Technical Report

UCAM-CL-TR-983
ISSN 1476-2986

Number 983

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

An evaluation of police interventions for cybercrime prevention

Maria Bada, Alice Hutchings,
Yanna Papadodimitraki, Richard Clayton

July 2023

15 JJ Thomson Avenue
Cambridge CB3 0FD
United Kingdom
phone +44 1223 763500

https://www.cl.cam.ac.uk/

Acknowledgements

We would like to thank Prof Benoît Dupont and Prof David Wall for their useful comments and suggestions on this technical report.

Technical reports published by the University of Cambridge Computer Laboratory are freely available via the Internet:

https://www.cl.cam.ac.uk/techreports/

ISSN 1476-2986

Contents

Executive summary

The UK's National Crime Agency (NCA) has been developing interventions to divert people who show signs of engaging in cybercrime and low-level Computer Misuse Act (CMA) 1990 offences from (further) offending. These interventions have been delivered with the assistance of the Regional Organised Crime Units (ROCUs), as well as local police, since at least 2014.

The interventions are part of the 'Prevent' objectives as set out in the Home Office's 2018 Serious and Organised Crime Strategy, and aim to stop people from being drawn into different types of serious and organised crime, and to develop techniques to deter people from continuing in serious and organised criminality [12].

Prevent interventions include 'cease and desist' letters, police visits, and workshops. 'Cease and desist' letters are considered a warning; they may be delivered as part of a police visit, by email, or by post. The letter requests that the individual stops a specified action, highlighting the risk of prosecution otherwise. The police visits discuss the suspected activities, relevant legislation, positive use of relevant skills, and other potential consequences such as the possibility of seizing equipment and/ or banning access to the internet. The police visits and 'cease and desist' letters are handled by ROCUs or local police forces.

The workshops are delivered by the NCA and ROCUs in collaboration with the private sector (e.g., cybersecurity industry, training providers). They are voluntary and young participants are required to be accompanied by a carer/guardian. The workshops aim to inform the participants and carers/guardians of the consequences of crime, promote positive behaviours and reduce the likelihood of (further) offending.

For our study, we used a cross-sectional survey to evaluate the effects of the workshops (intervention group) and compare to police visits and cease and desist letters (control group). The survey was conducted between February and March 2020; letters were sent to 182 recipients of an intervention (workshop, police visit, or cease and desist letter). The survey explored how participants perceive the police interventions, and included open and closed response questions on the interventions, their effects and consequences, cybercrime and its impact, awareness of the CMA, and technical skills.

The cybercrime interventions were associated with lower post-intervention self-reported offending. Those who attended workshops did not have significantly lower self-reported offending compared to those who did not attend after the intervention, the workshops do offer something different to the 'cease and desist' interventions (police visits and letters). Participants seem to value the opportunity to discuss their experience, receive information about developing technical skills lawfully, and about career opportunities with a participatory, informal approach. Regarding the perception of the likelihood of apprehension and the severity of punishment, they did not seem to have a deterrent effect on our group.

The results presented in this report are preliminary. Generalisation to a wider population is not possible due to certain limitations, mainly the use of a retrospective, cross-sectional survey which does not allow us to be sure of the real level of change as a result of the interventions; the small sample size; and the use of self-reported offending.

For this, we recommend the use of a randomised controlled trial (RCT) to measure the effects of cybercrime interventions. RCTs evaluate the effects of different interventions using random allocation between intervention and control groups (in this case workshops, and letters and police visits), to allow for causal inference. RCTs are a robust approach to examining intervention effects while controlling for bias and other factors. Moreover, the approach allows the respondents to conceal their activities, while providing useful data to the researchers. As research on cybercrime interventions is lacking (besides a few notable

exceptions), we recommend further exploration of the subject. Understanding cybercrime interventions and their impact on recipients is key in designing and implementing effective policies to tackle the increasing number of harmful online activities, especially at a time of fiscal constraints.

1 Overview of interventions

The UK's National Crime Agency (NCA) has been developing interventions to divert people who show signs of engaging in cybercrime and low-level Computer Misuse Act (CMA) 1990 offences from (further) offending. These interventions have been delivered with the assistance of the Regional Organised Crime Units (ROCUs), as well as local police, since at least 2014.

The interventions are part of the 'Prevent' objectives as set out in the Home Office's 2018 Serious and Organised Crime Strategy (note: this is different to the Prevent Duty, which relates to extremism and radicalisation). The critical objectives of 'Prevent' are to stop people from being drawn into different types of serious and organised crime, and the development of techniques to deter people from continuing in serious and organised criminality [12].

Prevent interventions include 'cease and desist' letters, police visits, and workshops. 'Cease and desist' letters are considered a warning; they may be delivered as part of a police visit, by email, or by post. The letter requests that the individual stops a specified action, highlighting the risk of prosecution otherwise. The police visits typically discuss the suspected activities, relevant legislation, positive use of relevant skills, and other potential consequences such as the possibility of seizing equipment and/ or banning access to the internet. The police visits and 'cease and desist' letters are handled by ROCUs or local police forces.

The workshops are delivered by the NCA and ROCUs in collaboration with the private sector (e.g., cybersecurity industry, training providers). They are voluntary and young participants are required to be accompanied by a carer/guardian. The workshops are full day events that aim to inform both the participants and carers/guardians of the consequences of crime, promote positive behaviours and reduce the likelihood of (further) offending. These interventions fall within [93] conceptualisation of secondary prevention, as they are targeted to those at risk of engaging in crime or escalating to more serious offending.

The number of cybercrime interventions has increased in recent years, along with international interest in the approach. Moreover, as far as central youth justice policymaking is concerned, there is an identified need to bridge the gap between research and practice [94] which is prominent in cybercrime. Therefore, understanding the impact of the interventions is vital for informing future policy and initiatives, and supporting transnational knowledge sharing.

We consider three specific types of intervention.

"Cease and desist" visits by police. These typically include a discussion on the suspected activities, the relevant legislation, and the positive use of skills. Additionally, they note the possibility of custodial sentences, and removal of Internet access and confiscation of computer equipment.

"Cease and desist" letters. These letters are mailed to the residential addresses of relevant individuals (e.g. those suspected of using tools in illegal activities or using illegal services relating to cybercrime). The letters request that the individual stop a specified action, highlighting the risk of prosecution. The letters may also be hand-delivered during a face to face visit by police where they serve to provide a permanent reminder of the verbal warnings that have been given. The cease and desist visits and letters are handled by ROCUs or by local police forces.

Workshops are full day events delivered by the NCA and ROCUs in collaboration with the private sector. They are attended by people deemed at risk of (further) offending and aim to inform about the consequences of crime, but also to promote positive behaviours. They involve a series of talks on relevant legislation, training, work opportunities, and practical advice. Young participants have to be accompanied by a carer/guardian, and there is specific material aimed at these attendees designed to further support the aims of the workshops.

1.1 Background

1.1.1 Law enforcement operations

In 2014, Operation DERMIC targeted purchasers of the Blackshades remote access tool (RAT) which allowed taking control of a computer. This was followed by Operation VIVARIUM in 2015. This operation dealt with customers of the Lizard Stresser online booter service, which provided denial of service attacks (DoS) (attacks making a service/ network inaccessible by overloading the systems). Both operations led to several arrests, mainly of young people, many of whom reportedly were drawn in through curiosity without realising their activities could be illegal [20]. Operation DERMIC included a follow-up 'cease and desist' activity of 80 police visits and a substantial number of emails and letters to known buyers of Blackshades [35]. Operation VIVARIUM also involved 28 police visits to customers of the service, whose average age was 19 [21].

The most recent large-scale operations were Operation VIRUS (December 2018 to June 2019) and Operation PowerOFF, which began in April 2018 and targeted customers of the booter services website WebStresser [8]. The operations were followed by 'cease and desist' letters, police visits and workshops.

1.1.2 Recipients of cybercrime interventions

Actors involved in cybercrime span from young people with limited technical skills to experts employed by organised criminal groups, depending on the offence. While the cybercrime interventions do not specifically target young offenders, they are the most common recipients [20] with an average age of 17 [21]. They are predominantly male, and they tend to be involved in low-level offences, purchasing the use of tools and/or services for activities such as DoS attacks and remote access [21]. They tend to get introduced to cybercrime though online gaming and fora [20] [13], however their motivations vary. Most of the intervention recipients are involved out of curiosity, desire to prove themselves or to complete a challenge; financial gain is not a priority nor is it a goal [36] [10] [13] [16] [21].

2 Desisting from and deterring cybercrime

Desistance is seen as an ongoing process rather than an event that happens at a single point in time [38]. Factors that support desistance include aging, identity transformation, having a stable close environment, employment, education [39], and hope [40]. Research on the subject tends to focus on street crime, where offender careers tend to start in adolescence [41]. This is the stage that risk taking behaviours peak compared to other age groups [42]. Young offenders link their offending behaviour to lack of maturity and understanding of the consequences [43]. It is possible that some young people unwittingly commit low-level offences as they are not aware of ethical and legal boundaries. So far, there is no agreement on the possibility of achieving or commencing desistance during this stage [44] [45]. However, it has been established that -in general- crime declines as we age [46] [47].

Adding to desistance literature, deterrence research points to factors that seem to have a deterrent effect in terms of crime such as increased risk of apprehension and certainty of punishment [48] [49] [50], and police presence and targeted policing [51]. Moreover, perceptions relating to sanction risk seem to have a deterrent effect too [52]. On the other hand, evidence suggests that factors such as imprisonment, increased length of sentence, and severity of punishment do not have a deterrent effect but may have a criminogenic effect instead [48] [53] [54]. The same applies to intervention programmes aiming to deter through exposure to harsh conditions such as shock incarceration [55] and boot camps [56]. On the contrary, programmes based on Therapeutic Communities and Restorative Justice principles have shown better outcomes [58] [57], and their effectiveness could be increased with a degree on individualisation [59]. Finally, perceptions of police legitimacy are equally important to influencing compliance with the law [60]. According to Tyler [61], compliance is conditioned by an individual's perceptions of fairness and legitimacy; failing to satisfy the individual's expectations can trigger feelings of injustice and attempts to restore justice [62].

When it comes to cybercrime, research findings mirror existing literature. Offenders may not realise their online activities can have real consequences for real people [17] [63]. Such situations can occur while playing online games, retaliating during bullying incidents, or pulling pranks against their peers [10] [16]. Studies have shown that even university students are confused about cybercrime legislation; there is an evident normalization of risky or harmful online behaviour as well as a variety of misconceptions about cybercrime [64]. Additionally, young people perceive cybercrime to be less serious when compared to other crimes [17] and believe the likelihood of getting caught or sentenced is low [22].

Additionally, Hutchings [14] found that online offenders perceive the likelihood of detection as low. Kirwan and Power [66] and Young et al. [67] suggest that online offenders believe there is a low chance of punishment, but high returns which can lead to perceptions of potential gains outweighing the associated risks. Adding to this, is the perception that traditional deterrents will have even more limited effects on cybercrime due to anonymity, and attribution and evidence collection difficulties [68]. Lastly, the increasing workload, and the lack of capacity in expertise and manpower of law enforcement is proving to be another hindrance in dealing with cybercrime [64] [65]; it adds to the perceptions around the low likelihood of apprehension and certainty of punishment.

3 The evidence base for cybercrime prevention initiatives

Many evaluation studies looking at long-term effects of interventions have focused on prevention in early or middle childhood [69], and on serious and chronic offenders [70]. Research has shown that offline crime prevention programmes can potentially lead to an increase in crime in the longer term [71] [72]. A number of factors are theorised to increase the likelihood of future offending such as defiance, depending on the strength of the social bonds and perceptions of fairness [73]; enticement caused by the 'forbidden fruit effect' [74]; displacement, with crime moving to other locations, times, targets, methods, perpetrators, or offences [76]; adaptation of tools to commit crime [74]; creating a 'badge of honour effect', enhancing the criminal status of individuals [77]; net-widening, by including more individuals into prevention programmes [4]; and labelling and stigmatisation due to increased contact with the criminal justice system [78].

Despite these factors referring to offline crime, still they are of importance to cybercrime. Motivations such as curiosity and innovation [79] [80], ego [75] [81], and peer recognition [16] [81] are prevalent both in cybersecurity and cybercrime communities. Also, not having face-to-face interactions with victims may also play a role in offending. The online disinhibition effect refers to a diminished internal censorship when communicating in cyberspace, where people hide their real identity and act in a manner they would not offline [82]. So, individuals with greater technical expertise, may directly and indirectly increase their ability to engage in cybercrime [1] [83] [10].

Antisocial peer group interactions is a strong predictor of cybercrime [84] [85] as well; social networks or online forums can provide offenders with the knowledge or social contacts to commit cybercrime [13]. For example, online gaming environments can increase opportunities and motivation for cybercrime [10] [21] [86] with a typical example being the use of unauthorised access to gaming accounts to steal virtual objects or credits [87]. In such cases it could be difficult to develop effective deterrence messaging even if the likelihood of apprehension is high due to the strong influence of the peer group.

Regarding crime prevention initiatives on cybercrime, Brewer et al. [4] reviewed a range finding there is not much evidence to support their application in this field. They suggest that those engaged in cybercrime may differ from those involved in other forms of criminality, and the criminogenic factors may play a role in the effectiveness of deterrence mechanisms. Campaigns that promote positive behaviours or attitudes, may have some success if they are deployed at the early stages of offending [4]; however, the views of the public and the offenders on legitimacy and procedural justice are equally important when considering what countermeasures are appropriate [88] with respect to cybercrime. On the other hand, Lee and Holt [89] suggest integrating cybercrime diversion practices and material into existing intervention programmes rather than designing bespoke interventions; their study points to a degree of behavioural overlap between offline offending and cybercrime in young people.

4 Research questions and hypotheses

The NCA's approach to cybercrime interventions has attracted international attention and has been adopted by other jurisdictions. However, evaluations of these interventions remain scarce, especially regarding the views of the recipients. Understanding the impact of the interventions is key in informing future policies and initiatives, and supporting transnational knowledge sharing. For this, our research questions explore the perceptions and attitudes of the recipients of the interventions, namely:

- Do those who attend a workshop have lower levels of re-offending thereafter, compared to those who did not attend?
- What are the reactions of the participants and their families to the interventions?
- How and why do the participants become involved in harmful online behaviours?
- How do the participants perceive the lawfulness of these activities?
- What are the participants' perceptions of the likelihood of detection and the seriousness of punishments?
- Are the police perceived to be legitimate by participants?

Our hypotheses are:

H_1 There will be significantly lower self-reported involvement in each harmful online activity after the interventions, compared to before the interventions.

H_2 There will be a significantly lower overall rate of involvement in harmful online activities after the interventions, compared to before the interventions.

H_3 Those in the intervention group will have significantly higher levels of self-reported overall pre-intervention involvement in harmful online activities, compared to the control group.

H_4 The intervention group will have significantly lower levels of self-reported overall rate of involvement in harmful online activities post-intervention, compared to the control group.

H_5 Those who perceive the likelihood of detection as higher will have significantly lower levels of post-intervention self-reported offending.

H_6 The intervention group will perceive the likelihood of detection as significantly higher than the control group.

H_7 Those who perceive the severity of consequences as higher will have significantly lower levels of post-intervention self-reported offending.

H_8 The intervention group will perceive the severity of consequences as significantly higher than the control group.

H_9 Those who have higher perceptions of police legitimacy and procedural justice will have significantly lower levels of post-intervention self-reported offending.

H_{10} The intervention group will perceive police legitimacy and procedural justice as significantly higher than the control group.

H_1 and H_2 test the relationship between the level of self-reported involvement in the harmful online activities before and after the interventions. This is explored for each type of activity, as well as overall. H_3 is included as those delivering and designing the interventions informed us that invitations to participate in the workshops are issued based on the police officers' views about the perceived seriousness of offending. H_4 tests the relationship between the intervention and control groups, and post-intervention self-reported offending. H_5, H_7, and H_9 test the relationship between post-intervention self-reported offending and perceptions of the likelihood of detection, severity of consequences, and police legitimacy and procedural justice, respectively. H_6, H_8, and H_{10} test the same independent variables against the type of intervention received.

5 Methodology

We used a cross-sectional survey to evaluate the effects of the workshops (intervention group) and compare to police visits and cease and desist letters (control group), between March 2018 and January 2020. Our aim was to provide an exploratory evaluation of the effectiveness of these interventions, to inform comprehensive evaluations and help refine policies and initiatives in the future.

5.1 Recruiting

The survey was conducted between February and March 2020. For data protection and privacy reasons, it was not possible for the researchers to directly contact the intervention recipients. For this reason, the NCA facilitated recruitment by forwarding invite letters on university letterhead (at least one letter was subsequently returned to sender (NCA)). Letters were sent to 182 participants who had received an intervention (workshop, police visit, or cease and desist letter) between March 2018 and January 2020. These included:

- 81 people who received interventions as part of Operation VIRUS between 4 December 2018 and 28 June 2019;
- 56 people who received interventions as part of Operation PowerOFF between 11 October 2019 and 31 January 2020[1];
- 13 people from interventions organised by ROCUs for other reasons between 25 January 2019 and 15 October 2019;
- 32 people who attended workshops organised by the NCA between 24 March 2018 and 8 June 2019.

The recipients were invited to complete an online survey about the intervention(s) they participated in, giving them the opportunity to anonymously self-report any (further) offending. The letters included the names of the researchers, information about the research and its independent nature, confidentiality and anonymity, a unique URL for the online survey (with the possibility to access it over Tor anonymity network), and a foam pop-out 'puzzle cube' as an incentive. The letter mentioned that individual responses would not be provided to other parties (incl. the police), and there will be no attempts to link responses to individuals. Unique URLs were used as a precaution to identify if more than one person has completed the survey (for example, if the URL has been posted on an online forum (see [15]).

5.2 Survey design

To construct the survey, we followed a multi-phase process. First, we developed an initial draft based on the relevant literature and previous work. After testing the survey amongst members of the Cambridge Cybercrime Centre, it was shared with the NCA and UK Home Office who provided further comments.

The survey first sought confirmation of the intervention, and its type (police visit, letter and/or workshop). This was included as some recipients may have not been aware they received a cease and desist letter, or they may have refused to engage with the police during the visit. If they were unaware of the letter intervention, they were redirected to a page with our contact details in case they wanted further information. They were

[1] Operations VIRUS and PowerOFF both targeted customers of the booter services website WebStresser [8]

still invited to complete the survey, but not presented with the questions relating to the intervention.

The survey included open and closed response questions on the intervention, its effects, and perceptions on policing and cybercrime (for a copy of the online survey, please see the end of this report). Broadly, the survey asked the participants about:

- self-rated technical skills;
- how they became involved in the alleged harmful online behaviours, and how long ago this was;
- their perceptions of the interventions; if their carers/guardians were aware of the intervention, and if so, their response;
- if they had committed any (subsequent) offences after receiving the intervention, and if so the frequency and nature, and if this has increased or decreased since the intervention;
- if they no longer commit offences, why they stopped, their perception of being caught, their perceptions of the potential illegality of the harmful online activities;
- their perceptions of the police they interacted with; their perceptions of police legitimacy and procedural justice;
- demographic information (e.g., age group, gender, education level, employment status, and relationship status).

Throughout the survey, the activities of interest were referred to as 'harmful online activities'. Where we asked participants about these individually, the response options provided were:

1. Making online services unavailable (e.g. booting, denial-of-service attacks)
2. Tricking people into providing their username and password
3. Gaining access to protected computer systems
4. Gaining access to secure websites
5. Use of stolen credit cards (e.g. carding)
6. Trading in fake/stolen online accounts
7. Game cheating (e.g. modding)
8. Trolling/sending abusive messages
9. Controlling a botnet
10. Extracting data (e.g. SQL injection attacks)
11. Intercepting communications (e.g. Eavesdropping attacks)
12. Possession of malicious software (e.g. RATs)
13. Use/Distribution of malicious software
14. Other

The first questions asked about the type of intervention received, the number of times the participants received each intervention, and the timeframes. The options provided were:

1. Workshop
2. Police visit and cease and desist letter
3. Police visit without cease and desist letter
4. A cease and desist letter delivered by other means

5. Other

Respondents were asked to self-report what they believed were the main purposes of the intervention(s) received from the police (open ended question), and whether it was delivered to the right person. In addition to this measurement, a question was added 'Which, if any, of the following do you think caused the police to contact you for an intervention?', with the 14 harmful online activities provided as response options.

The conduct and the purpose of the police visit and the workshop were assessed by two questions, 'Which of the following occurred during the police visit (please select all that apply)?' and 'Which of the following occurred during the workshop (please select all that apply)?'. These items included eight possible responses:

1. A warning about my past behaviour
2. Questions about my past behaviour
3. An explanation of the illegality of some online activities
4. Discussion of the impact of cybercrime on its victims
5. Advice about opportunities to develop my skills
6. Advice about how to use my skills legally
7. Advice about career opportunities
8. Advice about how to stay safe online
9. Other

The participants' feelings after receiving a cease and desist letter from the police or during the initial visit from the police, as well as during the workshop were assessed by three questions: "How did you feel after the initial visit from the police?", "How did you feel after receiving a cease and desist letter from the police?", "How did you feel after attending a workshop?". The items were based on previous work [37]. The participants could choose from seven possible answers, measured on a Likert scale from 1= Not at all to 5= Very much:

1. Angry
2. Afraid
3. Surprised
4. Upset
5. Calm
6. Disappointed
7. Sad

The initial involvement in criminal activity was measured by two main questions: "How did you first become involved in the alleged harmful online activity?" and "Why did you engage in the harmful online activity?". The following categories were created to measure "How":

1. Through people I met playing online games
2. Through people I met on online communities/forums
3. Through family members
4. Through friends I met online
5. Through friends I met offline
6. Through school

7. Through my own research
8. Other

In order to assess the “Why” the following categories were used:

1. A way to improve my skills
2. A sense of belonging through hacking forums and online communities
3. A desire to prove myself to others
4. Financial gain
5. Political motivation
6. It was an interesting challenge
7. For fun
8. For revenge
9. Other

These survey items (both questions) were based on previous literature which finds that the majority of those engaged in, or on the periphery of cybercrime, become involved via an interest in computer gaming, but also a sense of belonging through hacking forums and online communities; a desire to prove oneself to the group; a desire to improve one’s skills or solve the difficult problems; and, lastly, financial gain [10] [13] [14] [21] [16].

The time frame since the participants were first involved in the alleged criminal activity was assessed using a Likert scale 1= Less than a year to 5= More than six years. A “Don’t know/Not sure” option was also provided.

The responses of parents/guardians were explored with two questions. First question was “Were your parents/guardians aware of the intervention? (e.g. letter, police visit, workshop)” with a two-item scale Yes/No. The second was “If so, what was their response?”, with response options:

1. They were surprised
2. They were supportive
3. They were calm
4. They were disappointed
5. They were upset
6. They were angry
7. Other

The items for these questions were based on previous research [9] [28] [24] [5].

When examining the effects in terms of delinquent behaviour we distinguish between involvement in, and the frequency and seriousness of delinquent acts. We measure not only if offenders ceased offending altogether, but if they reduced their offending across a variety of crime types. These specific measures of criminal offending contribute to a more detailed view on program effectiveness [32]. For survey development, we built upon the previous work on self-reported delinquency [32] [7] [29].

The type and frequency of the offence committed was assessed before as well as after the intervention. Seven questions were asked. The questions “Before the intervention on average, how often did you engage in the following?” and “Since you received the intervention, on average how often have you engaged in the following?” provided the 14 harmful online activities (incl. “Other”) as response options. They were measured on a Likert scale from 1= Never at all to 5= Monthly.

The participant's opinion about the illegality of their activities before the intervention was measured by "Before the intervention, which of the following activities did you think could be illegal?". The 14 harmful online activities were provided as response options, measured on a Likert scale from 1= Always illegal to 4= Not sure.

Questions were included to assess the opinion of participants on the likelihood of being detected by police if they were involved in the 14 harmful online activities, and the severity of the consequences. The question "Since you received the intervention, how likely do you think you would be detected by police, if you were involved in the following activities?" included the 14 harmful online activities, each measured on a Likert scale from 1= Very unlikely to 5= Not sure. The question "If you were caught being involved in the following activities, how severe do you think the consequences would be?" was measured for each harmful online activity on a Likert scale from 1= Very light to 4= Not sure.

The participant's perception of their anonymity online and also the likelihood of being caught was measured using four questions. The question "How much, if at all, did the intervention(s) change your perception of your anonymity online?" was measured on a Likert scale from 1= Not at all to 4= Extremely. The question "Why has your perception of being caught, if involved in harmful online activities, and/or of your online anonymity changed?" was open ended. Finally, the question "If you have stopped or reduced your involvement in harmful online activities, why?" was open ended, and "If you have stopped or reduced your involvement in harmful online activities, approximately how long ago was this?" was closed ended.

The effectiveness of the workshop was assessed also by asking participants about their engagement with the companies present or resources offered during the day using the question "Since the intervention, have you engaged further with any companies present or the resources offered at the workshop?". Potential options were:

1. Capture the Flags
2. Internships
3. Apprenticeships
4. Full time job
5. Other

In order to assess the awareness of the illicit nature of activities, we explored aspects such as awareness of the CMA 1990, awareness of legal and ethical ways to use IT skills, and the impact of cybercrime on victims before and after the intervention. The questions "Before the intervention(s), how aware were you of the Computer Misuse Act?", "Before the intervention(s), how aware were you of the impact of cybercrime on victims?" and "Before the intervention(s), how aware were you of legal and ethical ways to use IT skills?" were measured on a Likert scale from 1= Not at all aware to 4= Very aware.

Post-intervention, the questions "After the intervention(s), how aware were you of the Computer Misuse Act?" and "After receiving the intervention(s) how aware were you of the impact of cybercrime on victims?" were used. These included three possible answers:

1. After attending a workshop (if applicable)
2. After the initial police cease and desist visit (if applicable)
3. After receiving the cease and desist letter (if received without a visit)

They were measured using a Likert scale from 1= Not at all aware to 4= Very aware. For these questions we reviewed previous work on attitudes regarding crime and cybercrime [17] [22]).

