The Online Behaviour and Victimization Study

Questionnaire

Wave 1

M.S. van 't Hoff-de Goede
R. van der Kleij
S.G.A. van de Weijer
E.R. Leukfeldt

The Hague University of Applied Sciences
NSCR

<u>Online activities of Dutch citizens</u>

Thank you for taking part in this survey. Your opinions and experiences are very important to us and we greatly appreciate your participation.

What is this questionnaire about?
Researchers from THUAS and the NCSR would like to know your opinions on online activities and what you yourself do in this area. This pertains to the <u>activities in which you take part in your free time (when you are not at work)</u>. Examples of questions are: How much time do you spend online? And has anyone ever made changes to your website or profile page (such as Facebook) without your permission? The survey also includes statements. An example of a statement is: It is easy for me to keep my software up-to-date. You can then choose to answer with *completely agree, agree, neutral, disagree* or *completely disagree*. We will also describe a number of situations you might encounter online. For each one, we will ask what you would do in that situation. The survey takes about 25 minutes to complete.

It is entirely confidential!
We want to emphasise that you are under no obligation to participate. Your answers will be processed with complete anonymity. We fully guarantee your privacy. If you do not want your data to be used, you can rescind your permission (and therefore the information) at any time and without further explanation.

How will you answer?
- For the majority of questions, you can give one answer, except where the survey explicitly states that multiple answers are possible.
- Is there no answer that is exactly right in your situation? In that case, choose the answer that is the closest match for you.

Important: We ask that you fill in the entire questionnaire in a single sitting, without stopping or changing the device you are using to complete the survey.

If you would like more information on this survey, you may contact [panel company help desk].

□ I have read the information above and agree to take part in the survey.

In accordance with Dutch privacy legislation, we now ask you to create a temporary user account. For the purpose of this study, your personal data will be stored in this account. You will need to use this account one more time, at the end of the questionnaire.
Please enter a user name and password below.

1a. User name:
1b. Password *[hidden]*
[comments: 1) no limitations in terms of length, we want respondents to be able to use a sentence as their password 2) no further requirements for the password 3) no indicator of password strength will be shown to respondents]:
1c. Enter the password again *[hidden]:*

[continue]

[registration date/time and type of device]

2. *[state of mind]*

Below, there are 20 terms, each of which refers to a specific feeling or emotion. Would you please indicate the extent to which you are experiencing each feeling or emotion ***at this specific moment.*** The possible answers are: very slightly, a little, moderately, quite a bit and extremely.

		very slightly	a little	moderately	quite a bit	extremely
		1	2	3	4	5
a	Interested					
b	Distressed					
c	Exited					
d	Upset					
e	Strong					
f	Guilty					
g	Scared					
h	Hostile					
i	Enthusiastic					
j	Proud					
k	Irritable					
l	Alert					
m	Ashamed					
n	Inspired					
o	Nervous					
p	Determined					
q	Attentive					
r	Jittery					
s	Active					
t	Afraid					

[Source: PANAS scale]

[continue]

3. How often do you use the internet <u>for personal purposes</u>? Please select one answer.
- Less than once a month
- At least once a month, but not every week
- At least once a week, but not every day
- Every day
- Several times a day
- At least once an hour (during the hours I am awake)
- I am constantly, or nearly constantly, online (during the hours that I am awake)

4. Do you ever use the <u>internet</u> for personal purposes on the following devices?

		Never	Less than once a week	1 to 3 times a week	Every day, or nearly so	Several times a day
a	Tablet					
b	Mobile phone (smartphone)					
c	Laptop or notebook[1]					
d	Desktop computer[2]					
e	Other devices					

5. Which device do you use <u>most</u> when accessing the internet <u>for personal purposes</u>? *[only 1 answer is possible]*
- Tablet *(go to 6c)*
- Mobile phone (smartphone) *(go to 6d)*
- Laptop or notebook *(go to 6b)*
- Desktop computer *(go to 6a)*

6a. Does your <u>desktop computer</u> have ...	No	Yes	I don't know
... a virus scanner			
... a firewall			
... a means of backing-up[3] your files (such as to a physical external hard drive or the cloud[4])			
... an application for (illegally) downloading films, music and/or games (such as BitTorrent)			
... a browser extension, such as an ad blocker			
... a VPN connection[5]			

[go to question 7]

---

[1] A laptop or notebook is a portable computer.
[2] A desktop computer stays in one place and consists of a computer (on/under the desk), monitor, mouse and/or keyboard.
[3] To "back-up" a file means making an extra copy, just in case.
[4] A cloud service provides internet-based storage space for saving files such as photos.
[5] A VPN (Virtual Private Network) connection gives the user secure and anonymous access to a network, thereby making the internet connection more secure.

6b. Does your <u>laptop or notebook</u> have…	No	Yes	I don't know
… a virus scanner			
… a firewall			
… a means of backing-up[6] your files (such as to a physical external hard drive or the cloud[7])			
… an application for (illegally) downloading films, music and/or games (such as BitTorrent)			
… a browser extension, such as an ad blocker			
… a VPN connection[8]			

[go to question 7]

6c. Does your <u>tablet</u> have ...	No	Yes	I don't know
… a virus scanner			
… a firewall			
… a means of wirelessly backing-up[9] your files and photos (such as the cloud[10], Google Drive, NAS)			
… a VPN connection[11]			
… applications that were <u>not</u> downloaded from an official app store (Google Play, App Store)			

[go to question 7]

6d. Does your <u>mobile phone (smartphone)</u> have ...	No	Yes	I don't know
… a virus scanner			
… a firewall			
… a means of wirelessly backing-up[12] your files and photos (such as the cloud[13], Google Drive, NAS)			
… a VPN connection[14]			
… applications that were <u>not</u> downloaded from an official app store (Google Play, App Store)			

[go to question 7]

---

[6] To "back-up" a file means making an extra copy, just in case.
[7] A cloud service provides internet-based storage space for saving files such as photos.
[8] A VPN (Virtual Private Network) connection gives the user secure and anonymous access to a network, thereby making the internet connection more secure.
[9] To "back-up" a file means making an extra copy, just in case.
[10] A cloud service provides internet-based storage space for saving files such as photos.
[11] A VPN (Virtual Private Network) connection gives the user secure and anonymous access to a network, thereby making the internet connection more secure.
[12] To "back-up" a file means making an extra copy, just in case.
[13] A cloud service provides internet-based storage space for saving files such as photos.
[14] A VPN (Virtual Private Network) connection gives the user secure and anonymous access to a network, thereby making the internet connection more secure.

