have to deal with digital security.
  - [Q19r19] Digital security is annoying.
- Answers:
  - 5 fully agree [5]
  - 4 mainly agree [4]
  - 3 neutral [3]
  - 2 mainly disagree [2]
  - 1 fully disagree [1]
  - I don't understand the statement [9999]

**[Q20] What measures do you use for your digital security? Please click on all the measures you use for your digital security.**

- Answers – unchecked [0] – checked [1]:
  - [Q20r1] None
  - [Q20r2] (Regular) updates of the operating system and other programs
  - [Q20r3] (Regular) backups on an external hard drive
  - [Q20r4] (Regular) backups to the cloud
  - [Q20r5] Anti-virus software
  - [Q20r6] Firewall
  - [Q20r7] Ad blocker
  - [Q20r8] Anti-tracking tools
  - [Q20r9] Password manager
  - [Q20r10] End-to-end encryption for messages
  - [Q20r11] PIN, password or biometric processes to lock and unlock your devices (laptop, smartphone, tablet)
  - [Q20r12] Two factor authentication
  - [Q20r13] Tor network
  - [Q20r14] VPN (virtual private network)

**[Q21] How important is it for you to protect the following data on the internet (e.g., from external access and theft)?**

- Subquestions
  - [Q21r1] Your full name
  - [Q21r2] Address (home address)

- [Q21r3] Your personal telephone numbers
- [Q21r4] Your contacts
- [Q21r5] Your personal photos
- [Q21r6] Message threads, for example, from chats and emails
- [Q21r7] Location and movements, e.g., GPS data, your jogging route
- [Q21r8] The amount of your salary or earnings
- [Q21r9] ID, such as identity card and driving licence
- [Q21r10] Insurance documents
- [Q21r11] Delivery notes and invoices
- [Q21r12] IBAN / BIC and account details
- [Q21r13] Health data
- [Q21r14] Biometric data, such as fingerprints
- [Q21r15] Passwords
  
- Answers:
  - 5 very important [5]
  - 4 quite a bit important [4]
  - 3 moderately important [3]
  - 2 a little important [2]
  - 1 not important [1]
  - I don't understand the question [9999]

**[Q22] How likely is it that the following groups of people pose a risk to your digital security (e.g. unauthorised access to your personal data, stalk you online or restrict your access to digital services)?**

- Subquestions
  - [Q22r1] Family members
  - [Q22r2] Friends and acquaintances
  - [Q22r3] Work colleagues
  - [Q22r4] Officials from [insert country name], such as police, secret services and the government
  - [Q22r5] Officials from other countries, such as police, secret services and the government
  - [Q22r6] Private sector companies
  - [Q22r7] Criminals who want to get rich from your data
  - [Q22r8] Hackers-who gain unauthorised access to data and devices, for fun
  
- Answers:
  - 5 Very likely [5]
  - 4 Quite a bit likely [4]
  - 3 moderatley likely [3]
  - 2 a little likely [2]
  - 1 Not likely [1]

**[Q25] Do you have practical experience in the informatics, computer technology or information technology fields (e.g. through your job or education background)?**

- Answers
  - Yes [1]
  - No [2]
  - I prefer not to answer this question [9999]

**[Q26] Do you have an immigration background?**

People with an immigration background are defined as people who were not born as a [insert nationality of country] citizen or who have at least one parent who was not born as a insert nationality of country] citizen.

- Answers
  - Yes, I have an immigration background [1]
  - No, I don't have an immigration background [2]
  - I prefer not to answer this question [9999]