In addition, participants were asked: “When the police visited did you expect to be arrested?” with a closed Yes/No answer. A similar question has been used in previous research regarding offline crime [34].

Participants’ perceptions of the police in general as well as perception of the police after the actual intervention, was assessed using a number of questions. First, participants were asked about their perception of the police based on the intervention they received. The question “We are now going to ask you about your perception of the police and how you felt about the intervention” included four possible answers:

1. I felt I was listened to during the intervention
2. I was satisfied with the way the police officer/s conducted the intervention
3. I was satisfied with how I was treated
4. Felt I was able to tell my side of the story

We measured this with a two-item scale Yes/No. These items were adapted from previous work [25] [19]. “When you were visited by police ...” included four options:

1. How knowledgeable did you find the police officer/s?
2. How legitimate did you find the police officer/s?
3. How friendly did you find the police officer/s?
4. How trustful/honest did you find the police officer/s?

They were measured on a Likert scale from 1= Not at all to 5= Extremely. These items were adapted from previous research [18] [25] [23] [26] [27] [30].

The remaining questions explored participants’ perceptions of the police more broadly. The question, “On the whole, how good a job do you think the police are doing in ...” included five items:

1. Solving crime
2. Solving cybercrime
3. Dealing with problems that concern you
4. Working with your community to solve local problems
5. Preventing crime

The questions were measured using a Likert scale from 1= Very poor job to 5= Very good job. They were adapted from previous work [19] [6] [18].

Obedience to police and law was measured using the question “How much do you agree/disagree with the following statements?”; it included three items:

1. I feel a moral obligation to obey the law
2. I feel a moral obligation to obey police
3. Overall, I obey police with good will

They were measured by a Likert scale from 1= Strongly disagree to 5= Strongly agree and were adopted from previous work [19].

Trust and compliance to police was measured using the question “How likely would you be to ...” which included four items:

1. Call police to report a crime

2. Help police to find someone suspected of committing a crime by providing them with information
3. Report dangerous or suspicious activities to police
4. Willingly assist police if asked

These were measured by a Likert scale from 1= Very unlikely to 5= Extremely likely, and were adopted from previous work [19].

The technical skills of participants were assessed using the question "How would you rate your technical skills?" using four possible answers (with examples of what each level of skills means):

1. Basic (e.g. I don't use computers or smart devices unless I absolutely have to)
2. Below proficient (e.g. I can use Internet, common software, but cannot fix computer problems)
3. Proficient (e.g. I know some computer programming languages and can fix most computer problems)
4. Advanced (e.g. I am proficient in multiple programming languages, and can create my own apps)

This question was adopted from previous research [15]. Other studies have also been reviewed which aimed to understand basic technical competency among college student populations [1] [11].

Information about the demographics of participants were collected using closed ended questions about:

1. Age
2. Gender
3. Relationship status
4. Employment status
5. Level of education

5.3 Ethical considerations

During the study we encountered a number of ethical issues which we tried to consider and address throughout the lifecycle of the evaluation (from the design to the analysis and dissemination of results).

Key concerns for the study related to participants' confidentiality and vulnerable status. We addressed these by following established research practice and current legislation in relation to data collection and storage, and safeguarding (e.g., removing identifying information, advise participants, especially if under 16, to discuss the letter with their guardians/parents before participating). We ensured the participants were aware of their rights regarding participation in research as well as the research team's duties and legal requirements (e.g., disclosure of information pertaining to terrorism). We did not match responses to individuals, and did not collect personal information.

The use of unique URLs for each invited respondent was effective in identifying where non-invitees had responded to the survey and this justified our decision to make use of trackable URLs. We did not use the unique URLs for any other tracking. Our design meant we could not associate URLs with recipients; therefore, we could not crosscheck the accuracy of responses about which interventions had been received by each recipient.

The data collected was stored on encrypted drives, and any potentially identifying information were removed. Those claiming the final incentive of a t-shirt offered at the end of the survey, needed to provide a name and address. These were retained solely for the purpose of sending the package, and were deleted after one month when successful delivery could be assumed.

The research project adheres to established ethical frameworks (University of Cambridge School of Technology, British Society of Criminology, British Sociological Association) and was granted approval by the Ethics Committee of the Department of Computer Science and Technology. The University of Cambridge is registered with the Information Commissioner's Office who implement the Data Protection Act 2018. All personal data collected were processed in accordance with the provisions of the Data Protection Act 2018.

5.3.1 Incentives

The survey design involved two incentives: a foam pop-out puzzle cube (see Figure 1) which was sent with the invitation to participate, and a t-shirt (Figure 2) which was sent after participation. Ten of the 12 sides of the cube (printed double-sided) were printed with a number. Completing the puzzle provided a distinct set of characters which in sequence formed a code. An additional code was provided at the end of the survey. Together, these codes could then be entered at a website to claim the t-shirt. As the survey was not forced-response, recipients were not required to complete the survey in order to obtain the code and claim the final incentive.

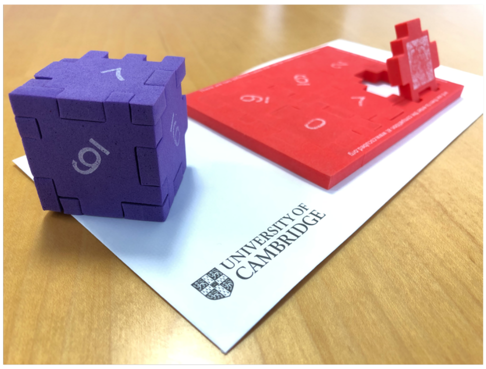


Figure 1: Foam pop-out puzzle cubes

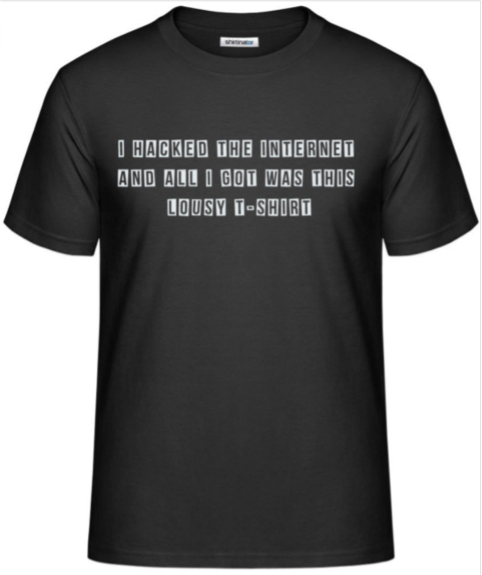


Figure 2: Example t-shirt

6 Results

Overall, there were 31 survey responses, with 23 unique participants, representing a 12.7% response (we removed additional responses from two survey URLs which had been shared and one non-completion). Four participants were from Operation PowerOFF, eight from Operation VIRUS, five from local and regional cease and desist referrals, and the remaining six from the workshop group. The response rates for each group were 7.14%, 9.88%, 38.4%, and 18.75%, respectively, with those who received interventions following targeted operations being least likely to respond.

6.1 Demographics

Most participants were in adolescence (12-17 years old) or early adulthood (18-24 years old) at the time of the survey, male (82.6%), single (47.8%), with a secondary education (52.2%), and rated themselves as having proficient technical skills (65.2%). Also, most participants were employed (26.1%) or studying (21.7%) (Table 1).

Table 1: Self-reported demographics

Demographic	Category	N	%
Age group (years)	12-17	8	34.8
	18-24	7	30.4
	25-34	5	21.7
	45-54	1	4.3
	Did not answer	2	8.7
Gender	Male	19	82.6
	Female	0	0.0
	Other	2	8.7
	Did not answer	2	8.7
Relationship status	Single	11	47.8
	In a relationship	7	30.4
	Engaged	1	4.3
	Married	1	4.3
	Did not answer	3	13.0
Employment status	Employed full-time	6	26.1
	Employed part-time	3	13.0
	Unemployed (currently looking for work)	0	0.0
	Student	5	21.7
	Self-employed	3	13.0
	Unable to work	4	17.3
	Retired	0	0.0
	Did not answer	2	8.7
Technical skills	Below proficient (e.g. I can use Internet, common software, but cannot fix computer problems)	1	4.3
	Proficient (e.g. I know some computer programming languages and can fix most computer problems)	15	65.2
	Advanced (e.g. I am proficient in multiple programming languages, and can create my own apps)	6	26.1
	Did not answer	1	4.3
Highest degree or level of education completed	Secondary education	12	52.2
	A Levels	4	17.4
	Trade/technical/vocational training	1	4.3
	Bachelor's degree	2	8.7
	Other	1	4.3
	Did not answer	3	13.0

6.2 Intervention

All participants indicated they had received at least one intervention. Twelve participants reported receiving a single intervention, namely a police visit with cease and desist letter (N=8), police visit without a cease and desist letter (N=2), or a workshop (N=2). Only one participant who reported multiple interventions had not participated in a workshop; they received a police visit with a cease and desist letter and a police visit without a letter. The remaining participants had all attended at least one workshop as well as at least one police visit. In total, 12 participants had attended at least one workshop, 15 participants had received a police visit with a cease and desist letter, eight participants had received one or more visits from police without a cease and desist letter, and only one participant received a cease and desist letter delivered by other means (Figure 3).

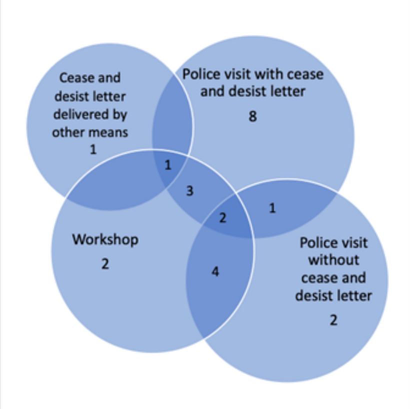

Cease and desist letter delivered by other means
1
Police visit with cease and desist letter
8
1
3
2
1
Workshop
2
4
Police visit without cease and desist letter
2

Figure 3: Participation in interventions

The earliest contact was April 2016, and the most recent was January 2020. To estimate the time elapsed between receiving the first intervention and completing the survey, the date of the intervention was set as the 15^{th} of the month. The median time elapsed was 390.5 days (M=465.3, range=41-1,411, SD=319.3). When asked how long ago they became involved in the alleged harmful online activity, two participants selected less than one year (8.7%), five selected one to two years (21.7%), three selected three to four years (13%), and four selected five to six years (17.4%). Four had become involved more than six years ago (17.4%), four did not know or were not sure (17.4%), and one participant did not answer (4.3%). One participant did not record the month and year they had first had contact with the police.

Participants were asked what they believed the main purpose of the interventions were. It appears that there were differing interpretations of the question. The main reason given was to prevent crime/re-offending (N= 11, e.g. 'to stop certain actions'; 'to stop my activity'). Some participants replied by naming the type of crime they had been involved in (N=4, e.g. 'DDOS Attacking'. 'Cybercrime ip [sic] flooding'). Two participants provided cynical responses ('Scare mongering', 'To check a box on a form'). Two participants referred to police responding to reports (e.g. 'Report from University Staff'). Interest in cyber skills was mentioned by two further participants (e.g. '... I believe that they were there because they were interested in my Cyber Skills'). Only one participant believed the police were there specifically in an investigative capacity ('To gather information on prior events'). The last participant was unsure ('dunno [sic]').

Participants were asked if they believed the intervention had been delivered to the right person. All but one participant answered yes. The participant stated:

> *They identified my link with the investigation but failed to realise my career in IT will require the use of tools which might otherwise be used maliciously.*

Participants were asked what behaviours they believe had caused the police to contact them for an intervention. Most participants provided just one behaviour, while one indicated 13 (the maximum possible) (M=1.0, SD=2.6). The most commonly reported behaviour was making online services unavailable (e.g. booting, denial-of-service attacks) (N=12), followed by gaining access to protected computer systems (N=10). Possession of malicious software (e.g., RATs) was reported by six participants, five reported controlling a botnet. Tricking people into providing their username and password, trolling/sending abusive messages, extracting data (e.g., SQL injection attacks), and use/distribution of malicious software were each reported by two participants. The other activities that were reported by only one participant (who had selected all available responses) were: gaining access to secure websites; use of stolen credit cards (e.g., carding); trading in fake/stolen online accounts; game cheating (e.g. modding); and intercepting communications (e.g., eavesdropping attacks).

Table 2 outlines what participants reported had occurred during police visits (N=23) and workshops (N=11). Participants selected a median of 6.0 responses from the options provided for the police visits (SD=2.5), and 5.5 responses from the options provided for workshops (SD=3.0). This table demonstrates that the focus of the police visits and workshops are quite different, with the former being more about providing warnings, and asking questions. In contrast, the workshops are more about noting the harmful outcomes of cybercrime, and the providing advice on how to develop relevant skills, their lawful use, and potential career options.

Table 2: What took place during police visits and workshops

	Police visit (N=23)		Workshop (N=11)	
	N	%	N	%
A warning about my past behaviour	18	78.3	6	54.5
Questions about my past behaviour	20	87.0	6	54.5
An explanation of the illegality of some online activities	18	78.3	9	81.8
Discussion of the impact of cybercrime on its victims	16	69.6	9	81.8
Advice about opportunities to develop my skills	13	56.5	7	63.6
Advice about how to use my skills legally	13	56.5	8	72.7
Advice about career opportunities	13	56.5	8	72.7
Advice about how to stay safe online	7	30.4	7	63.6

Participants were asked what they believed were the purposes of the cease and desist warning letters. Responses were mainly categorised as preventative (e.g., 'To prevent the activity from continuing') and to provide a warning (e.g., 'To let me know my activities might be a breach of the computer misuse act and to inform me that I should not repeat those activities or I could face prosecution'). One participant again took a cynical approach ('Scare tactics innit [sic]').

To sum up, the majority of the respondents received a police visit with a cease and desist letter; the median time between the first intervention and the survey was approx. 13 months. The main reason reported for the intervention was to prevent re-offending with the majority of respondents reporting making online services unavailable as the reason for the police contact. Finally, the respondents thought of the workshops as guidance sessions primarily.

6.3 Response to intervention

Table 3 shows how participants felt about receiving each intervention; participants were able to elaborate on their replies through the provided text box. For the 'cease and desist' letter, participants reported mainly feeling calm, surprised and disappointed and less likely to feel sad, upset or afraid. One participant provided an additional response of 'indifferent'. For the police visits, the most commonly reported response was surprised, calm and disappointed; and the least reported was sad, upset and angry. with three opting to do so. Additional responses provided were ‘irritated’, ‘disappointed in my behaviour’, and ‘I felt like an idiot’. Workshops’ participants were most likely to report feeling calm, surprised and afraid, and least likely to report feeling upset, sad and angry. Out of the three interventions, the workshop was least likely to provoke feelings of upset and sadness (most likely to be caused by police visit); the police visit was most likely to make participants feel surprised and disappointed (least likely to be caused by the workshop), and the ‘cease and desist’ letter was most likely to make participants feel calm (with all interventions scoring high).

Of the 23 participants, 18 (78.3%) indicated their carers/guardians were aware of the intervention. These participants were asked about their responses, with the most common being ‘they were supportive’ (N=12). Eleven participants advised their carers/guardians were surprised, and ten advised they were calm. ‘Disappointed’ and ‘upset’ were selected by five participants. Four participants advised their carers/guardians had been ‘angry’.

Table 3: How participants felt about receiving each intervention

	Police visit (N=23)					Cease and desist letter (N=17)					Workshop (N=12)				
	Mean	Median	SD	Min	Max	Mean	Median	SD	Min	Max	Mean	Median	SD	Min	Max
Angry	1.4	1.0	0.9	1	4	1.7	1.0	1.3	1	5	1.1	1.0	0.3	1	2
Afraid	2.1	1.0	1.6	1	5	1.5	1.0	0.7	1	3	1.7	1.0	1.2	1	5
Surprised	3.3	3.0	1.5	1	5	2.4	2.0	1.5	1	5	2.3	2.0	1.4	1	5
Upset	1.7	1.0	1.3	1	5	1.5	1.0	1.2	1	5	1.4	1.0	0.7	1	3
Calm	2.8	3.0	1.2	1	5	2.9	3.0	1.4	1	5	2.8	3.0	1.5	1	5
Disappointed	2.3	2.0	1.5	1	5	1.9	1.0	1.6	1	5	1.5	1.0	1.2	1	5
Sad	1.9	1.0	1.6	1	5	1.4	1.0	1.1	1	5	1.2	1.0	0.4	1	2

In summary, the workshop was least likely to provoke feelings of upset and sadness out of the three interventions, and most likely to provoke feelings of calmness, surprise and fear. The carers/guardians of the participants seem to have been supportive, although surprised, with the participation in the intervention.

6.4 Involvement in harmful online activity

When asked how they first became involved in the alleged harmful online activity, participants selected between one and six of the response options provided (M=2.0, SD=1.5). The most commonly reported mechanism was through their own research (N=16). Ten participants became involved through friends they met playing online games. ‘Through people I met on online communities/forums’ and ‘through friends I met online’ were both selected by nine participants. Through school was reported by three participants. Through family members and friends met offline were only reported by one participant.

Two participants declined to answer why they engaged in the harmful online activity. The remaining participants selected between one and six reasons (M=2.0, SD=1.7). The most commonly reported reason was for fun (N=13), followed by ‘it was an interesting challenge’ (N=12). Ten participants reported it was a way to improve their skills, while eight said it was due to a desire to prove themselves to others. Five participants reported revenge, while three said it provided a sense of belonging in hacking forums and online communities. Only two participants sought financial gain, and none were motivated politically. Three participants provided free-text responses, namely: ‘My behaviour was caused by anxiety/stress’; ‘Peer-pressure from users online’; and ‘Mainly because I felt worthless and depressed and lonely’.

Concluding, the majority of participants became involved in the alleged harmful online activity through their own research, mainly for fun but also for a challenge.

6.5 Pre- and post-intervention self reported offending behaviours

Of the 20 participants who self-reported their involvement in the harmful online activities after the intervention, six reported involvement in at least one type of activity. Three of these had attended a workshop, and three had not. The responses to how often participants engaged in various forms of cybercrime were re-coded so that Never=0, One-off occurrence=1, Monthly=2, Weekly=3, and Daily=4. Four participants responded 'Never' for all offence types, with one responding 'Other' and explaining 'I stopped my data deleting 10 months before the intervention'. The average summed score for all participants before the intervention was 6.9 (M=3.0, SD=9.9, range=0-37).

For offending after the intervention, three participants did not complete this section. Of the remaining 20, 14 reported 'Never' for all offence types (M=0.0, SD=1.1, range=0-4). Table 4 shows the results for self-reported offending before and after the intervention, by behaviour type. Four participants indicated they had committed various activities once, while two others continued to be involved in more than one offence type at least occasionally. No participants had a higher score for self-reported offending after the intervention than before. As the distributions were positively skewed, to test the difference between scores for each harmful online activity before and after the intervention (H_1), Wilcoxon Signed Rank tests were used. The behaviours that were significantly reduced following the intervention were making online services unavailable (e.g., booting, denial-of-service attacks), game cheating (e.g., modding), possession of malicious software (e.g., RATs), and use/distribution of malicious software.

Table 4: Self-reported offending before and after the intervention

	Before the intervention (N=23)					After the intervention (N=20)					Wilcoxon Signed Rank test
	Mean	Median	SD	Min	Max	Mean	Median	SD	Min	Max	Z
Making online services unavailable (e.g. booting, denial-of-service attacks)	1.2	1.0	1.5	0	4	0.1	0.0	0.2	0	1	-2.683**
Tricking people into providing their username and password	0.1	0.0	0.5	0	2	0.1	0.0	0.2	0	1	-1.000
Gaining access to protected computer systems	0.7	0.0	1.2	0	3	0.0	0.0	0.0	0	0	-1.841
Gaining access to secure websites	0.3	0.0	0.6	0	2	0.0	0.0	0.0	0	0	-1.633
Use of stolen credit cards (e.g. carding)	0.2	0.0	0.5	0	2	0.1	0.0	0.2	0	1	-1.732
Trading in fake/stolen online accounts	0.1	0.0	0.6	0	3	0.0	0.0	0.0	0	0	-1.000
Game cheating (e.g. modding)	1.2	0.5	1.4	0	4	0.2	0.0	0.4	0	1	-2.232*
Trolling/sending abusive messages	0.4	0.0	0.9	0	3	0.1	0.0	0.2	0	1	-1.604
Controlling a botnet	0.6	0.0	1.4	0	4	0.0	0.0	0.0	0	0	-1.732
Extracting data (SQL injection attacks)	0.3	0.0	0.8	0	3	0.0	0.0	0.0	0	0	-1.342
Intercepting communications (Eavesdropping attacks)	0.4	0.0	1.0	0	4	0.0	0.0	0.0	0	0	-1.342
Possession of malicious software (e.g. RATS)	0.9	0.0	1.5	0	4	0.2	0.0	0.5	0	2	-2.041*
Use/Distribution of malicious software	0.6	0.0	1.3	0	4	0.0	0.0	0.0	0	0	-2.041*
Other	0.3	0.0	1.0	0	4	0.0	0.0	0.0	0	0	-1.000

* sig at the $p<0.05$ level

** sig at the $p<0.01$ level

The summed scores are used to test if the overall reduction in re-offending was significant (H_2). Again, these distributions are positively skewed, so a Wilcoxon Signed Rank test was used. The two scores (self-reported offending pre- and post-intervention) are significantly different ($Z=-3.4$, $p<.001$).

Table 5 shows before and after self-reported offending scores for self-reported participation in a workshop. The difference between the self-reported offending scores before and after the interventions were significant for those that reported having participated in a workshop, and those that did not. Although those who attended a workshop had higher self-reported offending scores before the intervention, a Mann-Whitney U test finds this difference as not significantly different to those that did not attend a workshop ($Z=-1.708$, p=0.088) (H_3). After the intervention, there was no significant difference in self-reported offending for the two groups (Z=-0.047, p=0.963) (H_4).

Table 5: Self reported offending (summed) before and after the intervention, by workshop status

	Before the intervention (N=23)					After the intervention (N=20)					Wilcoxon Signed Rank test
	Mean	Median	SD	Min	Max	Mean	Median	SD	Min	Max	Z
Reported attending a workshop (n=12)	10.8	7.0	12.3	0	37	0.5	0.0	1.0	0	3	-2.371*
Did not report attending a workshop (n=11)	2.6	1.0	3.4	0	12	0.6	0.0	1.3	0	4	-2.585*

* sig at the p<0.05 level

When asked why they had stopped or reduced their involvement in harmful online activities, three participants directly referred to the intervention they had received:

> *The use of a botnet and DDOS attacks were use by me during my teenage years through gaming as a means of making money from competitive matches for cash prizes. I have since stopped as I no longer play such games and with the cease and desist order, if my activities continued i could be prosecuted.*[sic]
>
> *No need to do it anymore, and since been wary about the police visits*
>
> *Finding out how illegal it is to commit some of the crimes I did, really made me realize how I could affect my future. Its also highly unprofitable in the long run because I never knew they take all of the profits from crime and can restrict computer usage. As well as affecting nearly all job/apprenticeship opportunities with a criminal record.. I'd most probably be in prison with massive fines if it wasn't for the Cyber Prevent officers.*[sic]

Seven participants provided explanations that were relevant to the interventions. These mainly related to gaining awareness of the costs and harms, as well as illegality, of their activities:

> *Realised how stupid/dangerous it was.*
>
> *Since I now realise the consequences of said action*
>
> *I stopped because I found out it is illegal and harmful to companies and can cost them millions*
>
> *Because it's not cool, it just causes trouble if theres [sic] damage or fallout due to the attack*
>
> *My actions can negatively impact others.*
>
> *Because it's bad and harms people*
>
> *Aware of the legalities, gained other hobbies/interests.*

A further six participants referred to reasons external or prior to the interventions, mainly due to aging out of crime:

> *I had stopped prior to the cease and desist notice as i stopped playing online games so there was no need to continue, but if i started playing again i would not involve myself in any such activity as i am now aware of the illegality and the risks.* [sic]

> *Grew up...*
>
> *i stopped before i was warned, they took a while to show up (years after)*[sic]
>
> *I've stopped in anything illegal or harmful that could be caused, reason is that i want a life that's the same as the rest of the people, i don't want to live a life that's fucked. All i want is a flat and a desktop setup and to develop my own games in the future, that is all and that's what i want my life and existence to be* [sic].
>
> *I have stopped everything as I did this for fun when I was younger.*
>
> *too lazy tbh* [to be honest] [sic]

Participants were asked if the intervention made them feel they were more or less likely to be caught if they were involved in harmful online activities. Twelve participants responded more likely (52.2%), two responded less likely (8.7%), seven responded neither (30.4%), and two participants did not answer this question (8.7%). Only 14 participants answered the question 'How much, if at all, did the intervention(s) change your perception of your anonymity online'. Of these, four said 'not at all' (28.6%) and five responded 'somewhat (35.7%). Five participants indicated the intervention had very much or extremely changed their perceptions of anonymity (35.7%). Participants were provided the opportunity to expand on their responses. A number of participants indicated their views had changed, but none explicitly mentioned the mechanism for this, for example:

> *When i [sic] was younger I didn't realize everything can be traced*
>
> *Just because I know its wrong* [sic]
>
> *You're not as anonymous as you think online*
>
> *I feel IF I still wanted to commit a crime today I could, and MAYBE get a way with it in the short term, but with quantum computers on the rise, doesn't mean that my Encryption on an Encrypted Hard Drive will last forever. [sic] I would eventually get caught, maybe with a future family, and a successful life when I'm eventually put behind bars. I'd just much rather wait a year or two, concentrate on studies and be in a successful position at a company than get short term cash that I'd spend on phones that get outdated and rendered useless in a few years.*
>
> *I knew that the police could access information to a certain extent but i was unaware that it would go this far for something i didn't think was that serious.* [sic]

Two participants indicated their views about anonymity had not changed since the intervention, although one said that his awareness of the risky nature of his methods had changed:

> *I knew the risks when I was doing it years ago.. so my perceptions haven't changed*
>
> *I believe only the method in which I carried out attacks was which involved me to get caught. There are so many ways to remain anonymous online which is why people are still able to do these things on a daily basis. This is why perception has not changed too much, as I believe my method was very amateur and is nothing on people who do this kind of thing for a living yet remain anonymous.*

Another participant indicated their views had changed due to advances in technology:

> *Security has gotten better and it has been developed to improve systems and prevent crimes. Newer systems are more easily able to track perpetrators down.*

To conclude, the average summed score for involvement in harmful online activities for all participants before the intervention was 6.9. None had a higher score of self-reported offending after the intervention, nor was there a significant difference in self-reported offending between those who attended a workshop and those who did not. The majority of the participants referred to increased awareness of harm and illegal behaviour, and maturing as reasons for abstaining from the harmful behaviours. After the intervention about half of the respondents felt they were more likely to get caught while the majority did not change or changed somewhat their perceptions regarding anonymity online.