7. Which device are you using <u>to fill in this questionnaire?</u> *[only 1 answer is possible]*
- Tablet
- Mobile phone (smartphone)
- Laptop or notebook
- Desktop computer

[data concerning this device (operating system, type of browser, etc.) will be registered automatically by the panel company]

We will now ask you questions about a number of online activities. You have **5 minutes** to complete this section.*

[Time pressure – one-half of respondents will be shown this message.]
Experience has shown that, for many participants, this is <u>not enough time</u>. We ask that you <u>maintain a rapid pace</u> as you complete this section. Try to answer all the questions within the time you have.

[No time pressure – one-half of respondents will be shown this message.]
Experience has shown that, for most participants, this is <u>more than enough time</u>. We ask that you <u>maintain your own pace</u> as you complete this section.

[continue]

8. How often do you conduct the following online activities <u>in your free time (when you are not at work)</u>?

|		Never	Less than once a week	1 to 3 times a week	Every day, or nearly so	Several times a day
a	Reading/sending emails					
b	Looking up information (purposeful browsing)					
c	Aimless browsing					
d	Online banking					
e	Online shopping					
e	Downloading music, films, software and/or games					
f	Video chatting with others, such as via Skype or FaceTime					
g	Watching/streaming content online (such as via YouTube)					
h	Reading posts and viewing profiles on social media (such as Facebook, Twitter, Instagram and LinkedIn)					
i	Posting, sending messages or liking/sharing posts by other people on social media (such as Facebook, Twitter, Instagram and LinkedIn)					
j	Chatting via online chat rooms					
k	Posting in online discussion groups/internet forums					
l	Online gaming/playing games					
m	Online tasks related to your studies					
n	Building/maintaining websites					

Before you answer the following question, we would like you to watch a short video clip (30 seconds) about shopping online. Click the play button in the screen below.
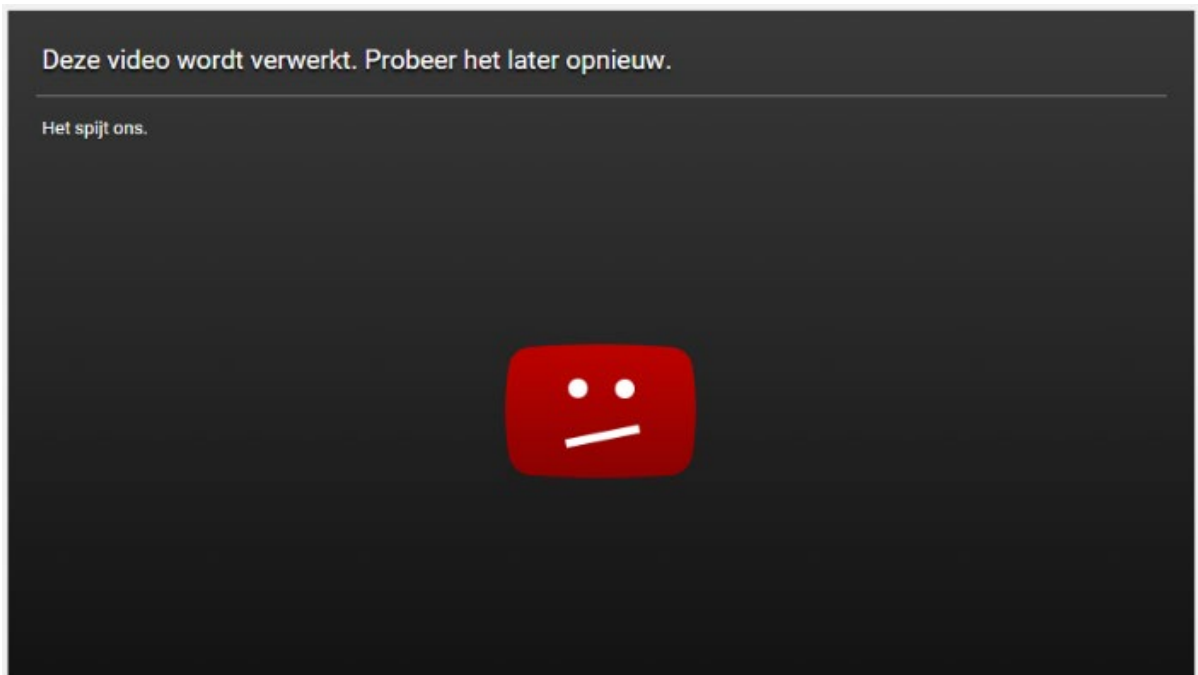
[Picture Translation:
This video is being processed. Try again later. // We are sorry. //]

[question 9a will appear as soon as the respondent attempts to play the video.]

9a.
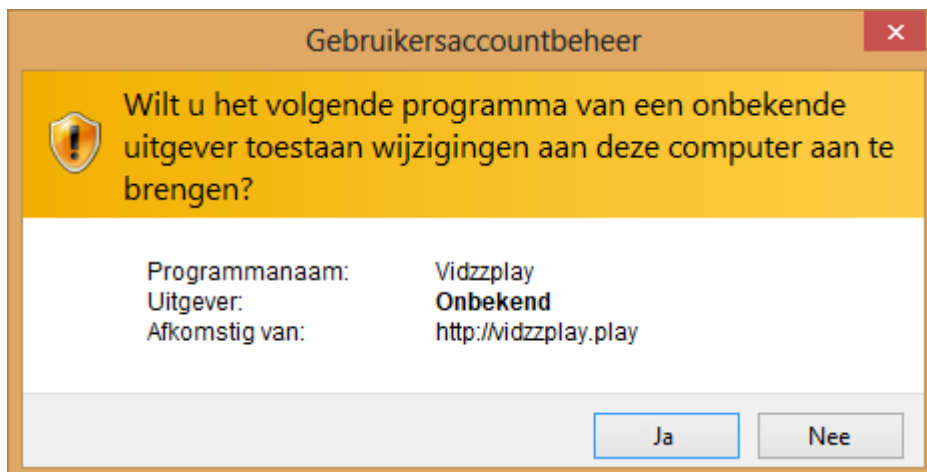
[Picture Translation:
User account management //
Do you allow the following program from an unknown publisher to make changes to this computer? //
Program name: Vidzzplay //
Publisher: unknown //
Origin: http://vidzzplay.play //
yes // no]

It is possible to buy products such as clothing, electronics and admission tickets online. You can make your purchases via online shops or directly from private citizens, such as via Marktplaats.nl (the online marketplace).

10. Have you purchased a product or products online in the last 12 months?
- Yes
- No

This is the end of section 2 on online activities. You were given 5 minutes to complete this section.

11a. How much **time pressure** did you experience when choosing your answers in the section about online activities?

No time pressure   Extreme time pressure

        1   2   3   4   5   6   7

11b. How **rushed** did you feel while answering the questions in the section about online activities?

Not rushed at all   Very rushed

        1   2   3   4   5   6   7

Many people receive an overwhelmingly large number of emails on a daily basis. We would like to know how people handle emails. You will now be presented with a number of emails, as if they are arriving in the inbox of someone named "Robin de Vries". We ask you to pretend you are Robin. What would Robin do with these emails? You will also be asked how certain you feel about your choices and which aspects of the email in question influenced your decision.

[continue]

[respondent will be presented with three vignettes, shown in the order of the version assigned to them (the versions are distributed randomly among respondents in equal proportions):

Version 1: KPN, DJguide, Rabo

Version 2: DjGuide, KPN, Rabo

Version 3: DjGuide, Rabo, KPN

Version 4: KPN, Rabo, DJguide

Version 5: Rabo, KPN, DjGuide

Version 6: Rabo, DjGuide, KPN

DJguide vignette [phishing, scarcity]

Below, you can see an image of an email Robin has received. Robin is a fan of Armin van Buuren and lives near Leiden, where this DJ has an upcoming performance during the festivities on the Dutch holiday known as King's Day.

Van: DJguide [mailto:info@djguides.nl]
Verzonden: Dinsdag 12 februari 2019 11:14
Aan: robin@devries.nl
Onderwerp: Gratis e-ticket Armin van Buuren Kingsday Leiden

GRATIS E-TICKET
ARMIN VAN BUUREN KINGSDAY LEIDEN

Armin van Buuren presents Kingsday Leiden

Armin van Buuren treedt dit jaar weer op in Leiden tijdens Koningsdag. Na het grote succes van vorig jaar vindt het feest 'Armin van Buuren presents Kingsday Leiden' dit jaar weer plaats op de Garenmarkt in de binnenstad van Leiden en jij kan er **GRATIS** bij zijn.

Op dinsdag 27 april vanaf 15.00 uur tot 22.00 uur kunnen oranje fans genieten van diverse optredens met als hoogtepunt een optreden van Leidenaar Armin van Buuren.

Ook dit jaar zal Armin van Buuren de oranjekoorts 'zijn stad' naar ongekende hoogte laten stijgen. Al 13 jaar lang treedt Van Buuren, één van de beroemdste DJ's ter wereld, op tijdens Koningsdag in Leiden. Dit is het hoogtepunt van het feest "Armin van Buuren presents Kingsday Leiden', dat dit jaar weer plaatsvindt op de Garenmarkt. Iedereen vanaf 16 jaar en ouder kan hier genieten van het ultieme Koningsdagfeest!

DOWNLOAD HIER JOU GRATIS TICKET

http://www.djguides.nl/gratis-ticket

[Description: this is a phishing e-mail from "DJguide" (not a well known company). It offers a free ticket to a performance of Armin van Buuren (famous DJ) on a festival (on Kingsday, national holiday in the Netherlands, in the city Leiden). URL: "download your free ticket here"]

12. If you were Robin, what would you do after receiving this email? For each action, please select either "yes" or "no".

		Yes	No
a	I would answer the email		
b	I would delete the email		
c	I would forward the email to someone else		
d	I would copy and paste the URL (the www address) from the email into a web browser		*
e	I would click on the link in the email		*
f	I would type the URL (the www address) into a web browser		*
g	I would save the email		
h	I would look for more information before making a decision		

i	I would do nothing		

13. How certain do you feel about your choices?

Not certain at all   Very certain
1   2   3   4   5

14. Which aspects of the email influenced your decision? You can choose more than one answer.
- The sender
- The subject
- The text in the email
- The image in the email
- The hyperlink in the email
- The target address of the hyperlink (the website to which the link directs the user)

KPN vignette [legitimate]