6.6 Awareness of the illicit nature and impact of activities

The aggregated responses of which activities participants thought could be illegal are shown in Table 6. Of the 23 participants, everyone responded it is always illegal to use stolen credit cards, 21 participants stated it is always illegal to trade in fake/ stolen accounts (with one stating it is sometimes illegal), 19 thought it is always illegal to gain access to secure websites and protected computer systems (with four and three thinking it is sometimes illegal, respectively). Finally, 19 believed it is always illegal to control a botnet (with two believing it is sometimes illegal), and 14 responded it is always illegal to make online services unavailable (with six responding it is sometimes illegal). One participant completed part of this section.

Table 6: Perceptions of legality before the intervention

	Always illegal		Sometimes illegal		Never illegal		Not sure	
	N	%	N	%	N	%	N	%
Making online services unavailable (e.g. booting, denial-of-service attacks) (N=23)	14	60.9	6	26.1	1	4.3	2	8.7
Tricking people into providing their username and password (N=23)	18	78.3	4	17.4	1	4.3	0	0.0
Gaining access to protected computer systems (N=23)	19	82.6	3	13.0	0	0.0	1	4.3
Gaining access to secure websites (N=23)	19	82.6	4	17.4	0	0.0	0	0.0
Use of stolen credit cards (e.g. carding) (N=23)	23	100.0	0	0.0	0	0.0	0	0.0
Trading in fake/stolen online accounts (N=23)	21	91.3	1	4.3	1	4.3	0	0.0
Game cheating (e.g. modding) (N=23)	7	30.4	5	21.7	9	39.1	2	8.7
Trolling/sending abusive messages (N=23)	9	39.1	7	30.4	1	4.3	6	26.1
Controlling a botnet (N=23)	19	82.6	2	8.7	1	4.3	1	4.3
Extracting data (SQL injection attacks) (N=23)	18	78.3	2	8.7	0	0.0	3	13.0
Intercepting communications (Eavesdropping attacks) (N=22)	17	77.3	2	9.1	0	0.0	3	13.6
Possession of malicious software (e.g. rats) (N=22)	13	59.1	2	9.1	5	22.7	2	9.1
Use/Distribution of malicious software (N=22)	18	81.8	3	13.6	1	4.5	0	0.0

Participants were asked also how aware they were of the CMA, the impact of cybercrime on victims, and legal and ethical ways to use IT skills, before and after the interventions. One participant did not complete this section.

Of the 22 participants, nine responded they were very aware/ fairly aware of the CMA before the intervention (with 13 responding not very/ not at all aware), and 13 stated they were very aware/ fairly aware of the impact of cybercrime before the intervention (with nine stating not very/ not at all aware). After attending a workshop (N=10), 10 responded they were very aware/ fairly aware of the CMA, and eight were very aware/ fairly aware of the impact of cybercrime (N=9). After attending a police visit (N=20), 16 stated they were very aware/ fairly aware of the CMA, and 14 were very aware/ fairly aware of the impact of cybercrime (N=16). Finally, after receiving a letter (without a visit) (N=14), 10 responded they were very aware/ fairly aware of the CMA, and seven were very aware/ fairly aware of the impact of cybercrime (N=9). Their responses are in Table 7.

Table 7: Awareness of CMA and impact of cybercrime before and after the intervention

		Not at all aware		Not very aware		Fairly aware		Very aware	
		N	%	N	%	N	%	N	%
Awareness of the Computer Misuse Act	Before any intervention (N=22)	7	31.8	6	27.3	4	18.2	5	22.7
	After attending a workshop (if applicable) (N=10)	0	0.0	0	0.0	6	60.0	4	40.0
	After the initial police and desist visit (if applicable) (N=20)	2	10.0	2	10.0	9	45.0	7	35.0
	After receiving the Cease and Desist letter (if received without a visit) (N=14)	3	21.4	1	7.1	7	50.0	3	21.4
Awareness of the impact of cybercrime on victims	Before any intervention (N=22)	3	13.6	6	27.3	7	31.8	6	27.3
	After attending a workshop (if applicable) (N=9)	1	11.1	0	0.0	4	44.4	4	44.4
	After the initial police and desist visit (if applicable) (N=16)	2	12.5	0	0.0	9	56.3	5	31.1
	After receiving the Cease and Desist letter (if received without a visit) (N=9)	2	22.2	0	0.0	4	44.4	3	33.3

Of the 22 participants who responded to the question regarding legal and ethical ways of using IT skills before the intervention, three (13.6%) were not at all aware, five (22.7%) were not very aware, 11 (50%) were fairly aware, and three (13.6%) were very aware. Those that participated in the workshops were also asked if they had since engaged with any of the companies present or the resources offered. Two participants had participated in 'capture the flag' events, one indicated they had taken up an apprenticeship, one had taken up a full time job, and another indicated they had taken up cybersecurity online training.

To sum up, before the intervention all respondents were aware of the illegal nature of using stolen credit cards and almost everyone was aware of the illegal nature of trading in fake/stolen online accounts. The majority of the respondents were very aware/ fairly aware of the CMA, the impact of cybercrime, and ethical ways to use IT skills before the intervention. After attending a workshop (N=10), all respondents were very aware/ fairly aware of the CMA, and the majority were very aware/ fairly aware of the impact of cybercrime.

6.7 Perceptions of likelihood of detection and severity of consequences

Perceptions of likelihood of detection by police since receiving the intervention for each type of harmful online activity are detailed in Table 8. Of our 19 participants, 11 responded it is very likely to be detected for use of stolen credit cards (with four responding somewhat likely), seven stated it is very likely to be detected for making online services unavailable (with seven stating it is somewhat likely), four thought it is very likely to be detected for use/ distribution of malicious software (with eight thinking it is somewhat likely), and three believed it is very likely to be detected for gaining access to protected computer systems (with nine believing it is somewhat likely).

Table 8: Perceptions of likelihood of detection after the intervention

	Very unlikely		Not likely		Somewhat likely		Very likely		Not sure	
	N	%	N	%	N	%	N	%	N	%
Making online services unavailable (e.g. booting, denial-of-service attacks) (N=21)	2	9.5	2	9.5	7	33.3	7	33.3	3	14.3
Tricking people into providing their username and password (N=21)	4	19.0	3	14.3	8	38.1	2	9.5	4	19.0
Gaining access to protected computer systems (N=21)	2	9.5	3	14.3	9	42.9	3	14.3	4	19.0
Gaining access to secure websites (N=21)	3	14.3	3	14.3	7	33.3	4	19.0	4	19.0
Use of stolen credit cards (e.g. carding) (N=21)	2	9.5	1	4.8	4	19.0	11	52.4	3	14.3
Trading in fake/stolen online accounts (N=21)	3	14.3	6	28.6	6	28.6	3	14.3	3	14.3
Game cheating (e.g. modding) (N=21)	10	47.6	2	9.5	4	19.0	0	0.0	5	21.7
Trolling/sending abusive messages (N=21)	4	19.0	5	23.8	5	23.8	2	9.5	5	23.8
Controlling a botnet (N=21)	3	14.3	3	14.3	6	28.6	5	23.8	4	19.0
Extracting data (SQL injection attacks) (N=21)	3	14.3	3	14.3	6	28.6	5	23.8	4	19.03
Intercepting communications (Eavesdropping attacks) (N=21)	3	14.3	4	19.0	5	23.8	4	19.0	5	23.8
Possession of malicious software (e.g. rats) (N=21)	6	28.6	3	14.3	5	23.8	4	19.0	3	14.3
Use/Distribution of malicious software (N=21)	3	14.3	1	14.3	8	38.1	4	19.0	3	13.0

A score for each participant for likelihood of detection was created by summing their responses (from one (very unlikely) to four (very likely) and dividing by the number of responses. Not sure responses were re-coded as non-responses, and therefore were not included in the score. Two participants did not complete this section, and two responded 'Not sure' to all options. Of the remaining 19 participants, the average score was 2.6 (M=2.9, SD=0.7, range=1-3.7). The distribution was negatively skewed. A two-tailed Spearman's correlation test revealed no significant relationship between perception of the likelihood of detection and summed self-reported offending (H_5, rs=.386, p=0.114). A Mann-Whitney U test found that those who participated in a workshop did not have significantly different perceptions of the likelihood of detection compared to those that did not (H_6, Z=-1.369, p=0.171).

Responses for the perceptions of the severity of consequences if caught engaging in each type of harmful online activities are provided in Table 9. Of the 19 participants, 16 said the use of stolen credit cards will have very severe consequences (with three saying severe), 13 thought the use/distribution of malicious software will have very severe consequences (with three thinking severe), and 12 responded controlling a botnet will have very severe consequences (with three responding severe). Notable mentions are possession of malicious software (11 believing it will have very severe consequences and two believing severe), gaining access to protected computer systems (nine stating it will have very severe consequences and seven stating severe), gaining access to secure websites (nine responding it will have very severe consequences and six responding severe), and making online services unavailable (eight thinking it will have very severe consequences and six thinking severe).

Table 9: Perceptions of severity of consequences if caught

	Very light		Light		Severe		Very severe		Not sure	
	N	%	N	%	N	%	N	%	N	%
Making online services unavailable (e.g. booting, denial-of-service attacks) (N=20)	0	0.0	2	10.0	7	35.0	8	40.0	3	15.0
Tricking people into providing their username and password (N=19)	1	5.3	5	26.3	7	36.8	3	15.8	3	15.8
Gaining access to protected computer systems (N=20)	1	5.0	1	5.0	7	35.0	9	45.0	2	10.0
Gaining access to secure websites (N=20)	0	0.0	3	13.0	6	30.0	9	45.0	2	10.0
Use of stolen credit cards (e.g. carding) (N=20)	0	0.0	0	0.0	3	15.0	16	80.0	1	5.0
Trading in fake/stolen online accounts (N=20)	1	5.0	2	10.0	9	45.0	6	30.0	2	10.0
Game cheating (e.g. modding) (N=20)	7	35.0	6	30.0	2	10.0	2	10.0	3	13.0
Trolling/sending abusive messages (N=20)	4	20.0	6	30.0	4	20.0	2	10.0	4	20.0
Controlling a botnet (N=20)	0	0.0	2	10.0	3	15.0	12	60.0	3	15.0
Extracting data (SQL injection attacks) (N=20)	1	5.0	2	10.0	5	25.0	9	45.0	3	15.0
Intercepting communications (Eavesdropping attacks) (N=20)	1	5.0	3	15.0	4	20.0	9	45.0	3	15.0
Possession of malicious software (e.g. rats) (N=20)	0	0.0	4	20.0	2	10.0	11	55.0	3	15.0
Use/Distribution of malicious software (N=20)	0	0.0	2	10.0	3	15.0	13	65.0	2	10.0

A score for each participant for severity of consequences was created by summing their responses (from one (Very light) to four (Very severe) and dividing by the number of responses. 'Not sure' responses were not included in the score. Of the 19 participants who responded, the average score was 3.2 (M=3.2, SD=0.6, range=2.2-4.0). The distribution was negatively skewed. There was no significant relationship between summed self-reported offending after the intervention and perceived severity of consequences (H_7, rs=.065, p=.792). A Mann-Whitney U test found that those who participated in a workshop did not have significantly different perceptions of the severity of consequences compared to those that did not (H_8, Z=-0.286, p=0.775).

To summarise, there was no significant relationship between perception of the likelihood of detection and summed self-reported offending, nor between summed self-reported offending and perceived severity of consequences. Those who participated in a workshop did not have significantly different perceptions of the likelihood of detection, nor of the severity of consequences after the intervention compared to those who did not participate.

6.8 Perceptions of procedural justice and police legitimacy

Participants were asked how they felt about the intervention. Of those who responded (N=19), 18 (94.7%) said they felt listened to during the intervention; 19 were satisfied with the way the police officer/s conducted the intervention, and 19 were satisfied with how they were treated. Only one felt they were unable to tell their side of the story. When the police visited, nine (47.4%) participants had expected to be arrested, and 10 (52.6%) did not. Participants' perceptions of police confidence and trustworthiness during the intervention are provided in Table 10.

Table 10: Perceptions of police confidence and trustworthiness

	Not at all		Somewhat		Moderate		Very		Extremely	
	N	%	N	%	N	%	N	%	N	%
Knowledgeable (N=19)	2	10.5	1	5.3	5	26.3	6	31.6	5	26.3
Legitimate (N=19)	1	5.3	4	21.1	3	15.5	5	26.3	6	31.6
Friendly (N=19)	1	5.3	0	0.0	4	21.1	7	36.8	7	36.8
Trustful/honest (N=19)	2	10.5	1	5.3	3	15.8	7	36.8	6	31.6

Participants were asked about their perceptions of police effectiveness, obligation to obey police, and willingness to cooperate with the police. Responses are provided in Tables 11 to 13.

Table 11: Perceptions of police effectiveness

	Very poor job		Poor job		Undecided		Good job		Very good job	
	N	%	N	%	N	%	N	%	N	%
Solving crime (N=21)	1	4.8	2	9.5	8	38.1	8	38.1	2	9.5
Solving cybercrime (N=21)	2	9.5	3	14.3	8	38.1	6	28.6	2	9.5
Dealing with problems that concern you (N=21)	1	4.8	5	23.8	8	38.1	6	28.6	1	4.8
Working with your community to solve local problems (N=20)	1	5.0	5	25.0	7	35.0	6	30.0	1	5.0
Preventing crime (N=20)	1	5.0	4	20.0	6	30.0	7	35.0	2	10.0

Table 12: Obligation to obey police

	Strongly disagree		Disagree		Undecided		Agree		Strongly agree	
	N	%	N	%	N	%	N	%	N	%
I feel a moral obligation to obey the law (N=18)	1	5.6	2	11.1	4	22.2	7	38.9	4	22.2
I feel a moral obligation to obey police (N=18)	2	11.1	2	11.1	2	11.1	9	50.0	3	16.7
Overall, I obey police with good will (N=19)	0	0.00	1	5.3	4	21.1	9	47.4	5	26.3

Table 13: Willingness to cooperate with police

How likely would you be to:	Very unlikely		Not likely		Somewhat likely		Very likely		Extremely likely	
	N	%	N	%	N	%	N	%	N	%
Call police to report a crime (N=20)	2	10.0	3	15.0	4	20.0	6	30.0	5	25.0
Help police find someone suspected of committing a crime by providing them with information (N=20)	3	15.0	1	5.0	5	25.0	5	25.0	6	30.0
Report dangerous or suspicious activities to police (N=20)	2	10.0	0	0.0	7	35.0	5	25.0	6	30.0
Willingly assist police if asked (N=20)	3	15.0	1	5.0	4	20.0	5	25.0	7	35.0

An overall score of perceptions of police legitimacy and procedural justice was created for each participant by averaging their responses to each question. A higher score indicated a higher perception of legitimacy. The distribution was normally distributed, with an average score of 2.9 (M=2.8, SD=0.8, range=1-4.5). There was no correlation between perceptions of police legitimacy and procedural justice and summed self-reported offending after the intervention (H_9, rs=.252, p=.298). There was no difference in perceptions of police legitimacy and procedural justice between those who did and did not attend a workshop (H_{10}, Z=-.247, p=.805).

Concluding, the majority of respondents said they felt listened to, satisfied with how they were treated and with the way the police officer/s conducted the interventions. There was no correlation between perceptions of police legitimacy and procedural justice, as there was no difference in perceptions of police legitimacy and procedural justice between those who did and those who did not attend a workshop.

7 Discussion

Our analysis shows that the interventions are associated with lower self-reported involvement in harmful online activities, compared to before the intervention. Activities that were significantly reduced after the intervention were DoS attacks, game cheating and modding, possession of malicious software, and use/distribution of malicious software. While self-reported offending for the other types of harmful online activities was lower, this was not significant. We note that it was difficult to compare participants according to the intervention received, as many received more than one intervention. However, we found that there was no significant difference in re-offending for those who participated in a workshop compared to those who did not.

Although the results are tentative, they could suggest increased awareness of cybercrime legislation and impact (harm and cost) following the interventions among our participants. The informative nature of the interventions can promote a better understanding of the CMA, the illegality of and the harm caused by these activities. The need for this is underlined by the widespread confusion about the lawfulness of the activities in the group under study but also the wider population. Moreover, these results may be supported further by the positive views of police legitimacy and procedural justice the participants indicated adding to the potential suitability of the intervention as a countermeasure for cybercrime.

Regarding perceptions relating to specific offences, a couple of points are worth mentioning. Use of stolen credit cards (e.g., carding) seems to be an activity of explicitly unlawful nature to our participants when looking at the highest degree of certainty (i.e., Very severe, Always illegal, Very likely). Prior to the interventions, it was considered an unequivocally illegal activity by all the participants. After the interventions, it is still thought to have the highest likelihood of detection, and the most severe punishment in case of apprehension.

Following use of stolen credit cards, gaining access to secure websites and protected computer systems are clearly considered to be unlawful, however they are considered to be less severe in terms of punishment and to bear a low chance of detection relative to the unlawfulness. The same applies to trading in fake/ online accounts. However, controlling a botnet, use/ distribution of malicious software and possession of malicious software score high in terms of illegality and severity of punishment. Also, the participants are well aware of the unlawful nature of being actively involved in illegal activities such as gaining access to secure websites and protected computer systems, controlling botnets, and use/ distribution of malicious software. However, when it comes to being detected for potential unlawful activity, they feel this is very likely for making online services unavailable (after use of stolen credit cards).

These patterns suggest that first and foremost, participants are clear on the unlawful nature of activities relating to financial services/ products and online illegal activities that have been reported on and publicised extensively. Also, the participants are mostly aware of the illegal nature of the activities they had been contacted for by the police (especially making online services unavailable such as DoS and gaining access to protected computer systems). Making online services unavailable is the most common reason participants were contacted by the police, yet they believe there is a low likelihood of detection. This could point to the participants' awareness of the technical and investigatory challenges which also have been discussed publicly and extensively, however it should be explored further.

The overall impressions of the participants about the interventions were positive. Primarily, the participants felt calm and surprised by the interventions. These results suggest that the participants were not expecting to be identified and/or apprehended for any harmful online activities they (might) have been involved. This can be related to the assumptions of low likelihood of apprehension or punishment which are prevalent among cyber offenders for several reasons (e.g., anonymity, attribution difficulties, police capacity).

More specifically, the workshop was the least likely, compared to police visits and 'cease and desist' letters, to provoke negative feelings (angry, calm, disappointed, sad, upset), barring 'afraid' which was more likely with the workshop rather than the letters. Also, the workshop was least likely to cause surprise, and participants were just as calm as in police visits. This could be because workshop participants are invited to the event, therefore they are aware of the intervention and its premise. Moreover, the interactive element of the workshop which allows space for discussion and clarifications (just as in police visits), the advice on how recipients can develop their skills further, the realisation of and hope for profitable career opportunities despite their identification by the police, and the presence of carers/guardians contribute to the avoidance of negative feelings. All elements combined can make the format of the workshop less intimidating and more informal which can facilitate establishing rapport with the young people.

While the NCA's own research found that gaming was a significant precursor to cybercrime activity, this was the second-highest rated pathway for our participants, with the primary way being through their own research. While this solo pathway was the most frequently selected, it is apparent online interactions are quite important, whether this be through gaming or online forums and communities. Offline contacts, including at school or through family and friends, were relatively less important for our group.

The motivations for becoming involved in harmful online activities seem to reflect the ones previously reported in relevant literature. Financial gain was not an important reason for involvement, and none of the participants were politically motivated. Participants were far more likely to be involved for the fun and challenging aspects of the activities, for skill development, and for earning kudos from their peers. Some participants expanded on their responses, explaining that they had become involved due to anxiety/stress, depression, peer pressure, and feelings of worthlessness. Low self-esteem may be why young people are joining online communities and platforms that can lead to harmful activities. Acceptance, validation and support within a virtual or physical community can counter feelings of isolation experienced by young people and provide a sense of belonging [90].

The majority of the participants identified as male, predominantly in adolescence or early adulthood. This comes as no surprise considering the majority of the cybercrime intervention recipients are young males with an average age of 17 (at the time of the intervention). However, the years between the alleged harmful activity and the intervention have a median of three to four years and a mode of one to two. This means that the majority of the participants were in early or late adolescence when the alleged harmful activity occurred as they were in late adolescence or early adulthood at the time of the intervention. These results are reflecting broader findings relating to the age-crime curve: offending tends to increase in late childhood, peaks during adolescence approx. between the ages of 15–19, and then drops in young adulthood, approx. in the early 20s [91]. This is reflected in some of the open-ended responses mentioned earlier where some of our participants referred to aging/ maturing as the reason for moving away from harmful online activities.

Throughout the survey we referred to harmful online activities, rather than crimes. This is because some of the behaviours listed, such as game cheating and modding, may not be criminal necessarily (instead they may infringe the terms of service). Another ambiguity lies in the possession of 'hacking tools'. Under section 3A of the UK's CMA

1990, making, supplying or obtaining malicious software is an offence, but only if intended to be used to break into, or compromise, computer systems. The Crown Prosecution Service [92] has issued guidelines, specifying that the prosecution must prove the defendant had the necessary intent, and that possession alone is not an offence. Indeed, one participant who worked in IT noted that they had been in possession of the malware for a legitimate purpose. However, five participants incorrectly thought that possession of malicious software was never illegal. Once more, this can hint at the confusion about the lawfulness of these actions, part of which can be attributed to the ambiguity and datedness of the CMA.

8 Conclusion

The results of this research project indicate:

H_1 (significant lower self-reported involvement in each harmful online activity after the interventions compared to before the interventions) was partially supported. The harmful online activities that were significantly reduced after the intervention were DDOS attacks, game cheating and modding, possession of malicious software, and use/distribution of malicious software. For the other types of harmful online activities self-reported offending was lower, but not significant.

H_2 (significant lower overall rate of involvement in harmful online activities after the interventions compared to before the interventions) was supported. Overall, the intervention group (workshops) and control group (letters and police visits) both had significantly lower rates of post-offending. However, those who participated in the workshops did not have significantly lower levels of post-intervention offending, compared to the control group (H_4).

While those who attended workshops did not have significantly lower self-reported offending after the intervention compared to those who did not, the workshops do offer something different to the 'cease and desist' interventions. Participants seem to value the opportunity to discuss their predicament, receive information about developing their technical skills lawfully, and about career opportunities with a participatory, informal approach.

We did not find any support for H_3 (significant higher levels of self-reported overall pre-intervention involvement in harmful online activities for those in the intervention group compared to the control group.). Those who participated in the workshops did report higher levels of pre-intervention offending, however this was mainly due to the presence of an outlier that reported very high levels of offending[2].

Also, we found no significant differences between the experimental and control groups in perceptions of likelihood of detection (H_5 and H_6), severity of consequences (H_7 and H_8), and police legitimacy and procedural justice (H_9 and H_{10}). Moreover, higher levels of perceived likelihood of detection, severity of consequences, and police legitimacy and procedural justice were not correlated with post-intervention self-reported offending, contrary to expectation.

Interestingly, neither the perception of the likelihood of apprehension nor the severity of punishment seem to have had a deterrent effect in our group. While the majority of views indicated perceptions of police legitimacy and procedural justice were positive, this was unrelated to self-reported offending.

These results are tentative and cannot be generalised to a wider population due to certain limitations. First, we used a retrospective, cross-sectional survey. With retrospective studies we cannot be sure about the level of real change [31]. Also, due to our small sample size, we were limited by the types of multi- and bi-variate statistical tests possible. While our response rate of 12.7% was not too bad, we note it could be better[3]. Moreover, we used self-reported offending. This type of reporting gathers more data about illicit behaviours compared to administrative data. However, participants may still under-report to conceal their activities and protect themselves from potential self-incrimination or because of forgetfulness. Lastly, this study focused on intervention recipients. Future work should include those involved in the delivery of the interventions (e.g., NCA, ROCUs,

[2] Due to skewed distribution, we used a non-parametric statistical test (rank ordering rather than mean scores). We found the difference was not significant.

[3] [33] achieved a response rate of 20.7% by offering a voucher of €50 as an incentive. This was not possible for our project due to limits set by our institution.

private sector) as they are integral to their effective implementation.

For the above reasons, we recommend that the NCA conducts a randomised controlled trial (RCT) to measure the effects of their interventions. RCTs evaluate the effects of different interventions using random allocation between intervention and control groups (in this case workshops, and letters and police visits), to allow for causal inference. RCTs are a robust approach to examining intervention effects while controlling for bias and other factors [25]. Moreover, the approach allows the respondents to conceal their activities, while providing useful data to the researchers [29]. Finally, our work was built on insights from previous studies. However, research on cybercrime interventions is lacking, besides a few notable exceptions [4]. For this, we recommend further exploration of the subject; understanding cybercrime interventions and their impact on recipients is key in designing and implementing effective policies to tackle the increasing number of harmful online activities, especially at a time of fiscal constraints.

References

[1] Bossler, A.M. and Burrus, G.B. 2011. The general theory of crime and computer hacking: low self-control hackers?. In: T.J. Holt and B.H. Schell, eds. Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications. Hershey, PA: ISI Global, 38–67.