Robin is a customer of the telecom company KPN. Robin feels it is important to stay up-to-date on developments and current events in connection with internet safety. Robin is particularly interested in information on how they can protect themselves better.
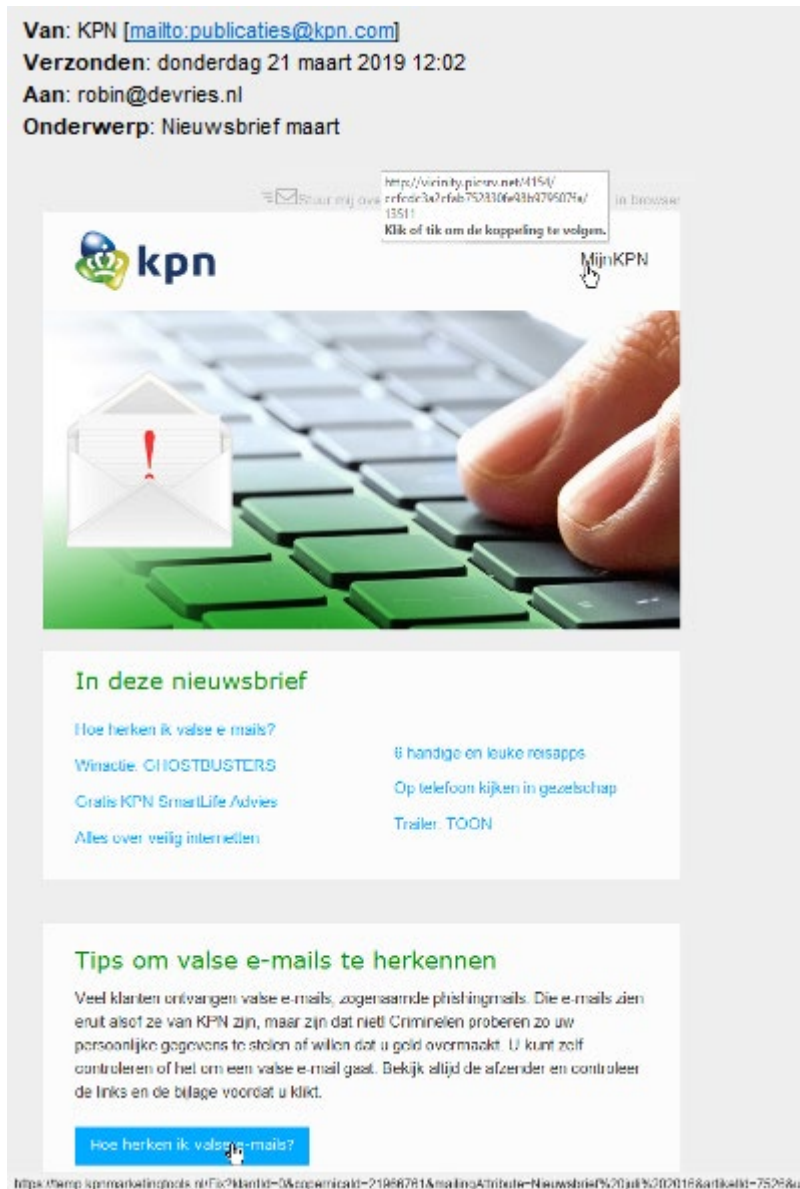
[Description: this is a legitimate e-mail from a large Telecom Provider (KPN) in The Netherlands. It is a news letter with advice on how to recognise fraudulent e-mails. URL: My KPN]

15. If you were Robin, what would you do after receiving this email? For each action, please select either "yes" or "no".

		Yes	No
a	I would answer the email		
b	I would delete the email		
c	I would forward the email to someone else		

d	I would copy and paste the URL (the www address) from the email into a web browser	*	
e	I would click on the link in the email	*	
f	I would type the URL (the www address) into a web browser	*	
g	I would save the email		
h	I would look for more information before making a decision		
i	I would do nothing		

16. How certain do you feel about your choices?

Not certain at all   Very certain

1   2   3   4   5

17. Which aspects of the email influenced your decision? You can choose more than one answer.
- The sender
- The subject
- The text in the email
- The image in the email
- The hyperlink in the email
- The target address of the hyperlink (the website to which the link directs the user)

Rabo vignette [phishing (authority)]

Robin has had a payment account at the Rabobank for some time. On 23 January, Robin received the following email in their inbox.

Van: Rabobank [mailto:bankzaken@rabobank.nl]
Verzonden: woensdag 23 januari 2019 17:58
Aan: robin@devries.nl
Onderwerp: Laatste herinnering: Uw aanvraag is nog niet verwerkt, voorkom een geblokkeerde betaalpas

Rabobank

Geachte relatie,

Uit onze administratie is gebleken dat u nog geen gebruik maakt van onze nieuwe betaalpas. De nieuwe betaalpas is beter beveiligd tegen frauduleuze praktijken en voldoet zich aan de Europese veiligheidsvoorschriften betreft bankzaken. Met de nieuwe betaalpas kunt u vertrouwd, veilig en gemakkelijk betalen en geld opnemen zoals u gewend bent en contactloos betalen in meer dan 12.000 winkels in heel Europa. Ook bent u beter beschermd tegen skimming en pinpas-fraude bij geldautomaten.

Het gebruik van uw huidige betaalpas wordt gedeactiveerd. In verband met de veiligheid van onze klanten is het verplicht uw huidige betaalpas te vervangen. Wij bieden onze klanten de mogelijkheid aan om dit kosteloos te doen. Klik hier om kosteloos uw nieuwe betaalpas aan te vragen en volg de benodigde stappen om uw aanvraag te voltooien. U ontvangt uw nieuwe betaalpas binnen **2 werkdagen** per post toegezonden.

Zolang u nog niet in bezit bent van een nieuwe betaalpas kunt u helaas nog geen gebruik maken van onze nieuwe dienstverlening.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd en van dienst te zijn geweest.

Alvast hartelijk dank voor uw medewerking.