[2] British Society of Criminology. 2015. Code of Ethics. Available at: www.britsoccrim.org/docs/CodeofEthics.pdf (accessed 15/11/2021).

[3] British Sociological Association. 2017. Statement of Ethical Practice. Available at: www.britsoc.co.uk/media/24310/bsa_statement_of_ethical_practice.pdf (accessed 15/11/2021).

[4] Brewer, R., De Vel-Palumbo, M., Hutchings, A., Holt, T.J., Goldsmith, A. and Maimon, D. 2019. Cybercrime Prevention (Crime Prevention and Security Management). Cham: Springer International Publishing.

[5] Brown, J.R. 2010. Trajectories of parents' experiences in discovering, reporting, and living with the aftermath of middle school bullying. Doctoral dissertation. Retrieved from ProQuest Dissertations and Theses (UMI No. 3409133).

[6] Eckert, R. 2009. Community policing as procedural justice: An examination of Baltimore residents after the implementation of a community policing strategy. (Master's thesis, Villanova University). Retrieved from ProQuest Dissertations and Theses (UMI Number: 1462400).

[7] Elliott, D. and Ageton, S. 1980. Reconciling race and class differences in self-reported and official estimates of delinquency. American Sociological Review, 45(1), 95-110.

[8] EUROPOL. 2018. World's biggest marketplace selling internet paralysing DDoS attacks taken down. EUROPOL, May 1. Available at: https://www.europol.europa.eu/media-press/newsroom/news/world's-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down) (accessed 02 December 2021).

[9] Ginner Hau, H. and Azad, A. 2019. Adolescent female offenders' subjective experiences of their families' roles in relation to their delinquency. Available at: http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-167718 (accessed 30 April 2020).

[10] Holt, T.J. and Bossler, A.M. 2014. An assessment of the current state of cybercrime scholarship. Deviant Behavior, 35(1), 20-40.

[11] Holt, T.J. and Kilger, M. 2012. Examining Willingness to Attack Critical Infrastructure Online and Offline. Crime & Delinquency, 58(5), 798–822. https://doi.org/10.1177/0011128712452963.

[12] Home Office. 2018. Serious and Organised Crime Strategy. Retrieved from https://www.gov.uk/government/publications/serious-and-organised-crime-strategy-2018 (accessed 30 April 2020).

[13] Hutchings, A. 2014. Crime from the keyboard: Organised cybercrime, co-offending,initiation and knowledge transmission Crime, Law and Social Change, 62(1), 1-20.

[14] Hutchings, A. 2016. Cybercrime trajectories: An integrated theory of initiation, maintenance, and desistance. In: T.J. Holt, ed. Crime Online: Correlates, Causes, and Context. Durham: Carolina Academic Press, 117-140.

[15] Hutchings, A. and Clayton, R. 2016. 'Exploring the provision of online booter services'. Deviant Behavior 37(10), 1163-1178.

[16] Jordan, T. and Taylor, P. 1998. A sociology of hackers. The Sociological Review, 46(4), 757-780.

[17] Kirwan, D. 2017. An Investigation of the Attitudes and Environmental Factors that Make People more Willing to Participate in Online Crime, Masters Dissertation, Technological University Dublin.

[18] Murphy, K., Hinds, L. and Fleming, J. 2008. Encouraging public cooperation and support for police. Policing and Society, 18(2), 136–155.

[19] Murphy, K., Mazerolle, L. and Bennett, S. 2014. Promoting trust in police: findings from a randomised experimental field trial of procedural justice policing. Policing and Society, 24(4), 405-424.

[20] National Crime Agency. 2016. Intelligence Assessment, Pathways into Serious and Organised Crime. https://nationalcrimeagency.gov.uk/who-we-are/publications/358-nca-intelligence-assessment-pathways-into-serious-and-organised-crime/file (accessed 30 April 2020).

[21] National Crime Agency. 2017. Pathways into cyber crime. Available at: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file (accessed 30 April 2020).

[22] Paulin, J., Searle, W. and Knaggs, T. 2003. Attitudes to Crime and Punishment. Wellington, New Zealand: Ministry of Justice.

[23] Ren, L., Cao, L., Lovrich, N. and Gaffney, M. 2005. Linking confidence in police with the performance of the police: Community policing can make a difference. Journal of Criminal Justice, 33, 55–66.

[24] Sawyer, J.L., Mishna, F., Pepler, D. and Wiener, J. 2011. The missing voice: Parents' perspectives of bullying. Children and Youth Services Review, 33, 1795–1803.

[25] Sherman, L.W., Strang, H., Barnes, G.C., Braithwaite, J., Inkpen, N. and Teh, M.M. 1998. Experiments in restorative policing: A progress report on the Canberra Reintegrative Shaming Experiments (RISE). Canberra: Australian Federal Police and Australian National University.

[26] Singer, L. 2004. Reassurance policing: An evaluation of the local management of community safety. Home Office Research Studies (Vol. 228). London: Home Office.

[27] Skogan, W.G., and Steiner, L. 2004. CAPS at Ten: Community policing in Chicago - An evaluation of Chicago's alternative policing strategy. Chicago, IL: The Chicago Community Policing Evaluation Consortium.

[28] Sturges, J.E., and Hanrahan, K.J. 2011. The Effects of Children's Criminality on Mothers of Offenders. Journal of Family Issues, 32(8), 985–1006.

[29] Thornberry, P.T. and Krohn, D.M. 2000. The self-report method for measuring delinquency and crime. In Criminal Justice 2000: Measurement and analysis of crime and justice, vol 4, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.

[30] Tuffin, R., Morris, J. and Poole, A. 2006. An evaluation of the impact of the National Reassurance Policing programme. Home Office Research Study 296. London: Development and Statistics Directorate, Home Office Research.

[31] de Vaus, D. 2002. Surveys In Social Research (5th ed.). Abingdon: Routledge

[32] de Vries, S., Hoeve, M., Asscher, J.J. and Stams, G.J. 2014. The effects of the prevention program 'New Perspectives' (NP) on juvenile delinquency and other life domains: study protocol for a randomized controlled trial. BMC Psychology, 2:10.

[33] Weulen Kranenbarg, M., Holt T.J. and van Gelder, J.L. 2019. Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. Deviant Behavior, 40(1), 40-55.

[34] Wikström, P.-O. H., Tseloni, A. and Karlis, D. 2011. Do people comply with the law because they fear getting caught? European Journal of Criminology, 8(5), 401–420.

[35] BBC. 2015. "Police target UK's young cybercriminals." BBC, December 08. Retrieved December 02, 2021. (https://www.bbc.co.uk/news/technology-35028690).

[36] CREST. 2015. Identify, Intervene, Inspire. Helping young people to pursue careers in cyber security, not cybercrime. UK: CREST.

[37] Botley, M., Jinks, B. and Metson, C., 2010. Young people's views and experiences of the youth justice system. University College London: Institute of Education.

[38] Weaver, Beth. 2019. "Understanding desistance: a critical review of theories of desistance." Psychology, Crime & Law, 25, 641-658.

[39] Laub, J. H., and Sampson, R. J. 2001. Understanding desistance from crime. Crime and Justice, 28, 1–69.

[40] Burnett, R. and Maruna, S. 2004. So 'Prison Works', Does It? The Criminal Careers of 130 Men Released from Prison under Home Secretary, Michael Howard. The Howard Journal of Criminal Justice, 43, 390-404.

[41] Piquero, N.L., and Benson, M.L. 2004. White-Collar Crime and Criminal Careers. Journal of Contemporary Criminal Justice, 20, 148-165.

[42] Shulman, E. P., Smith, A. R., Silva, K., Icenogle, G., Duell, N., Chein, J., and Steinberg, L. 2016. The dual systems model: Review, reappraisal, and reaffirmation. Developmental Cognitive Neuroscience, 17, 103-117.

[43] Maruna, S. 2001. Making Good: How Ex-Convicts Reform and Rebuild their Lives. American Psychological Association.

[44] Farrall, S. 2002. Rethinking What Works with Offenders: Probation, Social Context and Desistance from Crime. Cullompton: Willan.

[45] McMahon, G., and Jump, D. 2018. Starting to Stop: Young Offenders' Desistance from Crime. Youth Justice, 18(1), 3–17.

[46] Gottfredson, M. R. and Hirschi, T. 1990. A General Theory of Crime. Stanford: Stanford University Press.

[47] Moffitt, Terrie E. 1993. 'Life-course-persistent' and 'adolescence-limited' antisocial behaviour: A developmental taxonomy. Psychological Review, 100(4), 674-701.

[48] Durlauf, S. N. and Nagin, D. S. 2012. The Deterrent Effect of Imprisonment. In P. J. Cook, J. Ludwig, & J. McCrary (Eds.), Controlling Crime: Strategies and Trade-offs (pp. 43-94). University of Chicago Press

[49] Killias, M., Scheidegger, D., and Nordenson, P. 2009. Effects of increasing the certainty of punishment: a field experiment on public transportation. European Journal of Criminology, 6(5), 387–400.

[50] Nagin, D. S. and Pogarsky, G. 2001. Integrating Celerity, Impulsivity, and Extralegal Sanction Threats into Model of General Deterrence: Theory and Evidence. Criminology, 39(4), 865-892.

[51] Apel, R. and Nagin, D. S. 2011. General Deterrence. In M. Tonry (Ed.), The Oxford Handbook of Crime and Criminal Justice (1st ed., pp. 179-206). Oxford University Press.

[52] Nagin, D. S. 1998. Criminal Deterrence Research at the Outset of the Twenty-First Century. In M. Tonry (Ed.), Crime and Justice: A Review of Research (pp. 1-42). University of Chicago Press.

[53] von Hirsch, A., Bottoms, A. E., Burney, E., and Wikström, P-O. 1999. Criminal Deterrence and Sentence Severity: An Analysis of Recent Research. Hart Publishing.

[54] Nagin, D. S., Cullen, F. T., and Jonson, C. L. 2009. Imprisonment and Reoffending. Crime and Justice, 38(1), 115–200.

[55] Lipsey, M. W. and Wilson, D. B. 1998. Effective intervention for serious juvenile offenders: A synthesis of research. Pp. 313-345. In Serious & violent juvenile offenders: Risk factors and successful interventions, edited by Rolf Loeber and David P. Farrington. Thousand Oaks: Sage Publications.

[56] Aos, S., Phipps, P., Barnoski, R. and Lieb, R. 2001. The Comparative Costs and Benefits of Programs To Reduce Crime. Version 4.0 (WSIPP-01-05-1201). Olympia: Washington State Institute for Public Policy.

[57] Sherman, L. and Strang, H. 2007. Restorative justice: The evidence. London: The Smith Institute.

[58] Lipton, D., Pearson, F., Cleland, C., and Yee, D. 2002. The effects of therapeutic communities and milieu therapy on recidivism. Pp. 39-78. In Offender Rehabilitation and Treatment: Effective Programmes and Policies to Reduce Re-offending, edited by James McGuire. Chichester: John Wiley and Sons.

[59] Schmucker, M. and Lösel, F. 2015. The effects of sexual offender treatment on recidivism: An international meta-analysis of sound quality evaluations. Journal of Experimental Criminology 11: 597-630.

[60] Sunshine, J. and Tyler, T. R. 2003. The role of procedural justice and legitimacy in shaping public support for policing. Law & Society Review 37(3), 513–548.

[61] Tyler, T. R. 1990. Why People Obey the Law. New Haven: Yale University Press.

[62] Törnblom, K. and Vermunt, R. 2007. Towards an Integration of Distributive Justice, Procedural Justice, and Social Resource Theories. Social Justice Research 20, 312-335.

[63] Lusthaus, J. 2014. Electronic Ghosts. Democracy: A Journal of Ideas, 31.

[64] Conway, G. and Hadlington, L. 2018. How do undergraduate students construct their view of cybercrime? Exploring definitions of cybercrime, perceptions of online risk and victimization. Policing: A Journal of Policy and Practice, 98, 1752-4512.

[65] Harkin, D., Whelan, C. and Chang, L. 2018. The challenges facing specialist police cyber-crime units: an empirical analysis. Police Practice and Research 19(6), 519-536.

[66] Kirwan, G. and Power, A. 2013. Cybercrime: The Psychology of Online Offenders. Cambridge University Press.

[67] Young, R., Zhang, L., and Prybutok, V. R. 2007. Hacking into the minds of hackers. Information Systems Management, 24(4), 281-287.

[68] Brenner, S. 2012. Cybercrime and the Law: Challenges, Issues, and Outcomes. Northeastern University Press.

[69] Deković, M., Slagt, M.I., Asscher, J.J., Boendermaker, L., Eichelsheim, V.I. and Prinzie, P., 2011. Effects of early prevention programs on adult criminal offending: A meta-analysis. Clinical psychology review, 31(4), pp.532-544.

[70] Asscher, J. J., Deković, M., van der Laan, P. H., Prins, P. J. M. & van Arum, S. 2007. Implementing randomized experiments in criminal justice settings: an evaluation of multi-systemic therapy (MST) in the Netherlands. Journal of Experimental Criminology, 3(2), 113–129.

[71] Klenowski, P. M., Bell, K. J., and Dodson, K. D. 2010) An empirical evaluation of juvenile awareness programs in the United States: Can juveniles be 'scared straight'? Journal of Offender Rehabilitation, 49(4), 254-272.

[72] Petrosino A., Turpin-Petrosino, C., and Finckenauer, J. O. 2000. Well-meaning programs can have harmful effects! Lessons from experiments of programs such as Scared Straight. Crime & Delinquency, 46(3), 354-379.

[73] Sherman, L. 1993. Defiance, deterrence, and irrelevance: A theory of the criminal sanction. Journal of Research in Crime and Delinquency, 30(4), 445-473.

[74] Grabosky, P. N. 1996. Unintended consequences of crime prevention. Crime Prevention Studies, 5(1), 25–56.

[75] Grabosky, P. N. 2001. Virtual Criminality: Old Wine in New Bottles? Social & Legal Studies, 10(2), 243–249.

[76] Smith, R. G., Wolanin, N., and Worthington, G. 2003. e-Crime Solutions and Crime Displacement. Trends & Issues in Crime and Criminal Justice, 243. Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi243

[77] Hodgkinson, S. and Tilley, N. 2007. Policing anti-social behaviour: Constraints, dilemmas and opportunities. The Howard Journal of Criminal Justice, 46(4), 385-400.

[78] McAra, L. and McVie, S. (2010). Youth crime and justice: Key messages from the Edinburgh Study of Youth Transitions & Crime. Criminology & Criminal Justice, 10(2), 179-209.

[79] Hannemyr, G. 1999. Technology and Pleasure: Considered hacking constructive. First Monday, 4(2). http://journals.uic.edu/ojs/index.php/fm/article/view/647/562

[80] Steinmetz, K. F. 2016. Hacked: A Radical Approach to Hacker Culture and Crime. New York University Press.

[81] Wall, D. S. 2007. Cybercrime: The Transformation of Crime in the Information Age. Polity.

[82] Suler, J. 2004) The online disinhibition effect. CyberPsychology & Behavior, 7(3), 321–326.

[83] Chua, Y. T. and Holt T. J. 2016. A cross-national examination of the techniques of neutralization to account for hacking behaviors. Victims & Offenders, 11(4), 534–555.

[84] Holt, T. J., Bossler, A. M., and May, D. C. 2012. Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance. American Journal of Criminal Justice, 37(3), 378-395.

[85] Marcum, C. D., Higgins, G. E., Ricketts, M. L., and Wolfe, S. E. 2014. Hacking in High School: Cybercrime Perpetration by Juveniles. Deviant Behavior, 35(7), 581-591.

[86] Wall, D. S. 2017. Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing. Pp.1075-1096 in The Oxford Handbook on the Law and Regulation of Technology, edited by Roger Brownsword, Eloise Scotford and Karen Yeung. Oxford: Oxford University Press.

[87] Blackburn, J., Kourtellis, N., Skvoretz, J., Ripeanu, M. and Iamnitchi, A. 2014. Cheating in online games: A social network perspective. ACM Transactions on Internet Technology 13(3), 1–25.

[88] Hutchings, A. and Holt, T. J. 2017. The online stolen data market: disruption and intervention approaches. Global Crime 18(1), 11–30.

[89] Lee, J. R. and Holt, T. J. 2020. Assessing the factors associated with the detection of juvenile hacking behaviors. Frontiers in Psychology 11, 1-10.

[90] Gelder, K. 2007. Subcultures: Cultural histories and social practice. Abingdon: Routledge.

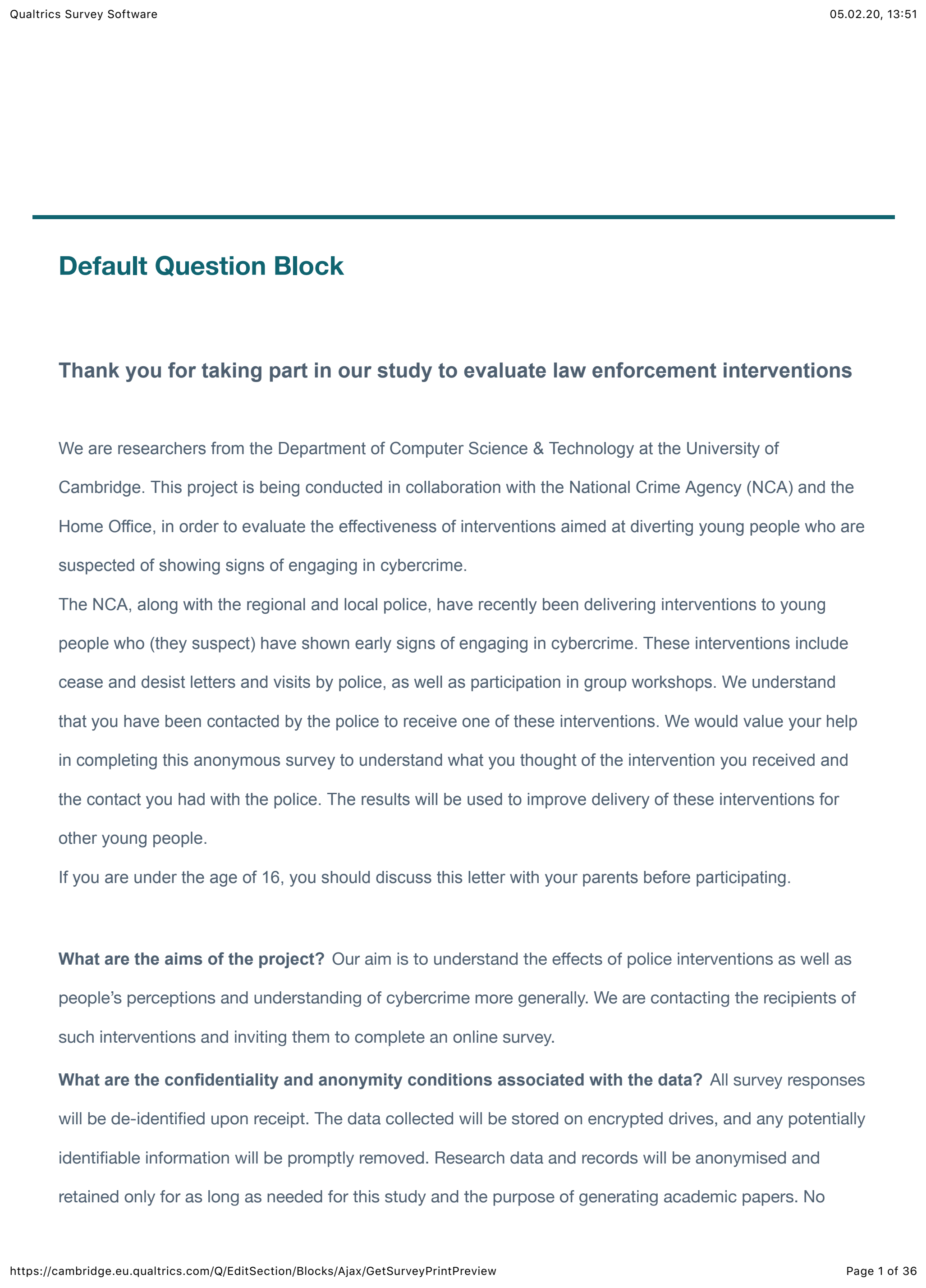
[91] Loeber, R. and Farrington, D. P. 2014. Age-Crime Curve. In Encyclopedia of Criminology and Criminal Justice, edited by Gerben Bruinsma and David Weisburd. New York: Springer.

[92] Crown Prosecution Service. 2020. Computer Misuse Act 1998. Legal guidance. London: Crown Prosecution Service. Retrieved April 30, 2020. (https://www.cps.gov.uk/legal-guidance/computer-misuse-act).

[93] Brantingham, P. J. and Faust, F. L. 1976. A conceptual model of crime prevention. Crime & Delinquency 22(3), 284–296.

[94] Ugwudike, P. and Morgan, G. 2019. Bridging the gap between research and frontline youth justice practice. Criminology & Criminal Justice 19(2), 232–253.

A Qualtrics survey



Default Question Block

Thank you for taking part in our study to evaluate law enforcement interventions

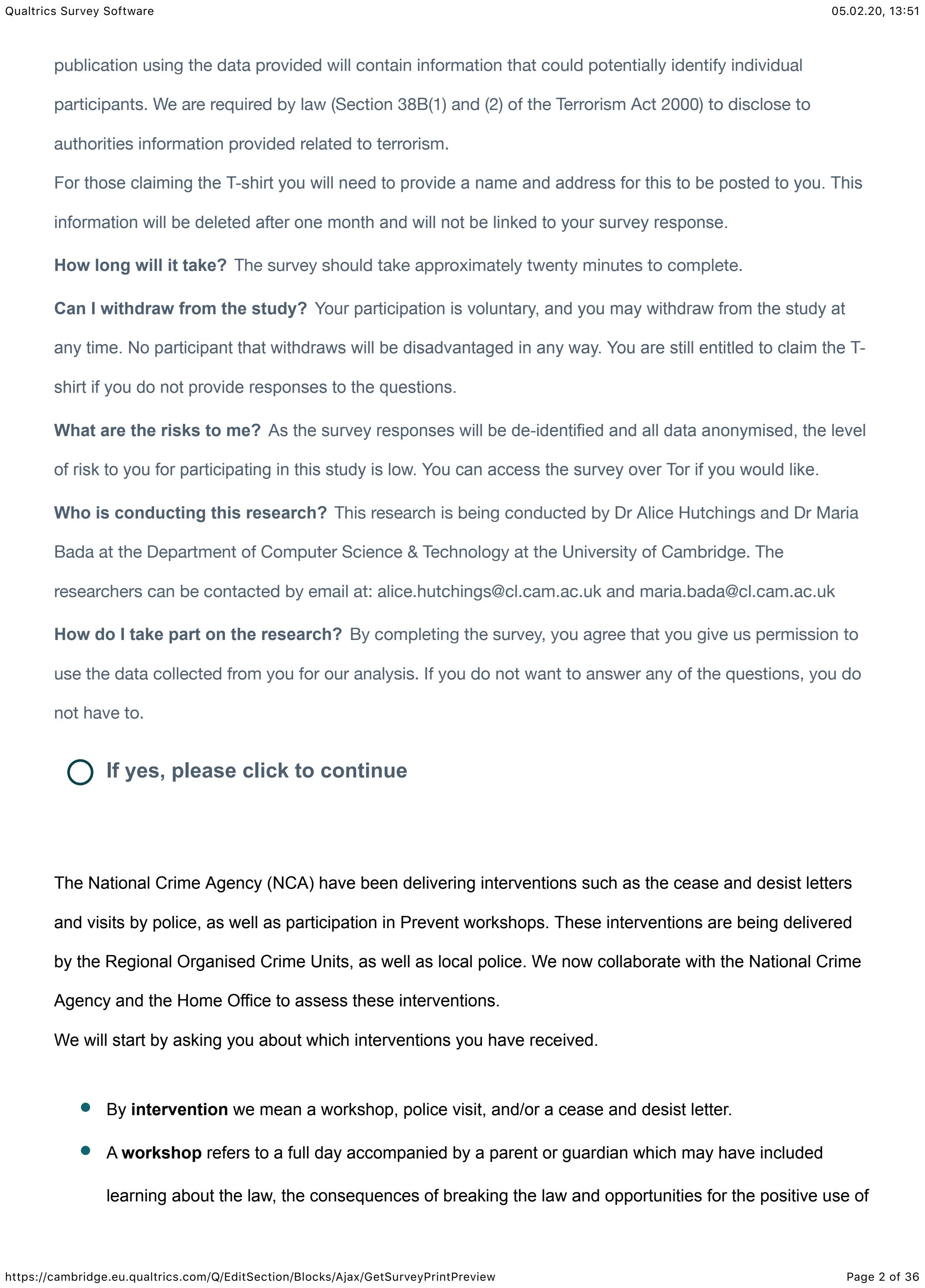
We are researchers from the Department of Computer Science & Technology at the University of Cambridge. This project is being conducted in collaboration with the National Crime Agency (NCA) and the Home Office, in order to evaluate the effectiveness of interventions aimed at diverting young people who are suspected of showing signs of engaging in cybercrime.

The NCA, along with the regional and local police, have recently been delivering interventions to young people who (they suspect) have shown early signs of engaging in cybercrime. These interventions include cease and desist letters and visits by police, as well as participation in group workshops. We understand that you have been contacted by the police to receive one of these interventions. We would value your help in completing this anonymous survey to understand what you thought of the intervention you received and the contact you had with the police. The results will be used to improve delivery of these interventions for other young people.

If you are under the age of 16, you should discuss this letter with your parents before participating.

What are the aims of the project? Our aim is to understand the effects of police interventions as well as people's perceptions and understanding of cybercrime more generally. We are contacting the recipients of such interventions and inviting them to complete an online survey.

What are the confidentiality and anonymity conditions associated with the data? All survey responses will be de-identified upon receipt. The data collected will be stored on encrypted drives, and any potentially identifiable information will be promptly removed. Research data and records will be anonymised and retained only for as long as needed for this study and the purpose of generating academic papers. No



publication using the data provided will contain information that could potentially identify individual participants. We are required by law (Section 38B(1) and (2) of the Terrorism Act 2000) to disclose to authorities information provided related to terrorism.

For those claiming the T-shirt you will need to provide a name and address for this to be posted to you. This information will be deleted after one month and will not be linked to your survey response.

How long will it take? The survey should take approximately twenty minutes to complete.

Can I withdraw from the study? Your participation is voluntary, and you may withdraw from the study at any time. No participant that withdraws will be disadvantaged in any way. You are still entitled to claim the T-shirt if you do not provide responses to the questions.

What are the risks to me? As the survey responses will be de-identified and all data anonymised, the level of risk to you for participating in this study is low. You can access the survey over Tor if you would like.

Who is conducting this research? This research is being conducted by Dr Alice Hutchings and Dr Maria Bada at the Department of Computer Science & Technology at the University of Cambridge. The researchers can be contacted by email at: alice.hutchings@cl.cam.ac.uk and maria.bada@cl.cam.ac.uk

How do I take part on the research? By completing the survey, you agree that you give us permission to use the data collected from you for our analysis. If you do not want to answer any of the questions, you do not have to.

○ **If yes, please click to continue**

The National Crime Agency (NCA) have been delivering interventions such as the cease and desist letters and visits by police, as well as participation in Prevent workshops. These interventions are being delivered by the Regional Organised Crime Units, as well as local police. We now collaborate with the National Crime Agency and the Home Office to assess these interventions.

We will start by asking you about which interventions you have received.

- By **intervention** we mean a workshop, police visit, and/or a cease and desist letter.
- A **workshop** refers to a full day accompanied by a parent or guardian which may have included learning about the law, the consequences of breaking the law and opportunities for the positive use of

your skills and interests.

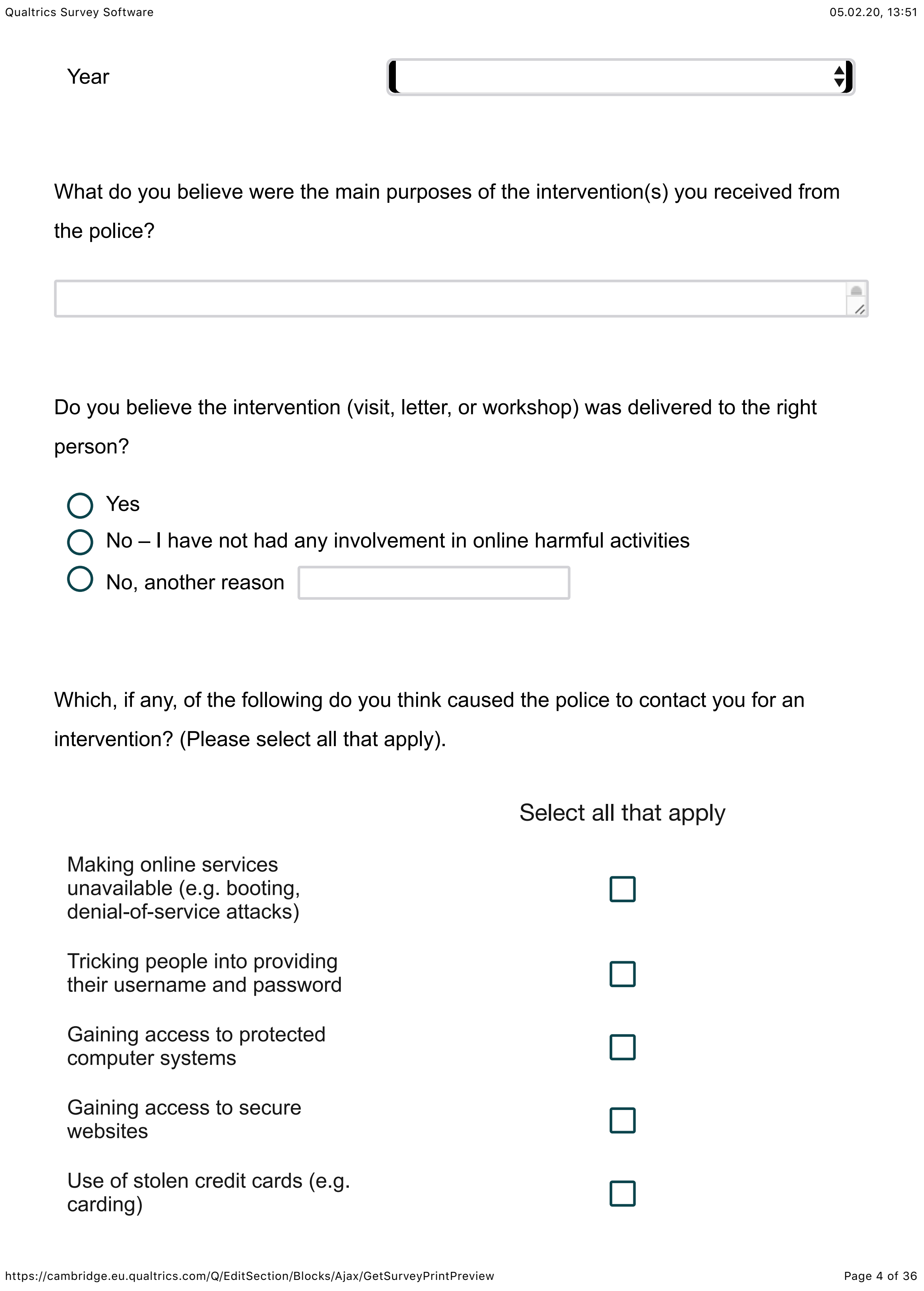
- A **police visit** may have involved the discussion of your cyber activities, the law in this area and advising you on the positive use of your skills and interests, or any activity that the Cyber Prevent Officers introduced you to such as on-line learning, CyberFirst or similar.
- A **Cease and Desist letter** may have been signed as part of a police visit, or one may have been delivered by other means.

Which of the following interventions, if any, have you received from the police? Please indicate how many times you have received these interventions. (Please select all that apply):

	None	Once	Twice	Three times	Four or more times
Workshop	○	○	○	○	○
Police visit and cease and desist letter	○	○	○	○	○
Police visit without cease and desist letter	○	○	○	○	○
A cease and desist letter delivered by other means	○	○	○	○	○
Other	○	○	○	○	○

How long ago was the first contact?

Month



Year ⬍

What do you believe were the main purposes of the intervention(s) you received from the police?

Do you believe the intervention (visit, letter, or workshop) was delivered to the right person?

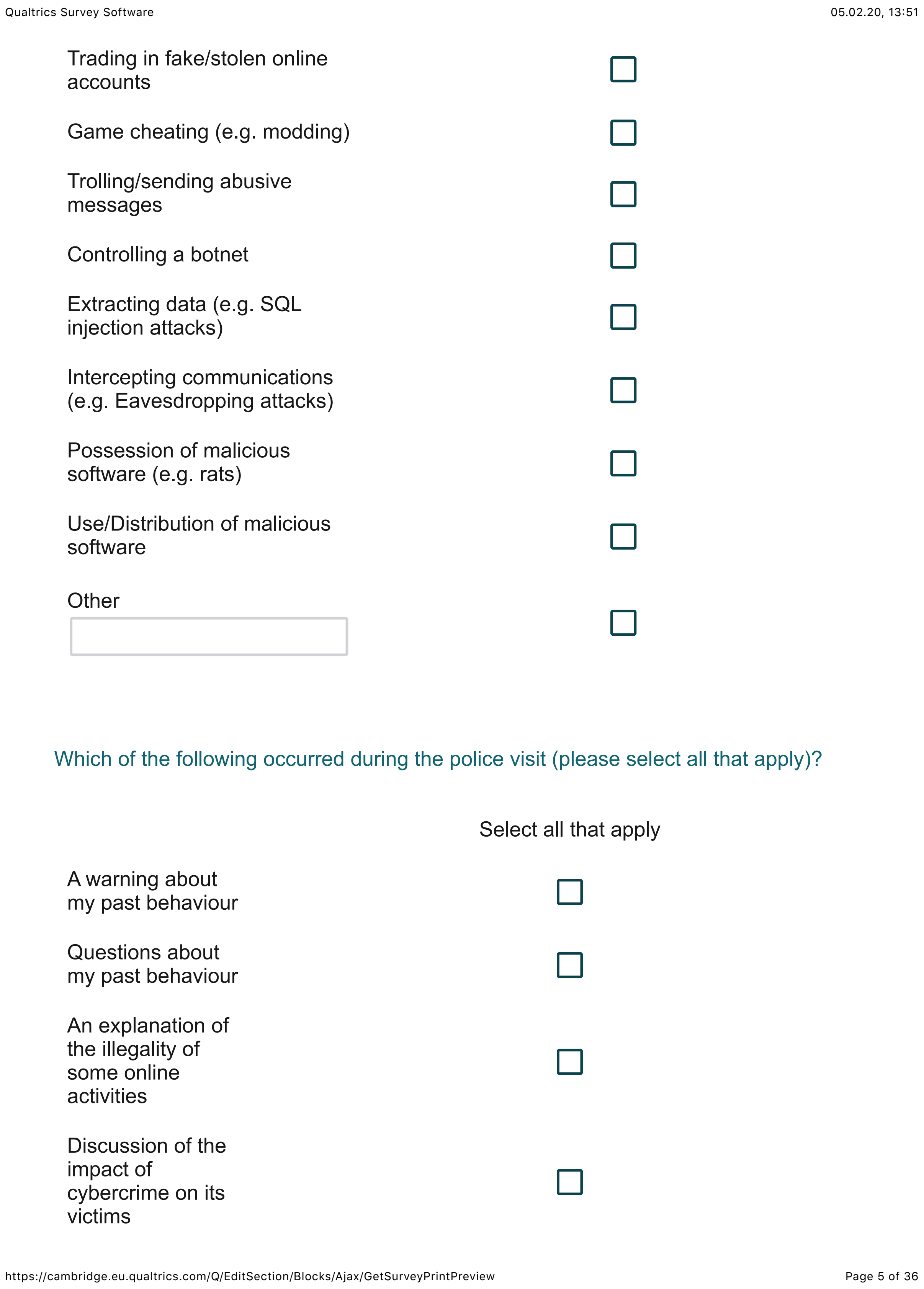
○ Yes

○ No – I have not had any involvement in online harmful activities

○ No, another reason

Which, if any, of the following do you think caused the police to contact you for an intervention? (Please select all that apply).

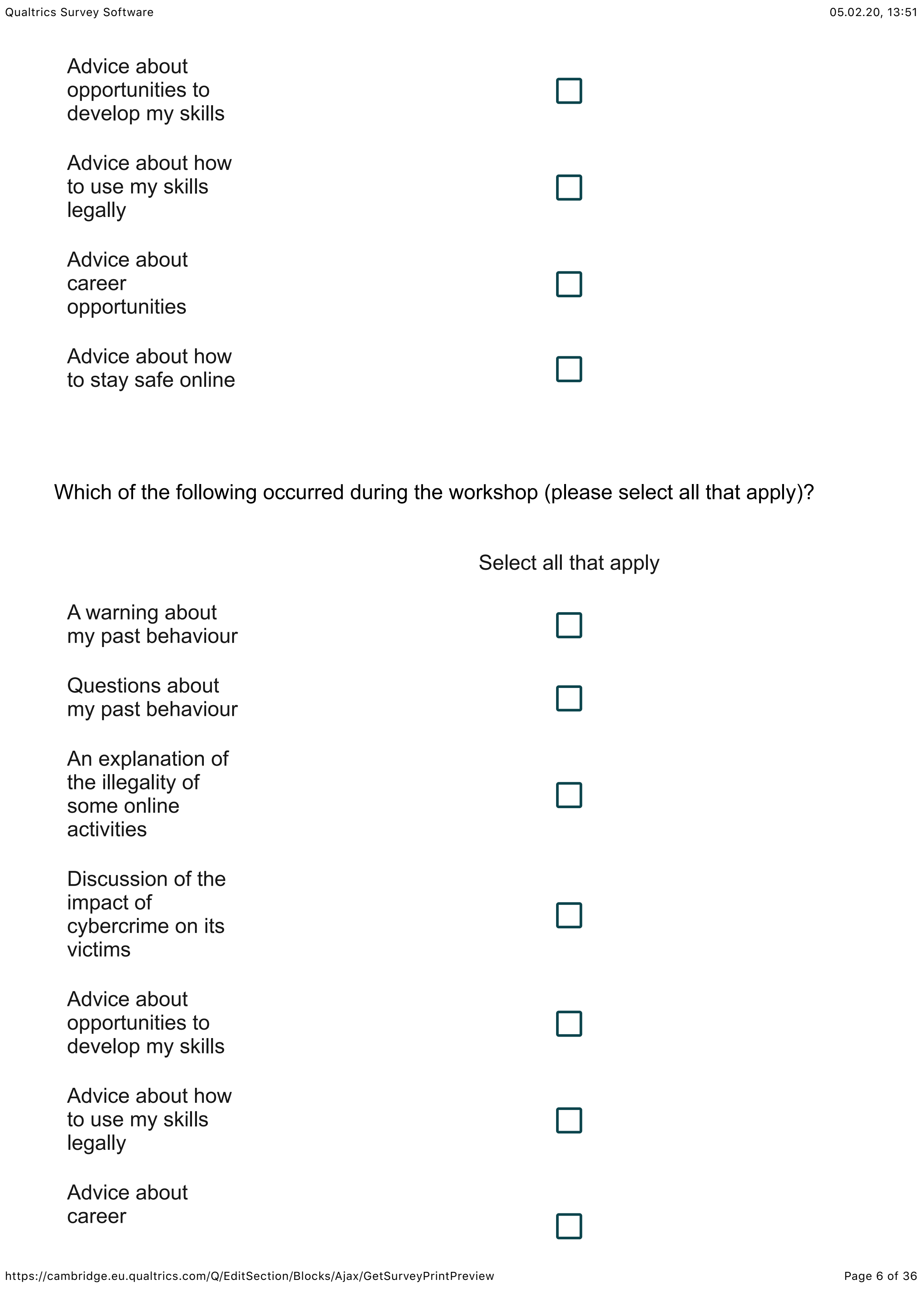
	Select all that apply
Making online services unavailable (e.g. booting, denial-of-service attacks)	□
Tricking people into providing their username and password	□
Gaining access to protected computer systems	□
Gaining access to secure websites	□
Use of stolen credit cards (e.g. carding)	□



Trading in fake/stolen online accounts	□
Game cheating (e.g. modding)	□
Trolling/sending abusive messages	□
Controlling a botnet	□
Extracting data (e.g. SQL injection attacks)	□
Intercepting communications (e.g. Eavesdropping attacks)	□
Possession of malicious software (e.g. rats)	□
Use/Distribution of malicious software	□
Other ▭	□

Which of the following occurred during the police visit (please select all that apply)?

	Select all that apply
A warning about my past behaviour	□
Questions about my past behaviour	□
An explanation of the illegality of some online activities	□
Discussion of the impact of cybercrime on its victims	□



Advice about opportunities to develop my skills	□
Advice about how to use my skills legally	□
Advice about career opportunities	□
Advice about how to stay safe online	□

Which of the following occurred during the workshop (please select all that apply)?

	Select all that apply
A warning about my past behaviour	□
Questions about my past behaviour	□
An explanation of the illegality of some online activities	□
Discussion of the impact of cybercrime on its victims	□
Advice about opportunities to develop my skills	□
Advice about how to use my skills legally	□
Advice about career	□

opportunities	
Advice about how to stay safe online	□

If you received a cease and desist letter, what did you think its purpose was?

How did you feel after the initial visit from the police?

	Not at all	Little	Moderate Amount	Much	Very Much
Angry	○	○	○	○	○
Afraid	○	○	○	○	○
Surprised	○	○	○	○	○
Upset	○	○	○	○	○
Calm	○	○	○	○	○
Disappointed	○	○	○	○	○
Sad	○	○	○	○	○
Other	○	○	○	○	○

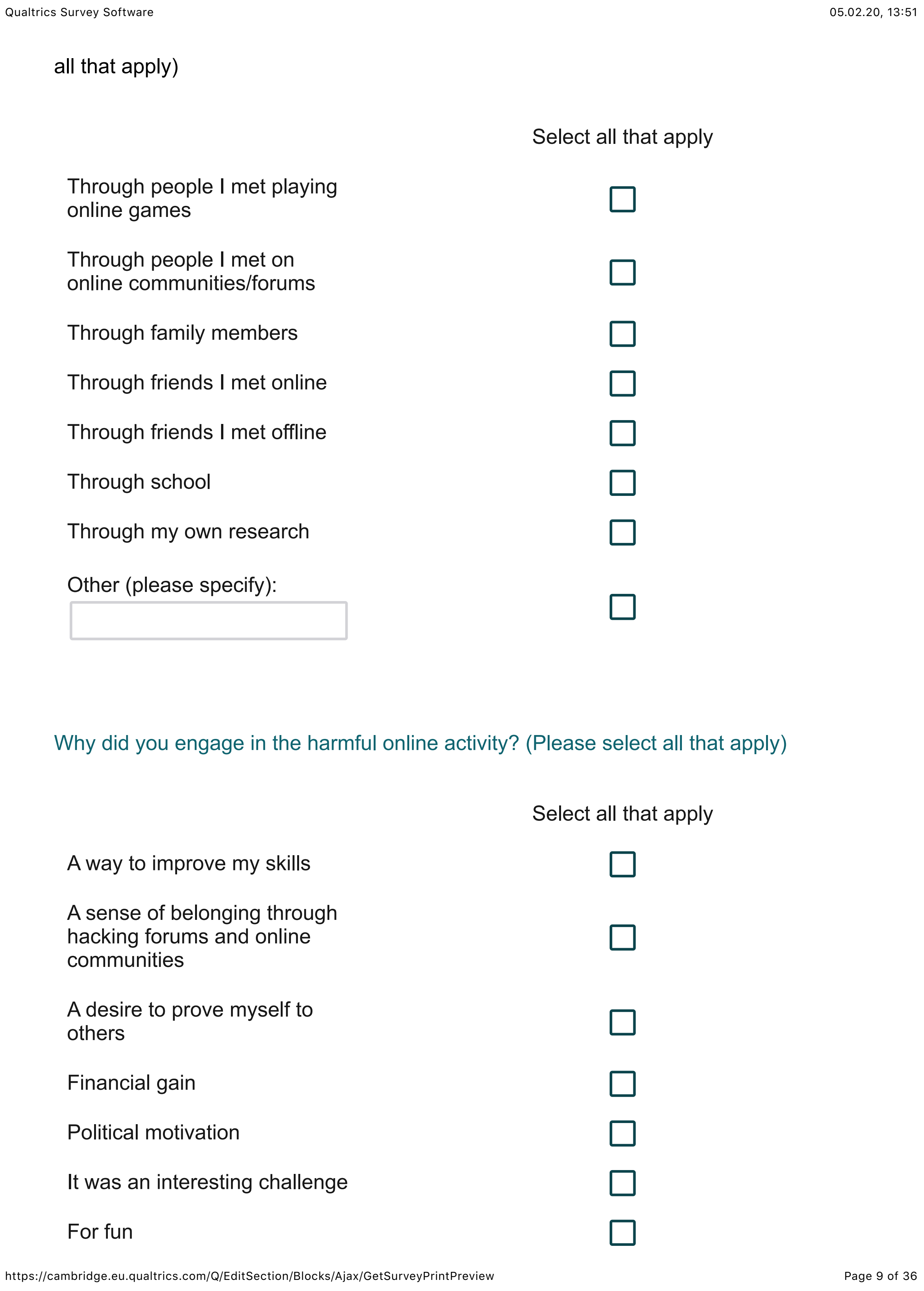
How did you feel after receiving a cease and desist letter from the police? (Multiple Choice)

	Not at all	Little	Moderate Amount	Much	Very Much
Angry	○	○	○	○	○
Afraid	○	○	○	○	○
Surprised	○	○	○	○	○
Upset	○	○	○	○	○
Calm	○	○	○	○	○
Disappointed	○	○	○	○	○
Sad	○	○	○	○	○
Other □	○	○	○	○	○

How did you feel after attending a workshop? (Multiple Choice)

	Not at all	Little	Moderate Amount	Much	Very Much
Angry	○	○	○	○	○
Afraid	○	○	○	○	○
Surprised	○	○	○	○	○
Upset	○	○	○	○	○
Calm	○	○	○	○	○
Disappointed	○	○	○	○	○
Sad	○	○	○	○	○

How did you first become involved in the alleged harmful online activity? (Please select



all that apply)

	Select all that apply
Through people I met playing online games	□
Through people I met on online communities/forums	□
Through family members	□
Through friends I met online	□
Through friends I met offline	□
Through school	□
Through my own research	□
Other (please specify): ________	□

Why did you engage in the harmful online activity? (Please select all that apply)

	Select all that apply
A way to improve my skills	□
A sense of belonging through hacking forums and online communities	□
A desire to prove myself to others	□
Financial gain	□
Political motivation	□
It was an interesting challenge	□
For fun	□

For revenge	□
Other (please specify) ▭	□

How long ago did you become involved in the alleged harmful online activity?

○ Less than one year
○ 1-2 years
○ 3-4 years
○ 5-6 years
○ More than 6 years
○ Don’t know/Not sure

Thank you for making it this far. The next set of questions are about what happened after you received the intervention.

Were your parents/guardians aware of the intervention? (e.g. letter, police visit, workshop)

○ Yes
○ No

If so, what was their response? (Please select all that apply):

	Select all that apply
They were surprised	□
They were supportive	□

They were calm	□
They were disappointed	□
They were upset	□
They were angry	□
Other □	□

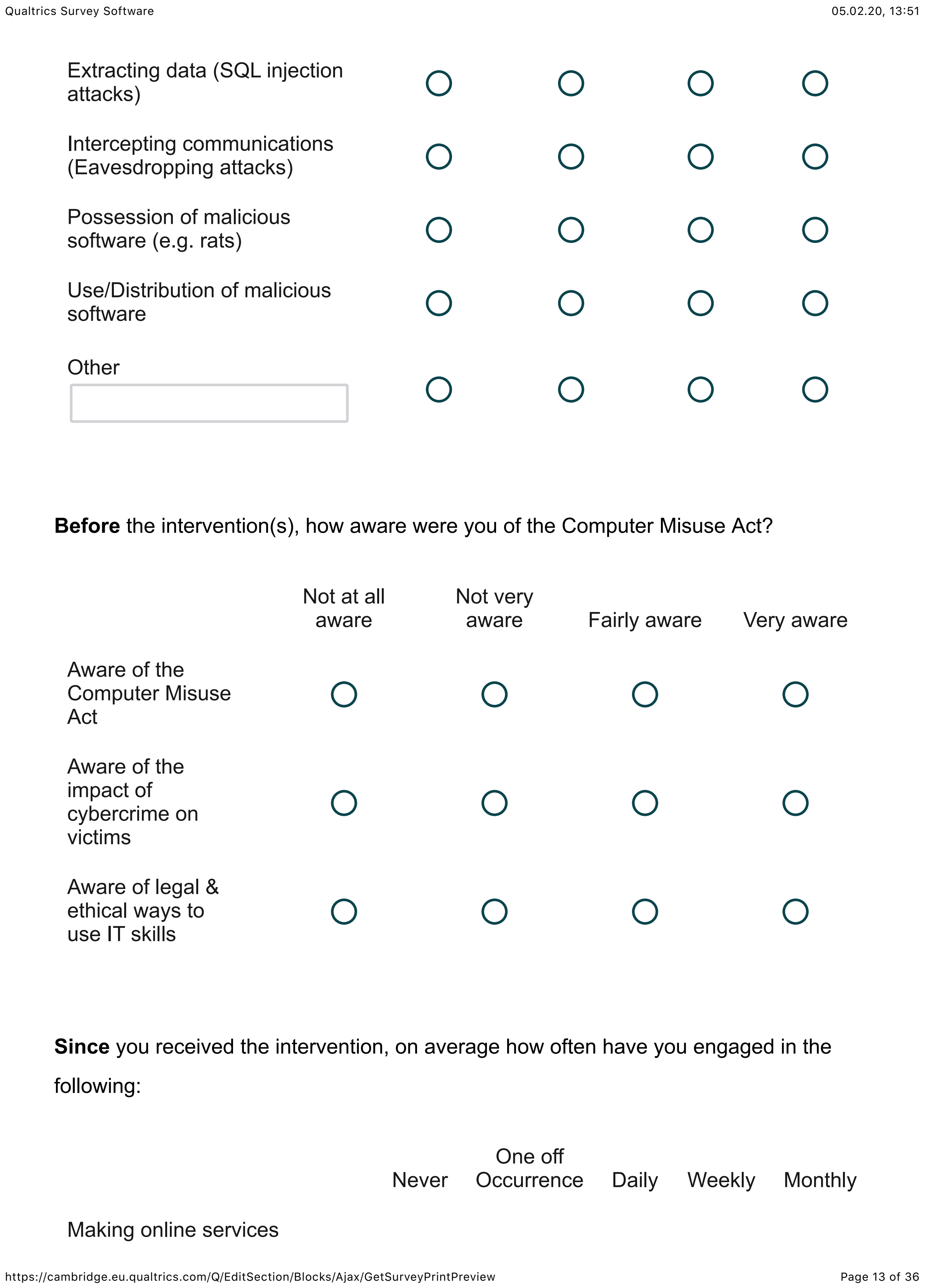
Before the intervention on average, how often did you engage in the following?