Met vriendelijke groet,
Rabobank

Afdeling Internetbankieren

http://rabobank.nl.condoclima.com/rabaanvraag/infoggen.html

*[Description: this is a phishing e-mail, pretending to originate from a large bank (Rabobank) in in The Netherlands. It warns the reader that they are not yet using their new debit card and that their current card is being blocked. They can receive a new card for free [..] within **2 work days.** URL: "click here"]*

18. If you were Robin, what would you do after receiving this email? For each action, please select either "yes" or "no".

		Yes	No
a	I would answer the email		
b	I would delete the email		
c	I would forward the email to someone else		
d	I would copy and paste the URL (the www address) from the email into a web browser		*

e	I would click on the link in the email		*
f	I would type the URL (the www address) into a web browser		*
g	I would save the email		
h	I would look for more information before making a decision		
i	I would do nothing		

19. How certain do you feel about your choices?

Not certain at all				Very certain
1	2	3	4	5

20. Which aspects of the email influenced your decision? You can choose more than one answer.
- The sender
- The subject
- The text in the email
- The image in the email
- The hyperlink in the email
- The target address of the hyperlink (the website to which the link directs the user)

This was the last email we wanted to show you.

[registration date/time and type of device]

21. Now you will be shown a number of statements about how you manage passwords, back-ups, updates and security software in your free time (when you are not at work). For each question, you will choose an answer ranging from *never* to *always*.

[Behaviour: using passwords]

		Never	Seldom	Sometimes	Often	Always	N/A
a	I share my personal passwords with others.	5	4	3	2	1	
b	I use simple, short passwords that often contain only one number or capital letter.	5	4	3	2	1	
c	I use the same password for <u>multiple purposes</u>, such as for both social media accounts and logging into online banking and online shops.	5	4	3	2	1	

[Behaviour: Backing-up important files]

d	I back-up[15] all my important files.	1	2	3	4	5	
e	I save personal information in an encrypted form so that it cannot easily be read by others.	1	2	3	4	5	

[Behaviour: installing software updates]

f	I install any operating-system updates on my devices as soon as those updates become available.	1	2	3	4	5	
g	I install updates for apps or software I use as soon as those updates become available.	1	2	3	4	5	

[Behaviour: using security software]

h	I update my security software[16] as soon as a new update become available.	1	2	3	4	5	
i	I use security software[17] to scan my devices for viruses and other malicious software.	1	2	3	4	5	

---

[15] To "back-up" a file means making an extra copy, just in case.

[16] Security software protects devices from malicious software such as spyware, viruses and ransomware. Examples include Windows Defender Antivirus, Panda Free Antivirus and Norton Security.

[17] Security software protects devices from malicious software such as spyware, viruses and ransomware. Examples include Windows Defender Antivirus, Panda Free Antivirus and Norton Security.

22. Now you will be shown a number of statements about how you use the internet in your free time (when you are not at work). For each question, you will choose an answer ranging from *never* to *always*.

[Behaviour: being careful online]

		Never	Seldom	Sometimes	Often	Always	N/A
a	I download software, films, games or music from <u>illegal</u> sources.	5	4	3	2	1	
b	I use browser extensions[18] to help me browse the internet safely, such as software that blocks advertisements or pop-ups.	1	2	3	4	5	
c	I use public WiFi networks (such as in a café or on public transportation) without a VPN connection.[19]	5	4	3	2	1	

[Behaviour: avoiding indiscriminate sharing of personal data]

d	I check the privacy settings on my devices, apps and/or social media.	1	2	3	4	5	
e	I share personal information such as my home address, email address or telephone number on social media.	5	4	3	2	1	
f	I am selective when it comes to accepting other people's requests to connect to my social media account(s).	1	2	3	4	5	

[Behaviour: handling emails that contain attachments or links with caution]

g	I immediately delete any email I find suspicious	1	2	3	4	5	
h	When I have doubts about the authenticity of an email, I contact the sender to ask if they did, in fact, send me an email.	1	2	3	4	5	
i	I open email attachments, even when an email comes from an unknown sender.	5	4	3	2	1	

[registration date/time and type of device]

---

[18] A browser extension is software that adds an extra functionality to a browser, such as managing cookies or advertisements when you are browsing the internet.

[19] A VPN (Virtual Private Network) connection gives the user secure and anonymous access to a network, thereby making the internet connection more secure.

23. How much do you know about cybersecurity?
- Almost nothing - Fairly little - A little - An average amount - Quite a bit - A lot - A very great deal

[* marks the correct answer; these will be deleted from the final questionnaire]

24. Here you see an image of an address bar. Is this a trustworthy URL (internet address)?
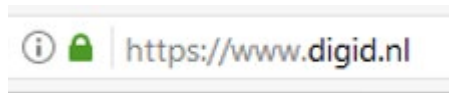   - Yes
   - No*
   - I don't know

[continue]

25. Here you see an image of an address bar. Is this a trustworthy URL (internet address)?
   - Yes*
   - No
   - I don't know

[continue]

In this portion of the survey, we will ask you a number of multiple choice questions about computer and internet-related terms. For each question, please select the correct answer. If you do not know the answer to a question, you may indicate this.

26. Which statement about saving extra copies of important files is correct?
    a. You should always create a physical back-up in two locations: at home and somewhere else
    b. It is unwise to rely on an online back-up alone, as you cannot be certain your files are truly safe there
    c. You should avoid using CDs and DVDs to back-up your files
    d. All the statements above are correct*
    e. I don't know

27. What is encryption? It means the content of a given file...
    a. ... can be accessed by all users
    b. ... has been encoded to protect it*
    c. ... has been checked for viruses
    d. ... has been deleted
    e. I don't know

28. Which statement is correct? A software update ...
    a. ... is a program designed to prevent, detect and remove malware
    b. ... is used to check networks or systems for malicious activities
    c. ... is released to repair security risks or make changes to the program*
    d. ... is a copy of data that has been stored on a data carrier (such as a computer) for the purpose of restoring it
    a. I don't know

29. Which of these passwords is the strongest?
    a. I love carrots and swimming*
    b. Penguin123
    c. doG?99
    d. F@c3B0oK
    e. I don't know

30. Which statement is correct? Installing a software update ...
    a. ... should be done no later than one month after the release date
    b. ... always occurs automatically, immediately after its release
    c. ... should ideally be done as soon as it's released
    d. ... is something that should be delayed, so you can wait and see if the update had any bugs
    e. I don't know

31. What does it mean to say a website is "infected"?
    a. That the website is not being displayed properly
    b. That the website is having trouble connecting to the network
    c. That the website contains malicious software*
    d. None of the answers above is correct
    e. I don't know

32. Which statement is correct? A firewall is a system that …
    a.   … is used to filter and block unwanted emails from your inbox
    b.   … can protect a network or computer from unauthorised use by external parties*
    c.   … is also known as an IDS (Intrusion Detection System)
    d.   All the statements above are correct
    e.   I don't know

33. What is an ad blocker?
    a.   A program that blocks undesired emails
    b.   Software that prevents other people from being able to take over the computer
    c.   A program that prevents websites from displaying undesired content*
    d.   A virus that locks the computer until the user pays a ransom
    e.   I don't know

34. Which information should you avoid sharing publicly on social media?
    a.   Your current location
    b.   A photo of your driving licence
    c.   Personal data such as your address, date of birth and telephone number
    d.   All the answers above are correct*
    e.   I don't know

35. What is online identity fraud?
    a.   Unauthorised use of another individual's personal data on the internet*
    b.   "Phishing" for log-in details and personal data belonging to another person
    c.   A form of bullying via new communication technologies
    d.   Spreading fake news online
    e.   I don't know

36. What is phishing? An attempt to …
    a.   … gain control over your computer's operating system
    b.   … find out log-in details and gain access to online accounts*
    c.   … sell you a product you don't need
    d.   None of the answers above is correct
    e.   I don't know

37. Which statement is correct? A spam filter is used to …
    a.   … prevent unauthorised users from accessing a network
    b.   … block undesired advertisements while browsing online
    c.   … keep undesired emails out of your inbox*
    d.   … limit access to suspicious websites
    e.   I don't know

38. What is two-factor authentication?
    a.   An extra layer of security on top of your password*
    b.   A check to see whether the proof of identification that was entered is real
    c.   Software that is used to disrupt computer systems
    d.   The combination of user name and password needed to create an account
    e.   I don't know

39. Four URLs (web addresses) are shown below. Please indicate which of these URLs will take you to a trustworthy (legitimate) website and which ones will direct you to a fake (phishing) website. If you are unsure, you can choose "I don't know".

		Trustworthy website	Malicious website	I don't know
a	www.abnamro.nl/nl/prive/service-en-contact	*		
b	www.bol.com/nl/l/software/N/7000/?view=list	*		
c	www.mijnoverheid.zcards.nl/digid		*	
d	www.nieuwbetaalpas.rabobankinternet.com		*	

[Description: The trustworthy URL's are from a large bank (a) and well known webshop (b). The phishing links pretend to be from a government page that people can log in to with their personal identification account (digid) (c) and a large bank (d). Hyperlink c can be recognized by the word "zcards" and hyperlink d by a typo.]

[Self-efficacy]

40. In this section, we will present you with statements about yourself and your characteristics. To what extent do you agree or disagree with the following statements? <u>There are no wrong or right answers for this portion.</u>

		Completely disagree	Disagree	Neutral	Agree	Completely agree
a	I am quite capable of using a strong, unique password for each one of my accounts.					
b	I find it complicated to ensure that my files are being backed-up.[20] (O)					
c	It is easy for me to keep my software up-to-date.					
d	It takes little effort on my part to ensure that a virus scanner and firewall have been installed on my devices.					
e	I find it very challenging to be cautious online. (O)					
f	I am able to determine what is and is not safe for me to post on social media.					
g	It is sometimes hard for me to tell whether or not it is safe to click on a link in an email. (O)					

[continue]

---

[20] To "back-up" a file means making an extra copy, just in case.

[Response costs]

41. To what extent do you agree or disagree with the following statements? <u>There are no wrong or right answers for this portion.</u>

		Completely disagree	Disagree	Neutral	Agree	Completely agree
a	Using exclusively strong, unique passwords would require me to develop a new habit and I find that challenging.					
b	Backing-up[21] my documents is really time-consuming for me.					
c	It is inconvenient for me to keep my software up-to-date all the time.					
d	It takes a lot of effort on my part to make sure all my devices have an effective virus scanner and firewall.					
e	I find it annoying when I have to think about whether I'm practising safe behaviour online.					
f	When I want to make a payment online, it takes only a short amount of time for me to check and see whether I'm in a safe online environment. (O)					
g	I struggle with the fact that I can't just open every attachment to an email.					
h	I consider it a big nuisance that you have to pay attention to so many things these days in order to use the internet safely.					

[continue]

---

[21] To "back-up" a file means making an extra copy, just in case.

42. *[a,b,c =protection motivation, d, e, f= locus of control]*

To what extent do you agree or disagree with these statements? <u>There are no wrong or right answers for this portion.</u>

		Completely disagree	Disagree	Neutral	Agree	Completely agree
a	If an important – and <u>affordable</u> – security product that will enhance my online security becomes available, I am prepared to spend money on that product.					
b	I am eager to minimise my risk of falling victim to cybercrime.[22]					
c	I want to do everything I can to protect myself against cybercrime.					
d	Where my online safety is concerned, the primary responsibility is <u>my own</u>.					

[continue]

		Is out of my control				Is within my control
e	Maintaining the security of my personal data					

[continue]

		the government/police				myself
f	The party who is responsible for protecting my personal data is …					

[continue]

---

[22] The term cybercrime, also known as internet crime, refers to all types of criminal behaviour that involve the use of ICT or the internet in order to commit the offence. Examples are online fraud, hacking into a database containing personal data and launching a DDoS attack to crash a bank's website.