	Never	One off Occurrence	Daily	Weekly	Monthly
Making online services unavailable (e.g. booting, denial-of-service attacks)	○	○	○	○	○
Tricking people into providing their username and password	○	○	○	○	○
Gaining access to protected computer systems	○	○	○	○	○
Gaining access to secure websites	○	○	○	○	○
Use of stolen credit cards (e.g. carding)	○	○	○	○	○
Trading in fake/stolen online accounts	○	○	○	○	○
Game cheating (e.g. modding)	○	○	○	○	○
Trolling/sending abusive messages	○	○	○	○	○
Controlling a botnet	○	○	○	○	○
Extracting data (SQL injection attacks)	○	○	○	○	○

Intercepting communications (Eavesdropping attacks)	○	○	○	○	○
Possession of malicious software (e.g. rats)	○	○	○	○	○
Use/Distribution of malicious software	○	○	○	○	○
Other ▭	○	○	○	○	○

Before the intervention, which of the following activities did you think could be illegal?

	Always Illegal	Sometimes Illegal	Never Illegal	Not Sure
Making online services unavailable (e.g. booting, denial-of-service attacks)	○	○	○	○
Tricking people into providing their username and password	○	○	○	○
Gaining access to protected computer systems	○	○	○	○
Gaining access to secure websites	○	○	○	○
Use of stolen credit cards (e.g. carding)	○	○	○	○
Trading in fake/stolen online accounts	○	○	○	○
Game cheating (e.g. modding)	○	○	○	○
Trolling/sending abusive messages	○	○	○	○
Controlling a botnet	○	○	○	○



Qualtrics Survey Software 05.02.20, 13:51

Extracting data (SQL injection attacks)	○	○	○	○
Intercepting communications (Eavesdropping attacks)	○	○	○	○
Possession of malicious software (e.g. rats)	○	○	○	○
Use/Distribution of malicious software	○	○	○	○
Other □	○	○	○	○

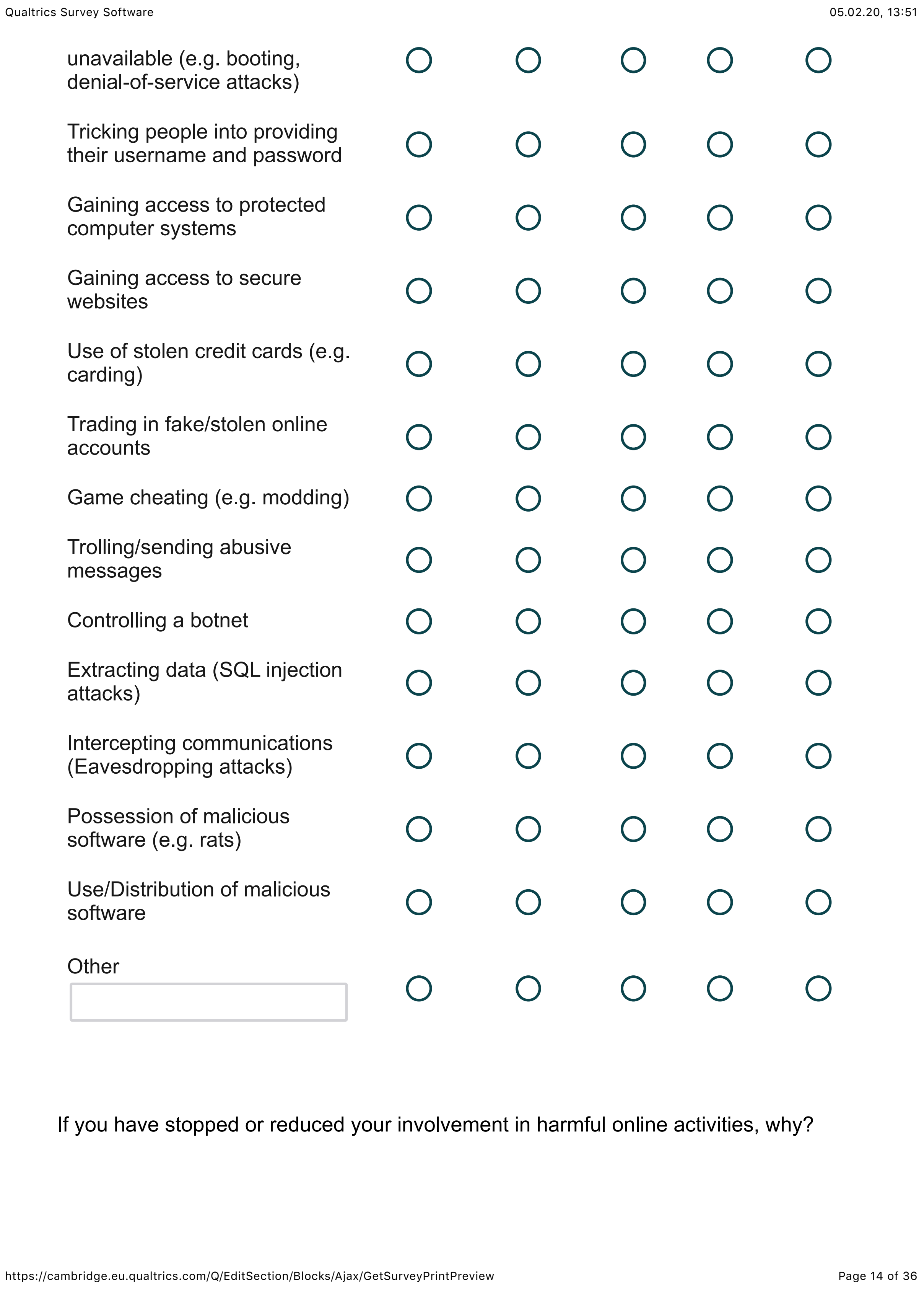
Before the intervention(s), how aware were you of the Computer Misuse Act?

	Not at all aware	Not very aware	Fairly aware	Very aware
Aware of the Computer Misuse Act	○	○	○	○
Aware of the impact of cybercrime on victims	○	○	○	○
Aware of legal & ethical ways to use IT skills	○	○	○	○

Since you received the intervention, on average how often have you engaged in the following:

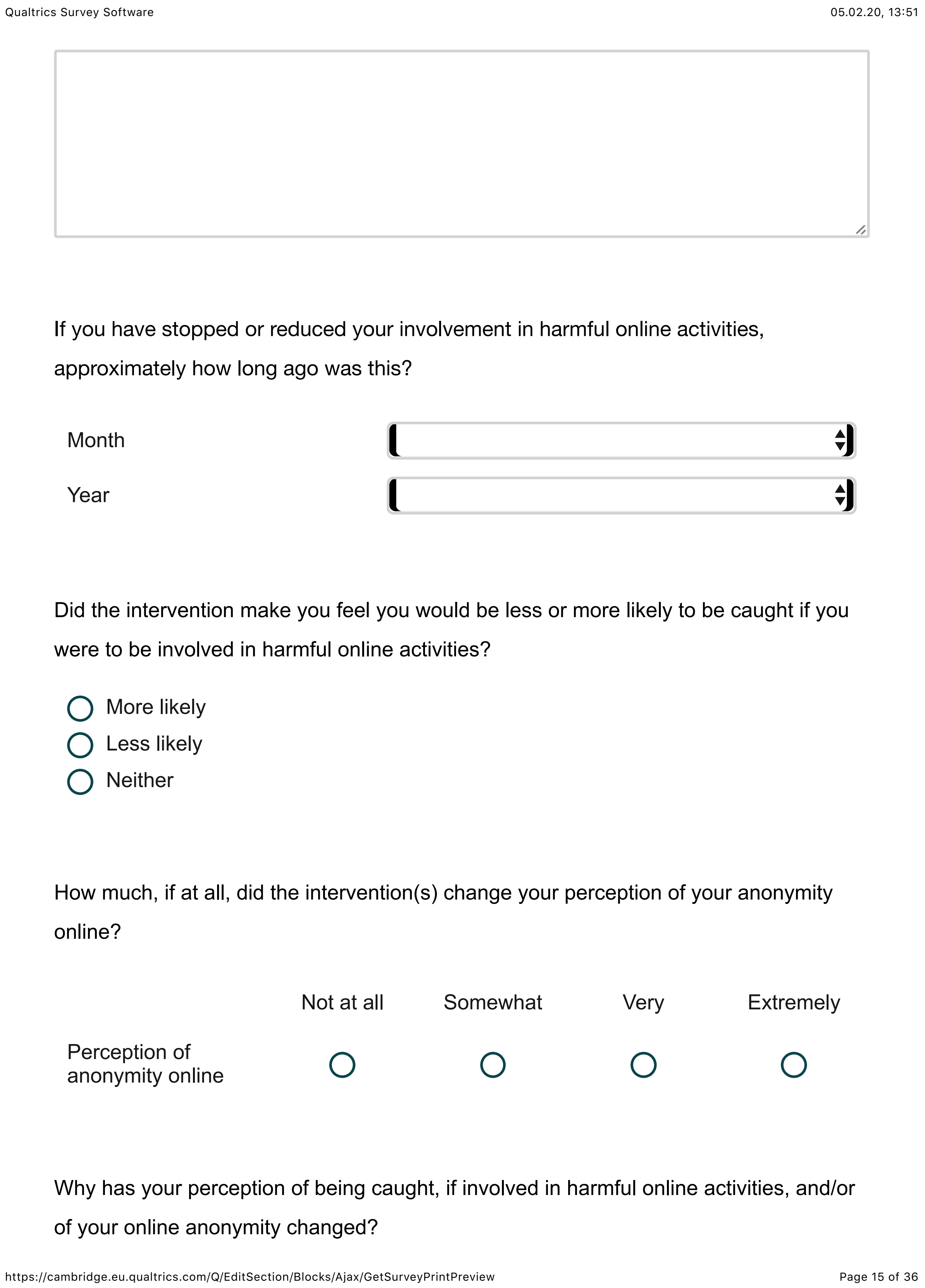
	Never	One off Occurrence	Daily	Weekly	Monthly
Making online services					

https://cambridge.eu.qualtrics.com/Q/EditSection/Blocks/Ajax/GetSurveyPrintPreview Page 13 of 36



unavailable (e.g. booting, denial-of-service attacks)	○	○	○	○	○
Tricking people into providing their username and password	○	○	○	○	○
Gaining access to protected computer systems	○	○	○	○	○
Gaining access to secure websites	○	○	○	○	○
Use of stolen credit cards (e.g. carding)	○	○	○	○	○
Trading in fake/stolen online accounts	○	○	○	○	○
Game cheating (e.g. modding)	○	○	○	○	○
Trolling/sending abusive messages	○	○	○	○	○
Controlling a botnet	○	○	○	○	○
Extracting data (SQL injection attacks)	○	○	○	○	○
Intercepting communications (Eavesdropping attacks)	○	○	○	○	○
Possession of malicious software (e.g. rats)	○	○	○	○	○
Use/Distribution of malicious software	○	○	○	○	○
Other □	○	○	○	○	○

If you have stopped or reduced your involvement in harmful online activities, why?



If you have stopped or reduced your involvement in harmful online activities, approximately how long ago was this?

Month	
Year	

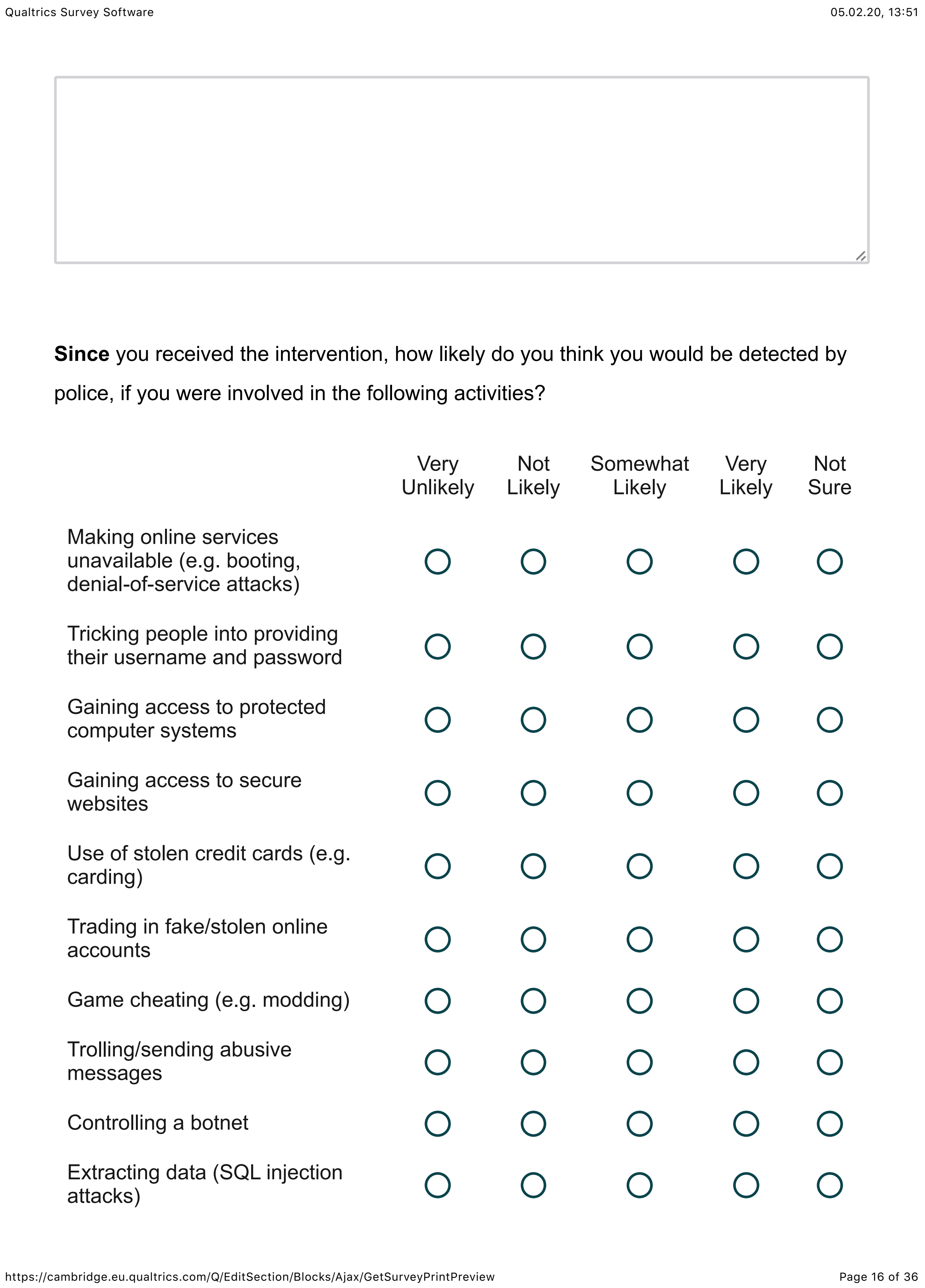
Did the intervention make you feel you would be less or more likely to be caught if you were to be involved in harmful online activities?

○ More likely
○ Less likely
○ Neither

How much, if at all, did the intervention(s) change your perception of your anonymity online?

	Not at all	Somewhat	Very	Extremely
Perception of anonymity online	○	○	○	○

Why has your perception of being caught, if involved in harmful online activities, and/or of your online anonymity changed?



Qualtrics Survey Software 05.02.20, 13:51

Since you received the intervention, how likely do you think you would be detected by police, if you were involved in the following activities?

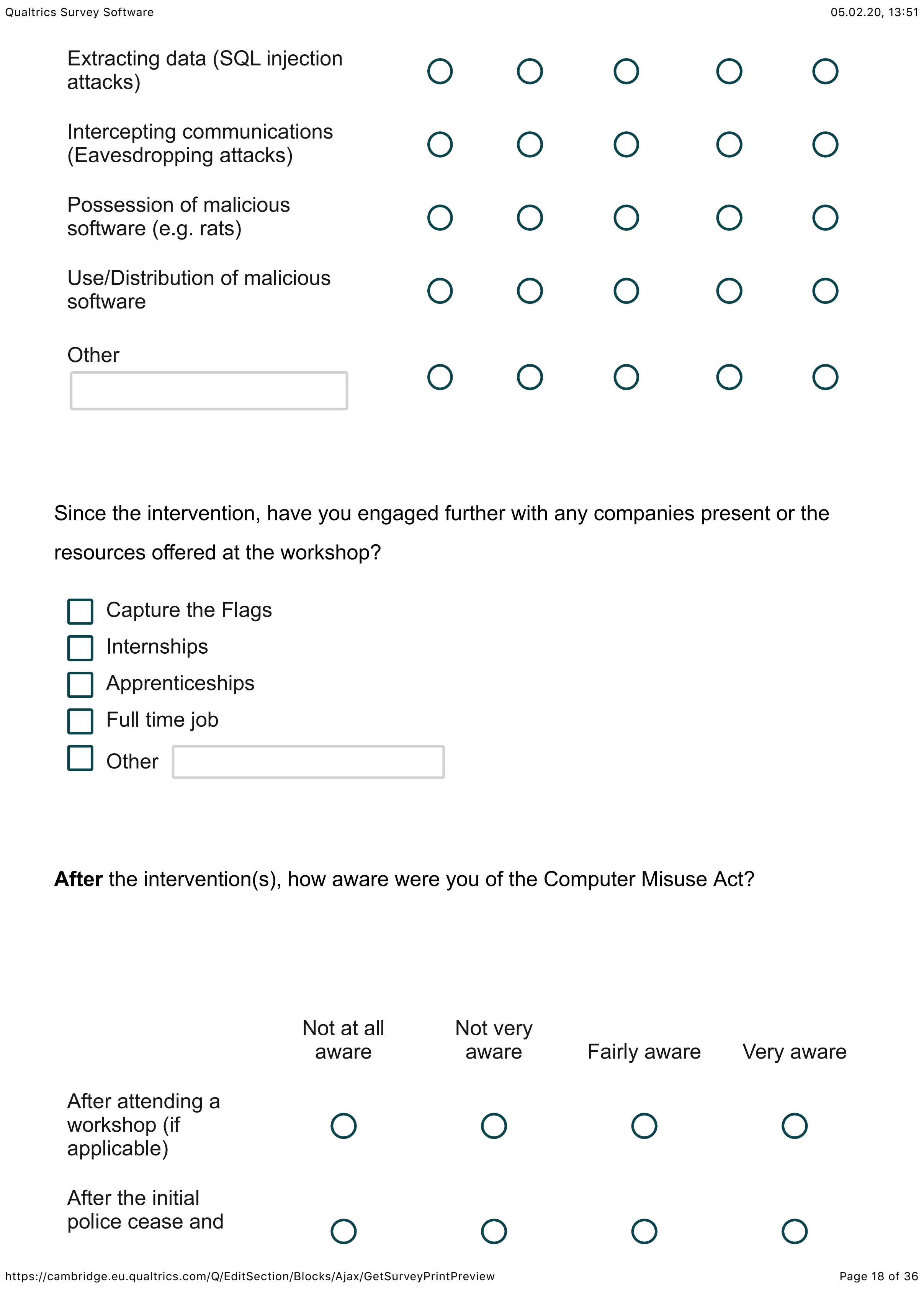
	Very Unlikely	Not Likely	Somewhat Likely	Very Likely	Not Sure
Making online services unavailable (e.g. booting, denial-of-service attacks)	○	○	○	○	○
Tricking people into providing their username and password	○	○	○	○	○
Gaining access to protected computer systems	○	○	○	○	○
Gaining access to secure websites	○	○	○	○	○
Use of stolen credit cards (e.g. carding)	○	○	○	○	○
Trading in fake/stolen online accounts	○	○	○	○	○
Game cheating (e.g. modding)	○	○	○	○	○
Trolling/sending abusive messages	○	○	○	○	○
Controlling a botnet	○	○	○	○	○
Extracting data (SQL injection attacks)	○	○	○	○	○

https://cambridge.eu.qualtrics.com/Q/EditSection/Blocks/Ajax/GetSurveyPrintPreview Page 16 of 36

Intercepting communications (Eavesdropping attacks)	○	○	○	○	○
Possession of malicious software (e.g. rats)	○	○	○	○	○
Use/Distribution of malicious software	○	○	○	○	○
Other □	○	○	○	○	○

If you were caught being involved in the following activities, how severe do you think the consequences would be?

	Very Light	Light	Severe	Very Severe	Not Sure
Making online services unavailable (e.g. booting, denial-of-service attacks)	○	○	○	○	○
Tricking people into providing their username and password	○	○	○	○	○
Gaining access to protected computer systems	○	○	○	○	○
Gaining access to secure websites	○	○	○	○	○
Use of stolen credit cards (e.g. carding)	○	○	○	○	○
Trading in fake/stolen online accounts	○	○	○	○	○
Game cheating (e.g. modding)	○	○	○	○	○
Trolling/sending abusive messages	○	○	○	○	○
Controlling a botnet	○	○	○	○	○



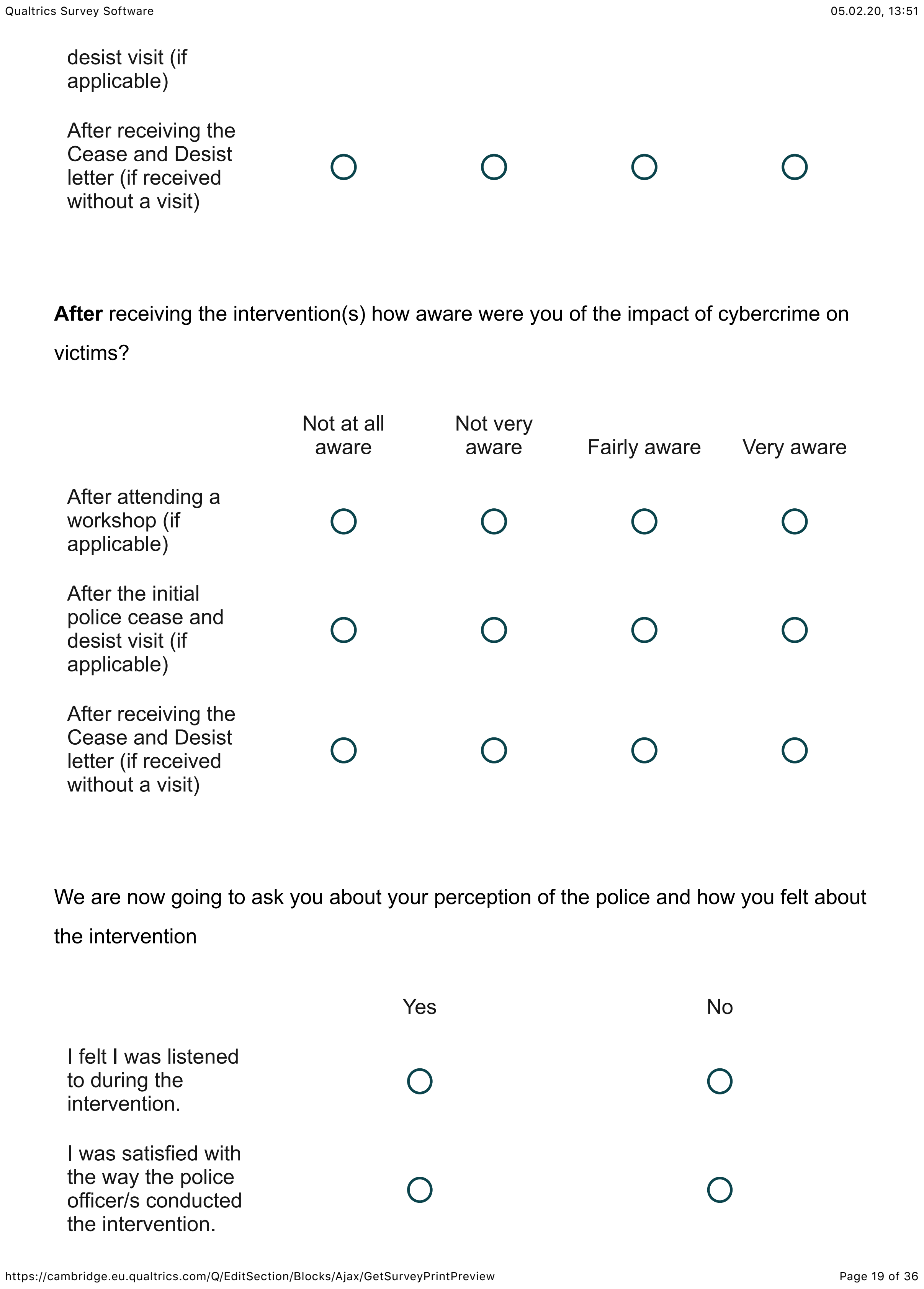
Extracting data (SQL injection attacks)	○	○	○	○	○
Intercepting communications (Eavesdropping attacks)	○	○	○	○	○
Possession of malicious software (e.g. rats)	○	○	○	○	○
Use/Distribution of malicious software	○	○	○	○	○
Other ▭	○	○	○	○	○

Since the intervention, have you engaged further with any companies present or the resources offered at the workshop?

□ Capture the Flags
□ Internships
□ Apprenticeships
□ Full time job
□ Other ▭

After the intervention(s), how aware were you of the Computer Misuse Act?

	Not at all aware	Not very aware	Fairly aware	Very aware
After attending a workshop (if applicable)	○	○	○	○
After the initial police cease and	○	○	○	○



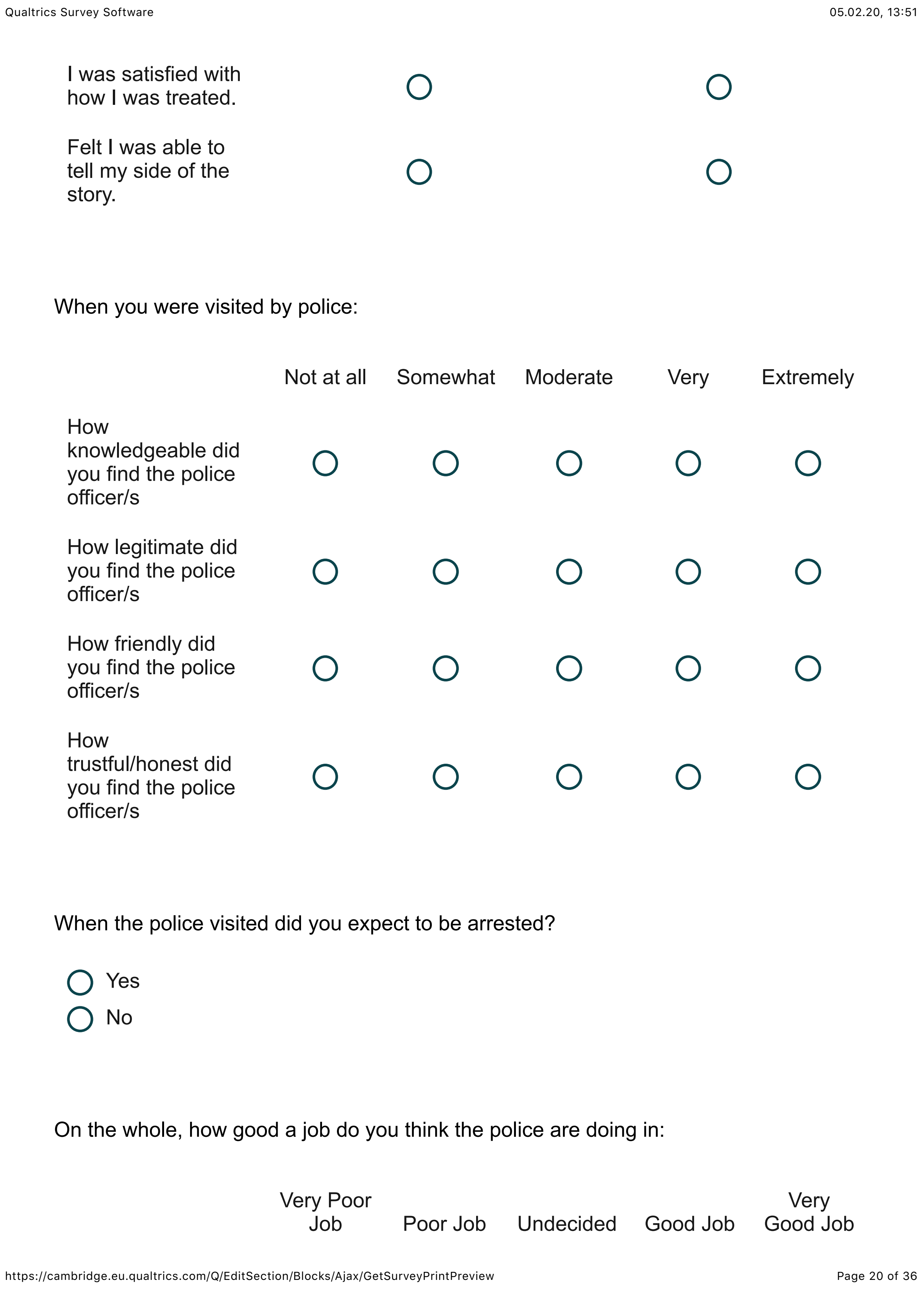
desist visit (if applicable)				
After receiving the Cease and Desist letter (if received without a visit)	○	○	○	○

After receiving the intervention(s) how aware were you of the impact of cybercrime on victims?

	Not at all aware	Not very aware	Fairly aware	Very aware
After attending a workshop (if applicable)	○	○	○	○
After the initial police cease and desist visit (if applicable)	○	○	○	○
After receiving the Cease and Desist letter (if received without a visit)	○	○	○	○

We are now going to ask you about your perception of the police and how you felt about the intervention

	Yes	No
I felt I was listened to during the intervention.	○	○
I was satisfied with the way the police officer/s conducted the intervention.	○	○



I was satisfied with how I was treated.	○	○
Felt I was able to tell my side of the story.	○	○

When you were visited by police:

	Not at all	Somewhat	Moderate	Very	Extremely
How knowledgeable did you find the police officer/s	○	○	○	○	○
How legitimate did you find the police officer/s	○	○	○	○	○
How friendly did you find the police officer/s	○	○	○	○	○
How trustful/honest did you find the police officer/s	○	○	○	○	○

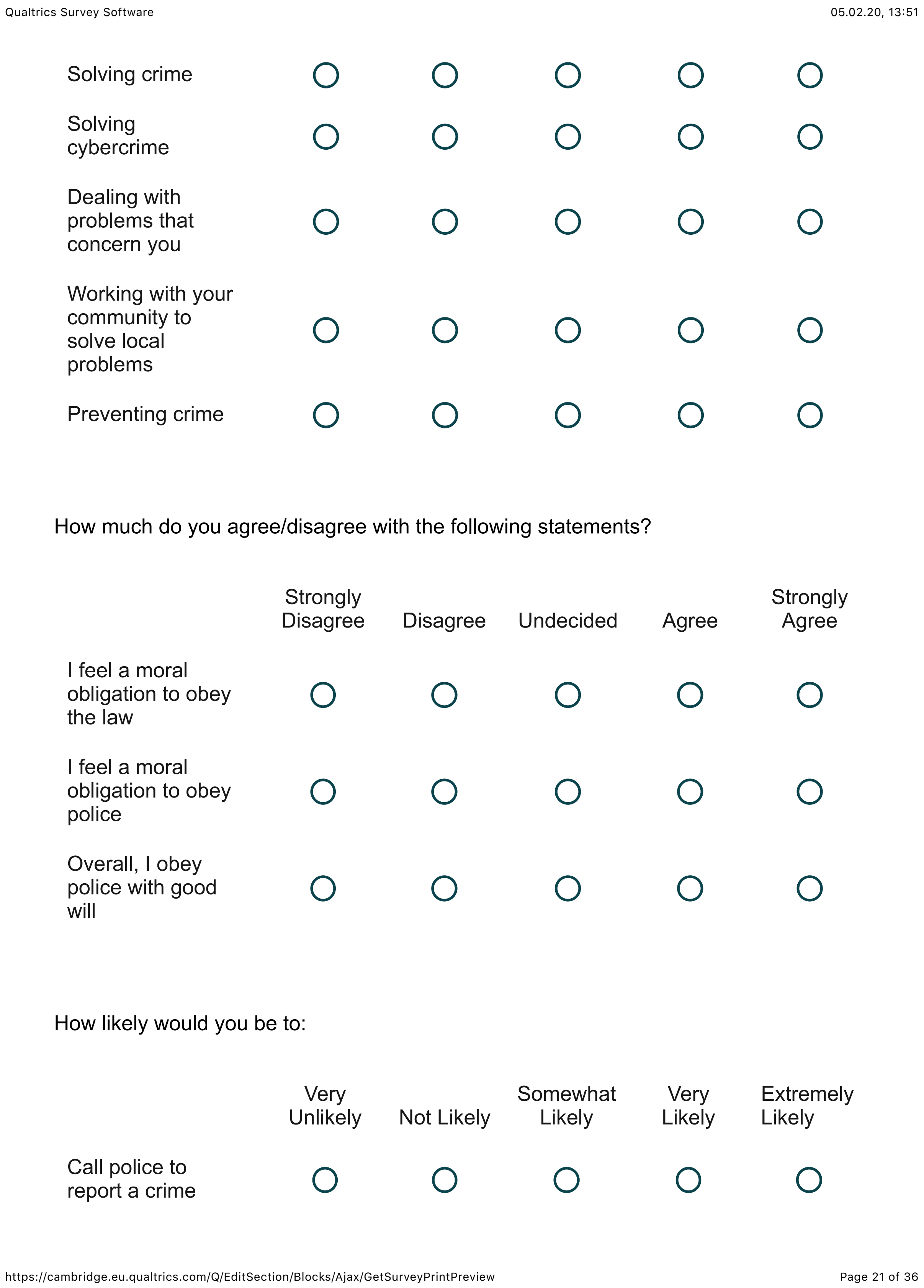
When the police visited did you expect to be arrested?

○ Yes

○ No

On the whole, how good a job do you think the police are doing in:

	Very Poor Job	Poor Job	Undecided	Good Job	Very Good Job



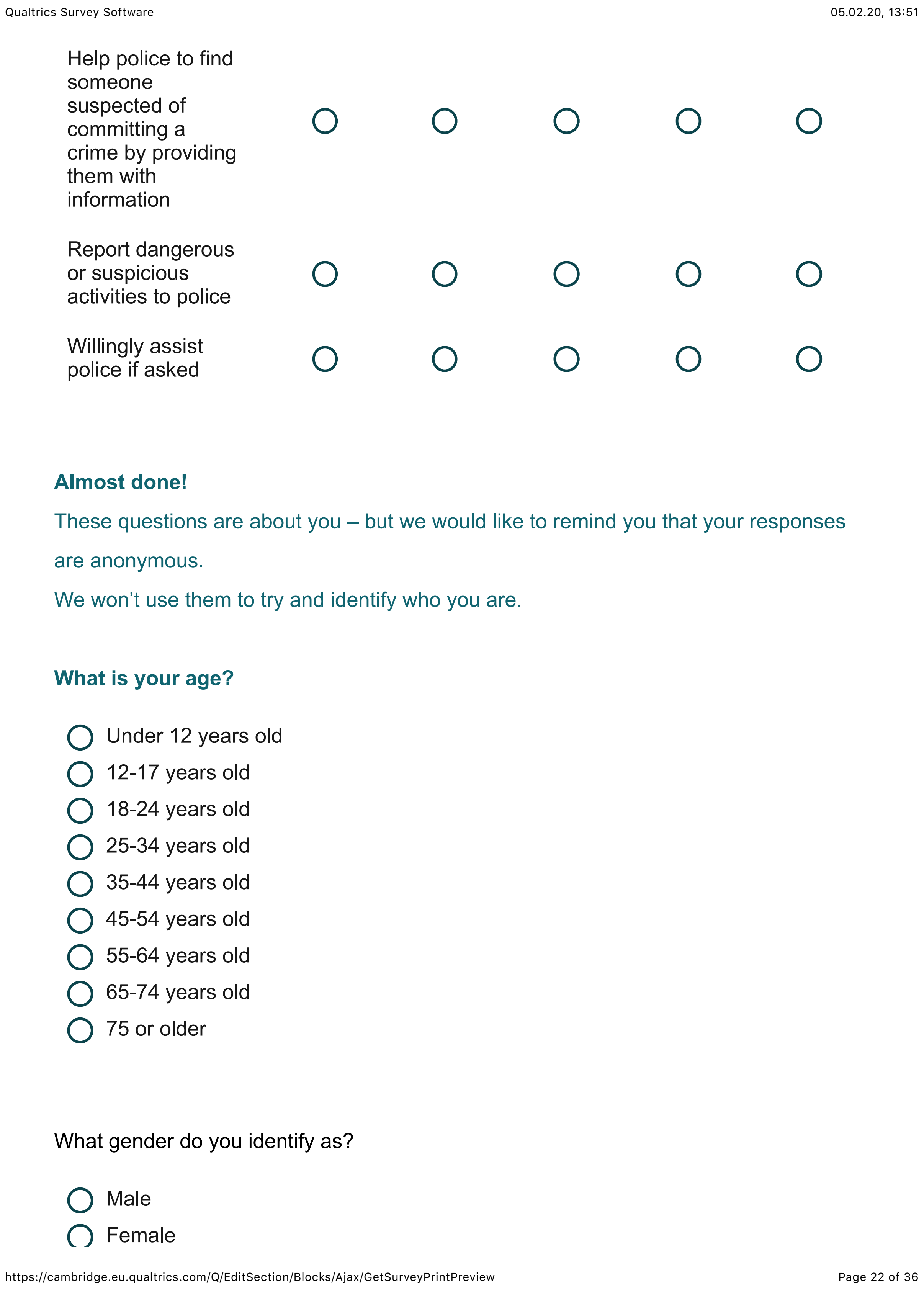
Solving crime	○	○	○	○	○
Solving cybercrime	○	○	○	○	○
Dealing with problems that concern you	○	○	○	○	○
Working with your community to solve local problems	○	○	○	○	○
Preventing crime	○	○	○	○	○

How much do you agree/disagree with the following statements?

	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree
I feel a moral obligation to obey the law	○	○	○	○	○
I feel a moral obligation to obey police	○	○	○	○	○
Overall, I obey police with good will	○	○	○	○	○

How likely would you be to:

	Very Unlikely	Not Likely	Somewhat Likely	Very Likely	Extremely Likely
Call police to report a crime	○	○	○	○	○



Help police to find someone suspected of committing a crime by providing them with information	○	○	○	○	○
Report dangerous or suspicious activities to police	○	○	○	○	○
Willingly assist police if asked	○	○	○	○	○

Almost done!

These questions are about you – but we would like to remind you that your responses are anonymous.

We won't use them to try and identify who you are.

What is your age?

○ Under 12 years old
○ 12-17 years old
○ 18-24 years old
○ 25-34 years old
○ 35-44 years old
○ 45-54 years old
○ 55-64 years old
○ 65-74 years old
○ 75 or older

What gender do you identify as?

○ Male
○ Female

○ Other ▭

What's your current relationship status?

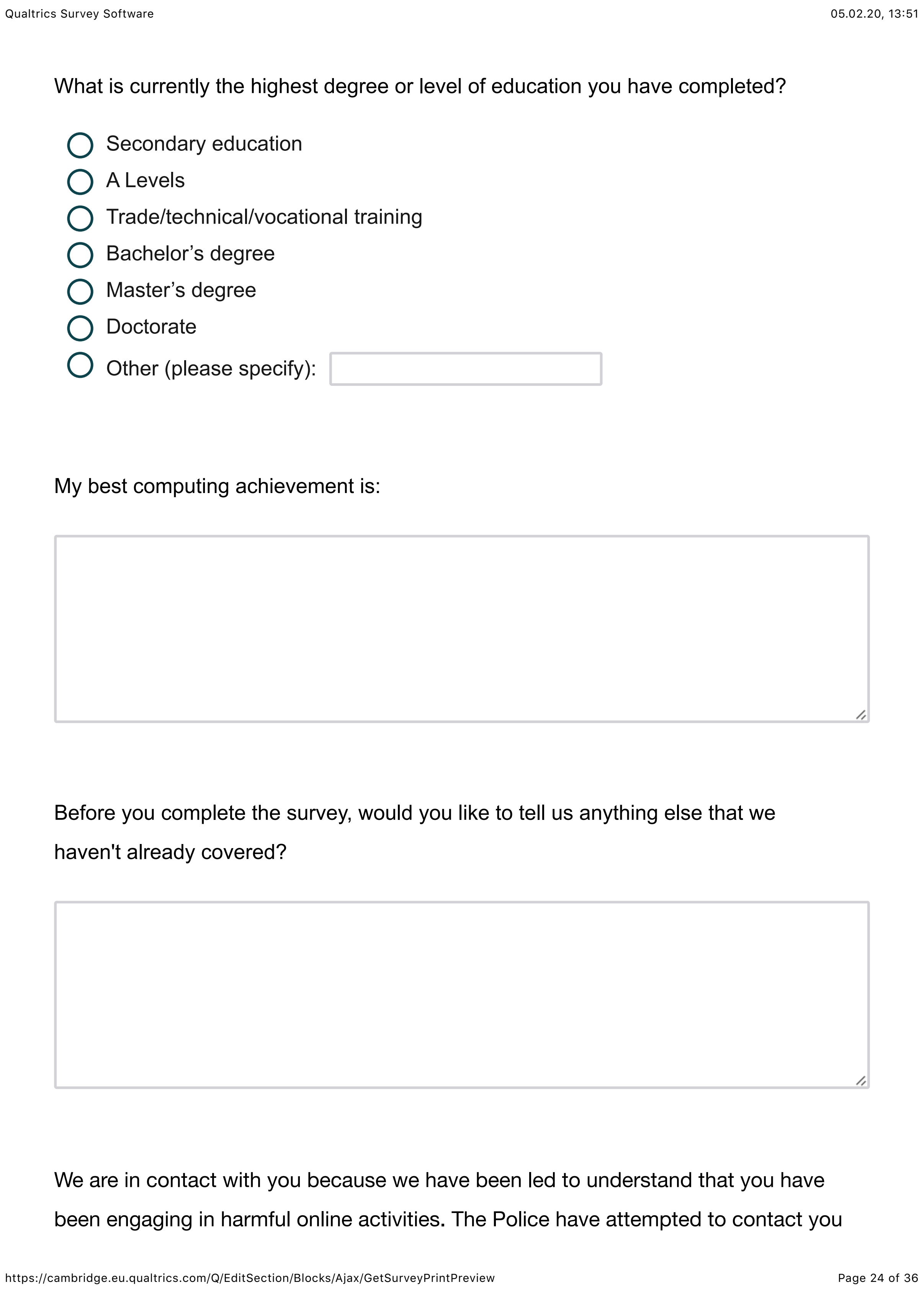
○ Single
○ In a relationship
○ Engaged
○ Married

What is your current employment status?

○ Employed full-time
○ Employed part-time
○ Unemployed (currently looking for work)
○ Student
○ Retired
○ Self-employed
○ Unable to work
○ Other ▭

How would you rate your technical skills?

○ Basic (e.g. I don't use computers or smart devices unless I absolutely have to)
○ Below proficient (e.g. I can use Internet, common software, but cannot fix computer problems)
○ Proficient (e.g. I know some computer programming languages and can fix most computer problems)
○ Advanced (e.g. I am proficient in multiple programming languages, and can create my own apps)



Qualtrics Survey Software 05.02.20, 13:51

What is currently the highest degree or level of education you have completed?

○ Secondary education
○ A Levels
○ Trade/technical/vocational training
○ Bachelor’s degree
○ Master’s degree
○ Doctorate
○ Other (please specify): □

My best computing achievement is:

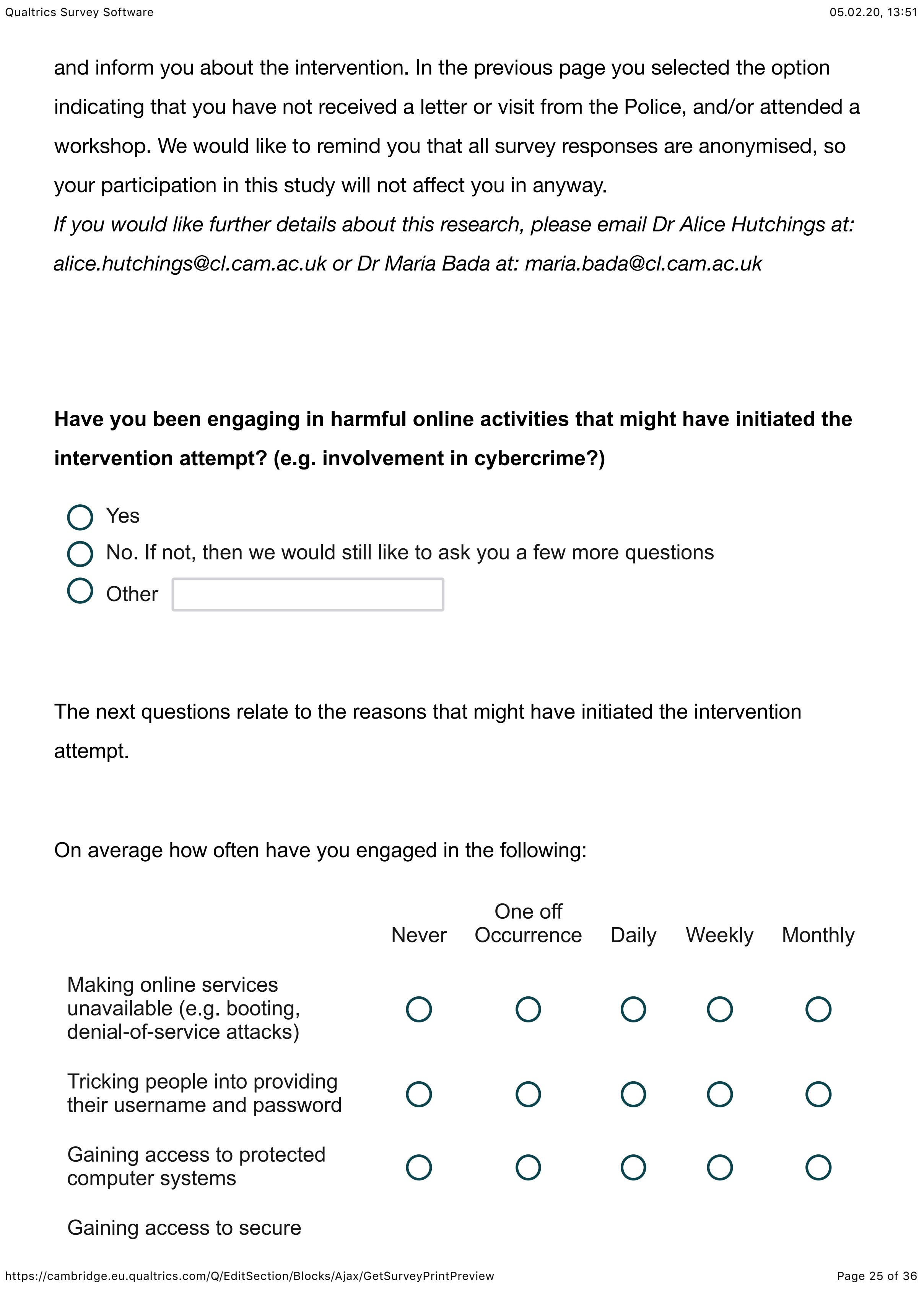
□

Before you complete the survey, would you like to tell us anything else that we haven't already covered?

□

We are in contact with you because we have been led to understand that you have been engaging in harmful online activities. The Police have attempted to contact you

https://cambridge.eu.qualtrics.com/Q/EditSection/Blocks/Ajax/GetSurveyPrintPreview Page 24 of 36



and inform you about the intervention. In the previous page you selected the option indicating that you have not received a letter or visit from the Police, and/or attended a workshop. We would like to remind you that all survey responses are anonymised, so your participation in this study will not affect you in anyway.

If you would like further details about this research, please email Dr Alice Hutchings at: alice.hutchings@cl.cam.ac.uk or Dr Maria Bada at: maria.bada@cl.cam.ac.uk

Have you been engaging in harmful online activities that might have initiated the intervention attempt? (e.g. involvement in cybercrime?)

○ Yes
○ No. If not, then we would still like to ask you a few more questions
○ Other ▭

The next questions relate to the reasons that might have initiated the intervention attempt.

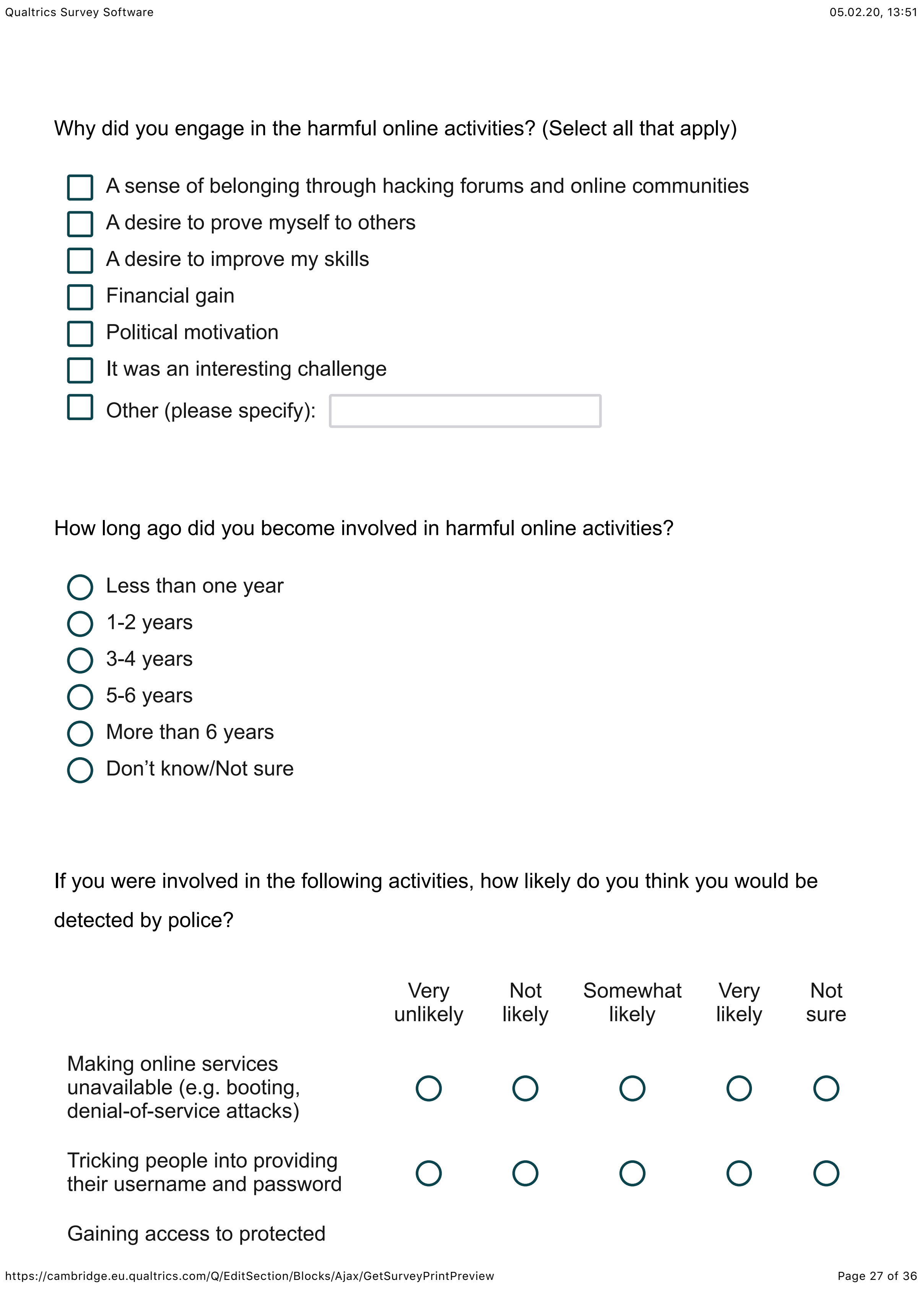
On average how often have you engaged in the following:

	Never	One off Occurrence	Daily	Weekly	Monthly
Making online services unavailable (e.g. booting, denial-of-service attacks)	○	○	○	○	○
Tricking people into providing their username and password	○	○	○	○	○
Gaining access to protected computer systems	○	○	○	○	○
Gaining access to secure					

websites	○	○	○	○	○
Use of stolen credit cards (e.g. carding)	○	○	○	○	○
Trading in fake/stolen online accounts	○	○	○	○	○
Game cheating (e.g. modding)	○	○	○	○	○
Trolling/sending abusive messages	○	○	○	○	○
Controlling a botnet	○	○	○	○	○
Extracting data (SQL injection attacks)	○	○	○	○	○
Intercepting communications (Eavesdropping attacks)	○	○	○	○	○
Possession of malicious software (e.g. rats)	○	○	○	○	○
Use/Distribution of malicious software	○	○	○	○	○
Other	○	○	○	○	○

How did you first become involved in the alleged harmful online activity? (Select all that apply)

□ Through people I met playing online games
□ People I met on online communities/forums
□ Through family members
□ Through friends
□ Through school
□ Through my own research
□ Other (please specify):



Why did you engage in the harmful online activities? (Select all that apply)

□ A sense of belonging through hacking forums and online communities
□ A desire to prove myself to others
□ A desire to improve my skills
□ Financial gain
□ Political motivation
□ It was an interesting challenge
□ Other (please specify): ______

How long ago did you become involved in harmful online activities?