43. *[Response efficacy]*

The following statements have to do with how people behave when using their computers. To what extent do you agree or disagree with the following statements? There are no wrong or right answers for this portion. We would like you to tell us your opinion.

		Completely disagree	Disagree	Neutral	Agree	Completely agree
a	By using strong, unique passwords, you can reduce your chances of being hacked.[23]					
b	By backing-up[24] your personal files frequently, you can reduce the severity of the consequences in the event your computer is hacked by cybercriminals.					
c	Keeping your software up-to-date has virtually no effect on your chances of becoming a victim of cybercrime.[25] (O)					
d	When a firewall has been installed on a computer, it is more difficult for cybercriminals to hack (i.e. break into) that computer.					
e	By paying close attention to what you do online, you can avoid falling victim to cybercriminals.					
f	It is safe to share your name and email address on social media. (O)					

---

[23] Hacking is gaining unauthorised access to an account, computer or other automated process, or part of such a system.

[24] To "back-up" a file means making an extra copy, just in case.

[25] The term cybercrime, also known as internet crime, refers to all types of criminal behaviour that involve the use of ICT or the internet in order to commit the offence. Examples are online fraud, hacking into a database containing personal data and launching a DDoS attack to crash a bank's website.

44. *[Opportunity: social support]*

The following statements have to do with your social environment. To what extent do you agree or disagree with the following statements?

		Completely disagree	Disagree	Neutral	Agree	Completely agree
a	People around me (friends/family/acquaintances) encourage me to back-up[26] my important files.					
b	If I were to tell people around me (friends/family/acquaintances) that I am very cautious when online, they would say that was wise.					
c	People around me (friends/family/acquaintances) feel that online safety is important.					
d	People around me (friends/family/acquaintances) often share personal information (such as their email address, home address or phone number) on social media (O)					
e	If I were to become a victim of cybercrime,[27] I would be able to talk about it with the people around me (friends/family/acquaintances).					

---

[26] To "back-up" a file means making an extra copy, just in case.
[27] The term cybercrime, also known as internet crime, refers to all types of criminal behaviour that involve the use of ICT or the internet in order to commit the offence. Examples are online fraud, hacking into a database containing personal data and launching a DDoS attack to crash a bank's website.

45. *[Opportunity: physical support]* The following statements <u>have to do with your home situation</u>. To what extent do you agree or disagree with the following statements?

		Completely disagree	Disagree	Neutral	Agree	Completely agree
a	Our household has the disposable income needed to purchase security measures, such as a virus scanner, VPN[28] or cloud-based service.[29]					
b	I have access to a password manager[30] for safely storing my passwords.					
c	I have access to information about online safety. such as through websites, television and social media or via newsletters.					

[registration date/time and type of device]

---

[28] A VPN (Virtual Private Network) connection gives the user secure and anonymous access to a network, thereby making the internet connection more secure.
[29] A cloud service provides internet-based storage space for saving files such as photos.
[30] A password manager or password safe is a secure digital vault for the creation, use and encrypted storage of your passwords.

The term cybercrime, also known as internet crime, refers to all types of criminal behaviour that involve the use of ICT or the internet in order to commit the offence. Examples are online fraud, hacking into a database containing personal data and launching a DDoS attack to crash a bank's website.

[Perceived vulnerability]

46. On average, how likely do you estimate <u>a person in the Netherlands</u> is to become a victim of cybercrime in the next twelve months?

[slider from 0 to 100%]

[page break]

47. How likely do you think it is that <u>you</u> will become a victim of cybercrime in the next twelve months?

[slider from 0 to 100%]

48. *[a t/m f= fear of victimisation, g= Perceived vulnerability, h= Perceived impact]*

To what extent do you agree or disagree with the following statements? <u>There are no wrong or right answers for this portion.</u>

		Completely disagree	Disagree	Neutral	Agree	Completely agree
a	I am afraid of becoming a victim of cybercrime in the near future.					
b	I find it frightening that someone could log into my online bank account without my permission.					
c	I am concerned that I might become a victim of phishing.[31]					
d	I worry about the possibility of my computer being hacked.[32]					
e	I think I could easily become the victim of online fraud.					
f	It worries me to think that ransomware[33] could be installed on my computer.					
g	It is entirely possible that I will become a victim of cybercrime in the next year.					
h	If I were to become a victim of cybercrime, the consequences could be severe.					

[continue]

---

[31] Phishing is a form of online fraud in which criminals create fake versions of legitimate entities' emails and websites in order to mislead victims for the purpose of obtaining their log-in details and gaining access to online accounts.

[32] Hacking is gaining unauthorised access to an account, computer or other automated process, or part of such a system.

[33] Ransomware is malicious software that can lock a computer, preventing it from being used, or encrypt files. In that case, you will not be able to use the computer or open the files until you have paid a ransom.

49. *[Perceived impact]*

We want to know how upset you would be if the following events occurred. <u>There are no wrong or right answers for this portion.</u> You can give an answer on a scale from *not upset at all* to *extremely upset.*

	How upset would you be if ...	Not upset at all				Extremely upset
a	... all your valuable possessions were stolen, and you were not insured against the loss nor was there any possibility of recovering a portion of your things	0	1	2	3	4
b	... someone stole your credit card information and used your card number to make purchases	0	1	2	3	4
c	... someone used online banking to log into your bank account and steal your money	0	1	2	3	4
d	... your device became slow to respond because there was malware[34] on it	0	1	2	3	4
e	... someone used your identity without your permission	0	1	2	3	4
f	... your email account automatically sent harmful software, such as a virus, to everyone in your address book	0	1	2	3	4
g	... someone you didn't know was able to see everything you typed on your computer	0	1	2	3	4

---

[34] <u>Malware</u> is malicious software that is installed on your computer without your permission and usually without your knowledge. Examples of malware are viruses, Trojan horses, worms and spyware.