○ Less than one year
○ 1-2 years
○ 3-4 years
○ 5-6 years
○ More than 6 years
○ Don’t know/Not sure

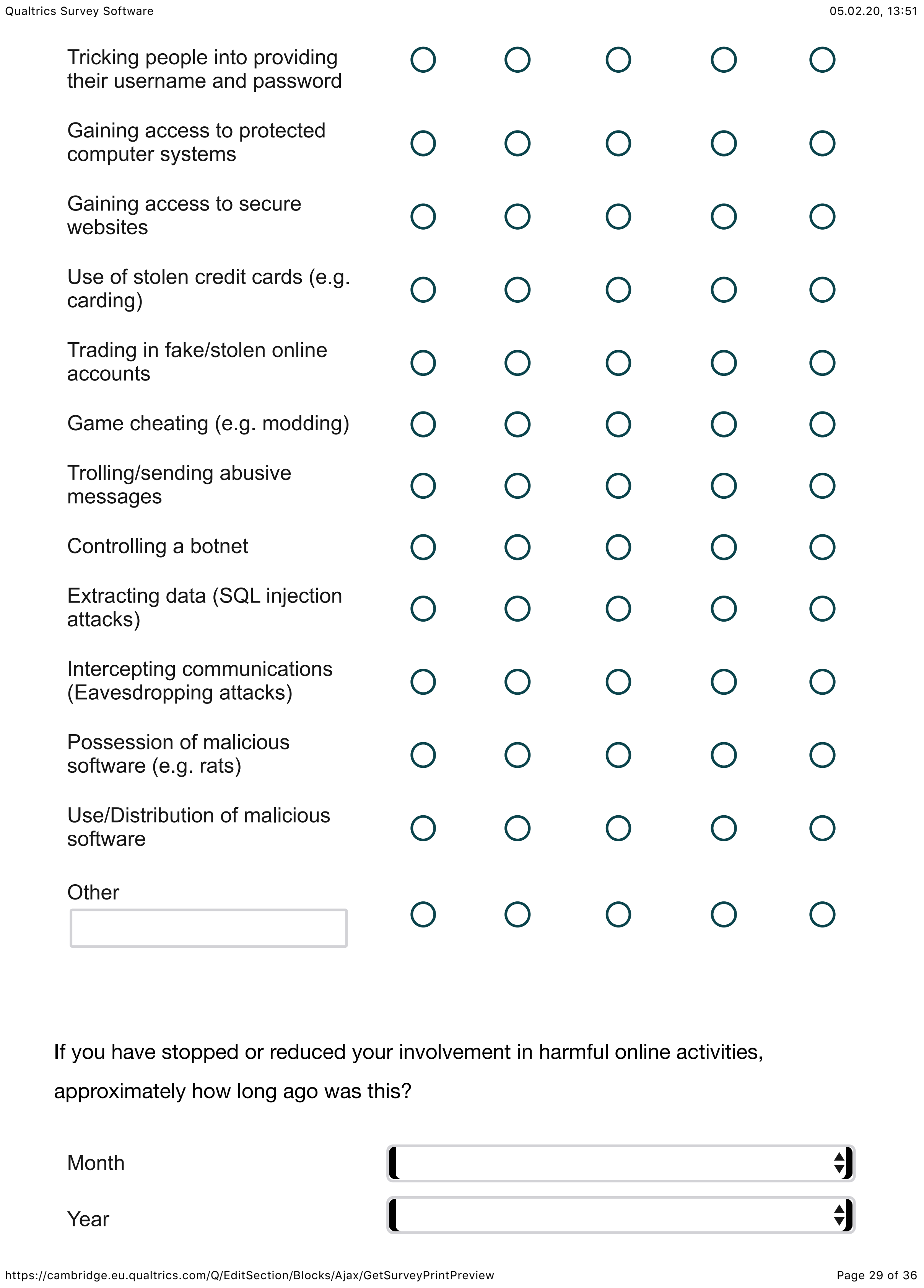
If you were involved in the following activities, how likely do you think you would be detected by police?

	Very unlikely	Not likely	Somewhat likely	Very likely	Not sure
Making online services unavailable (e.g. booting, denial-of-service attacks)	○	○	○	○	○
Tricking people into providing their username and password	○	○	○	○	○
Gaining access to protected					

computer systems	○	○	○	○	○
Gaining access to secure websites	○	○	○	○	○
Use of stolen credit cards (e.g. carding)	○	○	○	○	○
Trading in fake/stolen online accounts	○	○	○	○	○
Game cheating (e.g. modding)	○	○	○	○	○
Trolling/sending abusive messages	○	○	○	○	○
Controlling a botnet	○	○	○	○	○
Extracting data (SQL injection attacks)	○	○	○	○	○
Intercepting communications (Eavesdropping attacks)	○	○	○	○	○
Possession of malicious software (e.g. rats)	○	○	○	○	○
Use/Distribution of malicious software	○	○	○	○	○
Other ☐	○	○	○	○	○

If you were caught being involved in the following activities, how severe do you think the consequences would be?

	Very light	Light	Severe	Very severe	Not sure
Making online services unavailable (e.g. booting, denial-of-service attacks)	○	○	○	○	○



Tricking people into providing their username and password	○	○	○	○	○
Gaining access to protected computer systems	○	○	○	○	○
Gaining access to secure websites	○	○	○	○	○
Use of stolen credit cards (e.g. carding)	○	○	○	○	○
Trading in fake/stolen online accounts	○	○	○	○	○
Game cheating (e.g. modding)	○	○	○	○	○
Trolling/sending abusive messages	○	○	○	○	○
Controlling a botnet	○	○	○	○	○
Extracting data (SQL injection attacks)	○	○	○	○	○
Intercepting communications (Eavesdropping attacks)	○	○	○	○	○
Possession of malicious software (e.g. rats)	○	○	○	○	○
Use/Distribution of malicious software	○	○	○	○	○
Other □	○	○	○	○	○

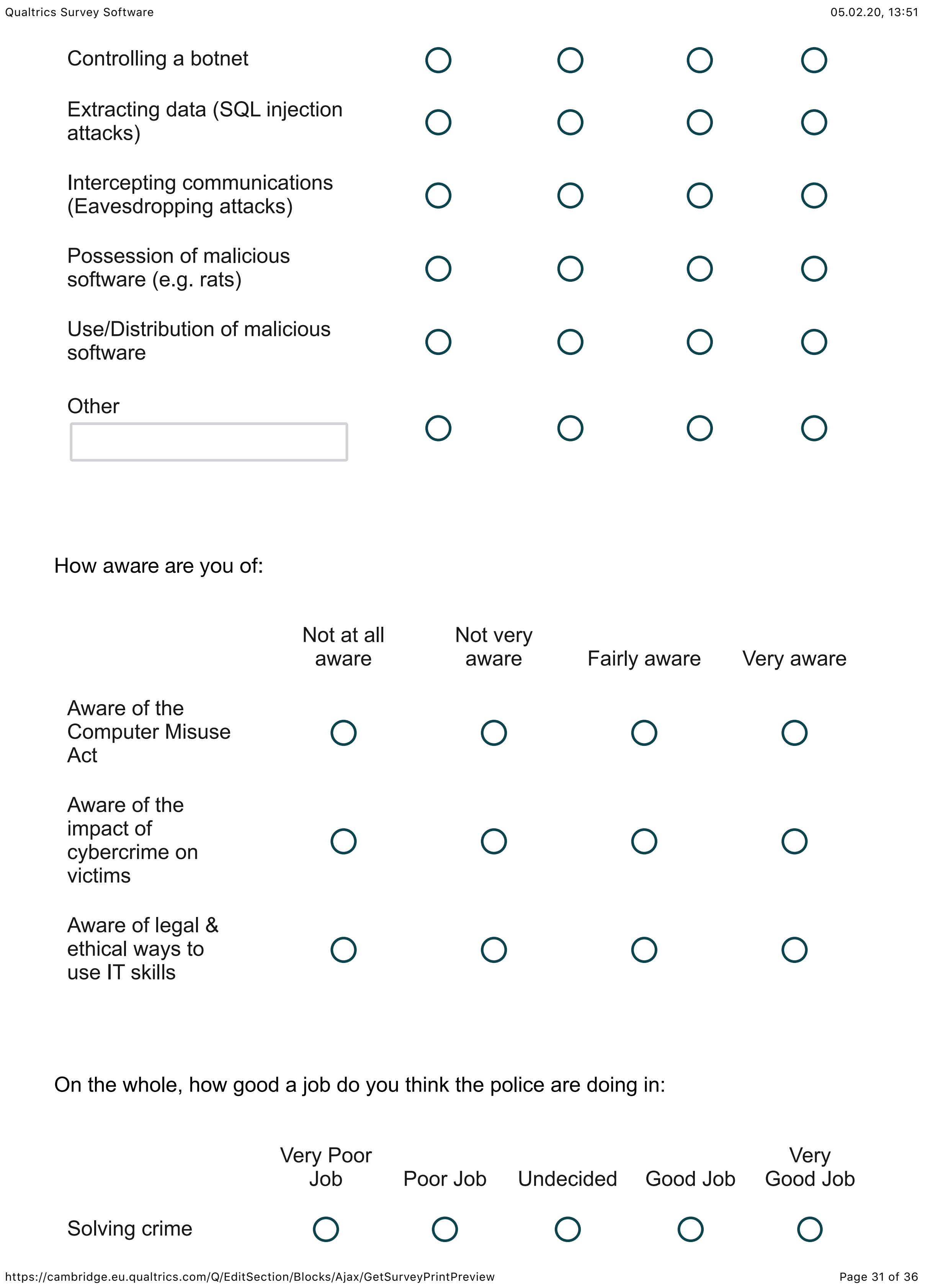
If you have stopped or reduced your involvement in harmful online activities, approximately how long ago was this?

Month	□ ▲▼
Year	□ ▲▼

If you have stopped or reduced your involvement in harmful online activities, why?

Which of the following activities did you think could be illegal?

	Always Illegal	Sometimes Illegal	Never Illegal	Not Sure
Making online services unavailable (e.g. booting, denial-of-service attacks)	○	○	○	○
Tricking people into providing their username and password	○	○	○	○
Gaining access to protected computer systems	○	○	○	○
Gaining access to secure websites	○	○	○	○
Use of stolen credit cards (e.g. carding)	○	○	○	○
Trading in fake/stolen online accounts	○	○	○	○
Game cheating (e.g. modding)	○	○	○	○
Trolling/sending abusive messages	○	○	○	○



Controlling a botnet	○	○	○	○
Extracting data (SQL injection attacks)	○	○	○	○
Intercepting communications (Eavesdropping attacks)	○	○	○	○
Possession of malicious software (e.g. rats)	○	○	○	○
Use/Distribution of malicious software	○	○	○	○
Other □	○	○	○	○

How aware are you of:

	Not at all aware	Not very aware	Fairly aware	Very aware
Aware of the Computer Misuse Act	○	○	○	○
Aware of the impact of cybercrime on victims	○	○	○	○
Aware of legal & ethical ways to use IT skills	○	○	○	○

On the whole, how good a job do you think the police are doing in:

	Very Poor Job	Poor Job	Undecided	Good Job	Very Good Job
Solving crime	○	○	○	○	○

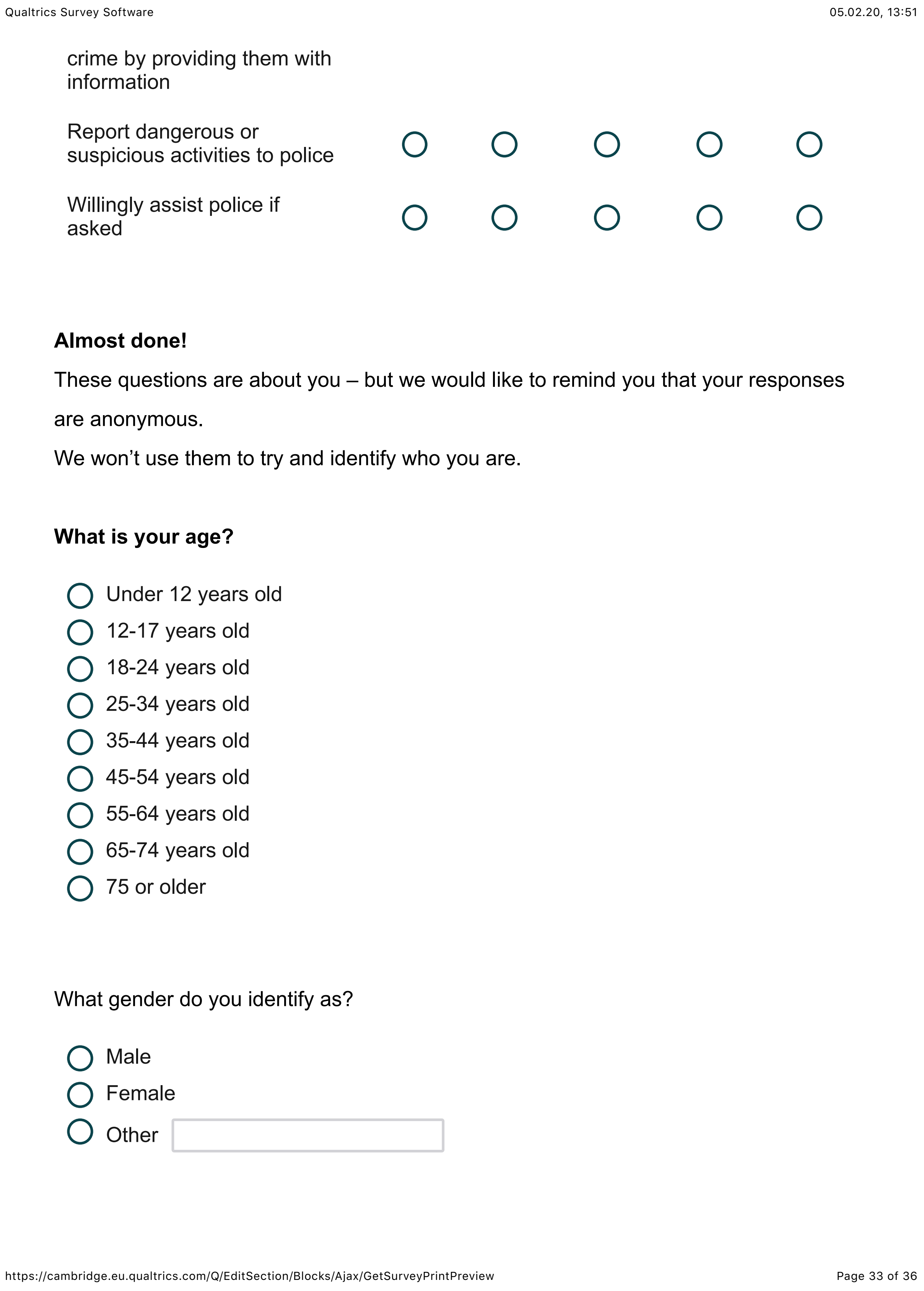
Solving cybercrime	○	○	○	○	○
Dealing with problems that concern you	○	○	○	○	○
Working with your community to solve local problems	○	○	○	○	○
Preventing crime	○	○	○	○	○

How much do you agree/disagree with the following statements?

	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree
I feel a moral obligation to obey the law	○	○	○	○	○
I feel a moral obligation to obey police	○	○	○	○	○
Overall, I obey police with good will	○	○	○	○	○

How likely would you be to:

	Very Unlikely	Not Likely	Somewhat Likely	Very Likely	Extremely Likely
Call police to report a crime	○	○	○	○	○
Help police to find someone suspected of committing a	○	○	○	○	○



crime by providing them with information					
Report dangerous or suspicious activities to police	○	○	○	○	○
Willingly assist police if asked	○	○	○	○	○

Almost done!

These questions are about you – but we would like to remind you that your responses are anonymous.

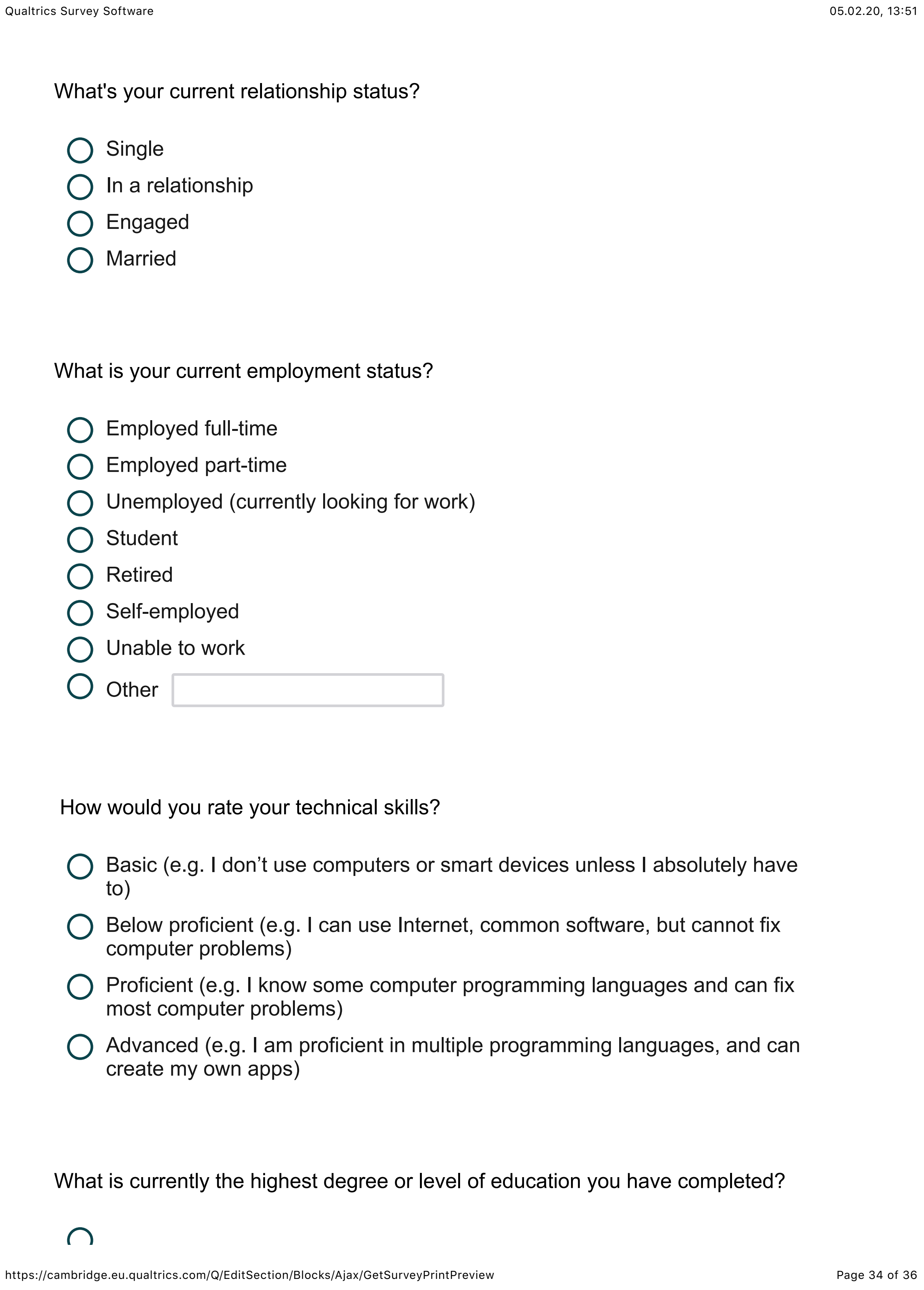
We won’t use them to try and identify who you are.

What is your age?

○ Under 12 years old
○ 12-17 years old
○ 18-24 years old
○ 25-34 years old
○ 35-44 years old
○ 45-54 years old
○ 55-64 years old
○ 65-74 years old
○ 75 or older

What gender do you identify as?

○ Male
○ Female
○ Other ______



What's your current relationship status?

○ Single
○ In a relationship
○ Engaged
○ Married

What is your current employment status?

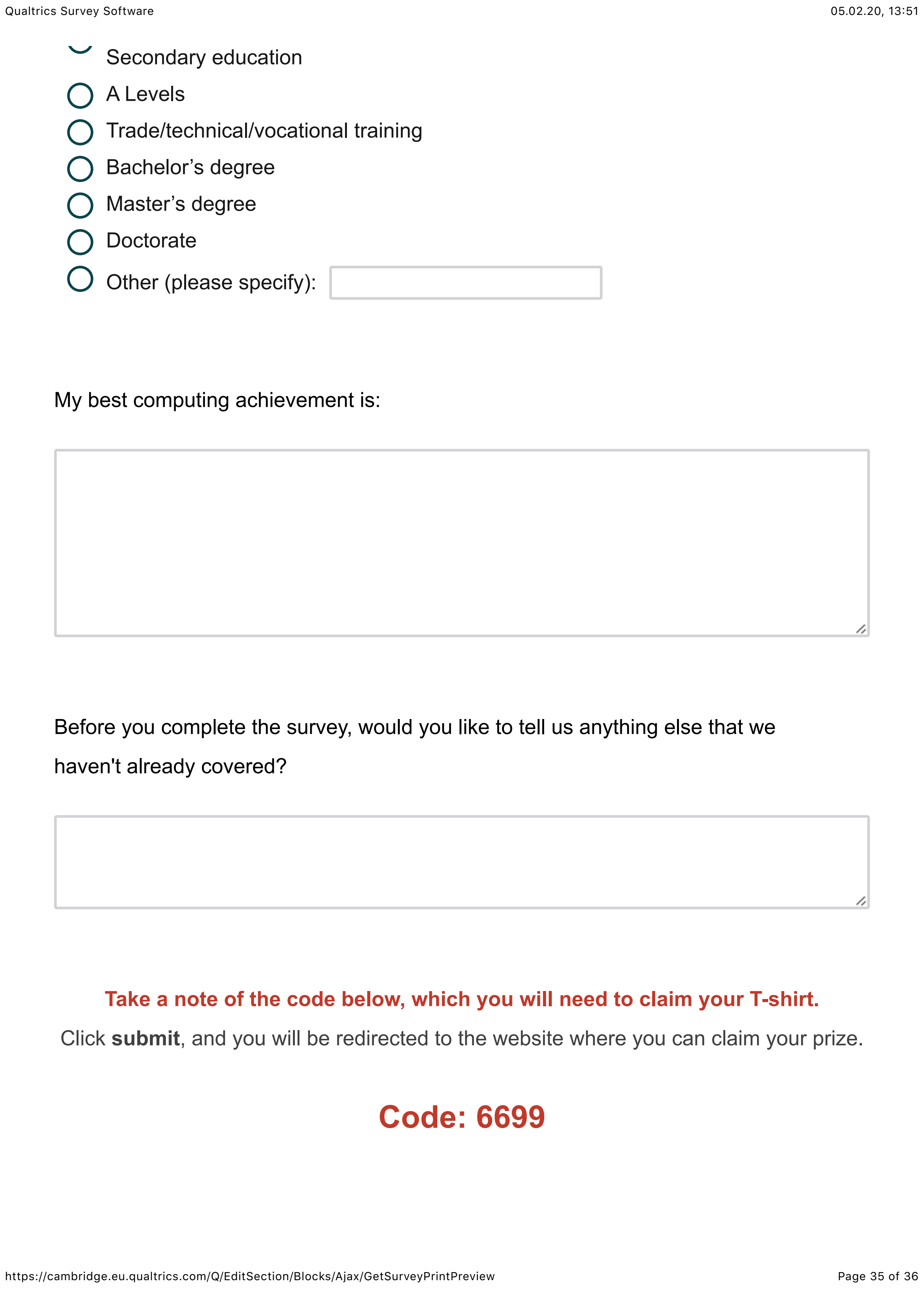
○ Employed full-time
○ Employed part-time
○ Unemployed (currently looking for work)
○ Student
○ Retired
○ Self-employed
○ Unable to work
○ Other ▭

How would you rate your technical skills?

○ Basic (e.g. I don't use computers or smart devices unless I absolutely have to)
○ Below proficient (e.g. I can use Internet, common software, but cannot fix computer problems)
○ Proficient (e.g. I know some computer programming languages and can fix most computer problems)
○ Advanced (e.g. I am proficient in multiple programming languages, and can create my own apps)

What is currently the highest degree or level of education you have completed?

○



○ Secondary education

○ A Levels

○ Trade/technical/vocational training

○ Bachelor’s degree

○ Master’s degree

○ Doctorate

○ Other (please specify):

My best computing achievement is:

Before you complete the survey, would you like to tell us anything else that we haven't already covered?

Take a note of the code below, which you will need to claim your T-shirt.

Click **submit**, and you will be redirected to the website where you can claim your prize.

Code: 6699

○ **SUBMIT**

Powered by Qualtrics