Please indicate whether you have encountered the following forms of cybercrime:

		Yes, within the past 12 months	Yes, more than 12 months ago	No	I don't know
50a	Have you ever been a victim of phishing[35]?	[skip to 50b]			
51a	Have you ever discovered that you had malware[36] on one of your devices (computer/laptop/smartphone/tablet)?	[skip to 51b]			
52a	Have you ever purchased a product or service online, and paid for at least a portion of it, after which the product or service never arrived because you were scammed by the seller?	[skip to question 52b]			
53a	Have you ever been a victim of online identity fraud[37]?	[skip to 53b]			
54a	Have you ever fallen for a scam in which you transferred money to someone who approached you (either by email or online) with a story about earning money quickly through an inheritance, investment, lottery or similar means (online advance-fee scam[38])?	[skip to 54b]			
55a	Has anyone ever made changes to your website and/or profile page (such as Facebook) without your permission?	[skip to 55b]			
56a	Has anyone ever accessed your online account(s) without your permission, for instance by guessing your password?	[skip to 56b]			
57a	Has anyone ever hacked into your computer and deleted, edited or stolen data?	[skip to 57b]			
58a	Has anyone ever logged into your email account without your permission?	[skip to 58b]			

---

[35] Phishing is a form of online fraud in which criminals create fake versions of legitimate entities' emails and websites in order to mislead victims for the purpose of obtaining their log-in details and gaining access to online accounts.

[36] Malware is malicious software that is installed on your computer without your permission and usually without your knowledge. Examples of malware are viruses, Trojan horses, worms and spyware.

[37] Identity fraud is when someone else uses your personal or financial details, without your permission, for their own monetary gain. For instance: when someone buys products under your name or pretends to be you in order to request official documents in your name. While identity fraud usually stems from the theft of identity-related information, it can also happen using personal identifying details you willingly provided.

[38] An online advance-fee scam is a form of internet fraud. The basic premise of an advance-fee scam is that the victim must pay an advance in order to receive a large sum of money. This is usually something like an alleged inheritance, investment or lottery.

59a	Have you ever been blocked from accessing your digital files, such as by a ransomware attack?	[skip to 59b]			
60a	Have you ever been a victim of another form of cybercrime?	[skip to 60b]			

50b. You have indicated that you have been a victim of phishing within the past 12 months.

51b. You have indicated that you have discovered malware on one of your devices within the past 12 months.

52b. You have indicated that you have been scammed by an online seller within the past 12 months.

53b. You have indicated that you have been a victim of online identity fraud within the past 12 months.

54b. You have indicated that you have been a victim of an online advance-fee scam within the past 12 months.

55b. You have indicated that someone else has made changes to your website and/or profile page without your permission within the past 12 months.

56b. You have indicated that someone else has accessed your online account(s) without your permission within the past 12 months.

57b. You have indicated that someone else has hacked into your computer and deleted, edited or stolen data within the past 12 months.

58b. You have indicated that someone else has logged into your email account without your permission within the past 12 months.

59b. You have indicated that you have been blocked from accessing your digital files within the past 12 months.

60b. You have indicated that you have been a victim of a different form of cybercrime within the past 12 months.

[for each question, the following follow-up questions will be asked:]

c. Did you suffer any harm or loss as a result of the (most recent) incident?

		Yes	No
a	Financial loss		
b	Loss of files/documents		
c	Loss of time		
d	Emotional harm		
e	Other harm or loss		

d. We would like to know whether your experience with cybercrime has had an impact on your online behaviour since then. As a result of the (most recent) incident, have you become more or less cautious online?

- Much less cautious
- A little less cautious
- My behaviour has not become more or less cautious
- A little more cautious
- Much more cautious

61. [self-control]

The following statements have to do with your self-image: how you see yourself. Please indicate how much each of the following statements reflects how you typically are.

		Does not apply to me at all				Very strongly applies to me
a	I have a hard time breaking bad habits.	1	2	3	4	5
b	I am lazy.	1	2	3	4	5
c	I say inappropriate things.	1	2	3	4	5
d	I do certain things that are bad for me, if they are fun	1	2	3	4	5
e	I wish I had more self-discipline.	1	2	3	4	5
f	Pleasure and fun sometimes keep me from getting work done	1	2	3	4	5
g	I have trouble concentrating.	1	2	3	4	5
h	Sometimes I can't stop myself from doing something, even if I know it is wrong	1	2	3	4	5
i	I often act without thinking through all the alternatives.	1	2	3	4	5
j	I am good at resisting temptation.	5	4	3	2	1
k	I am able to work effectively toward long-term goals.	5	4	3	2	1
l	I refuse things that are bad for me.	5	4	3	2	1
m	People would say that I have iron self-discipline	5	4	3	2	1

[Source: Brief Self Control Scale (BSCS)]

62. We would like to ask you a few questions about the specifics of your background.

a. What is your primary day-to-day occupation?
- I attend school
- I am ill/disabled
- I care for family members
- I am unemployed/looking for work
- I have a paid job
- I work as an unpaid volunteer
- I am retired
- Other, please specify:

b. Do you have a partner with whom you have been in a relationship for at least three months?
- No, I do not have a partner
- Yes, and I live with my partner (married or unmarried)
- Yes, but my partner and I do not live together

c. How many people are there in your household, including yourself?
... people aged 16 or older
... people younger than 16 years

[objective measurement of online behaviour]

[registration date/time and type of device]

[the "authority" persuasion technique will be applied to 1/3 of participants:]
The researchers from The Hague University of Applied Sciences and the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) emphatically request that you complete the following section in full.

[the "reciprocity" persuasion technique will be applied to 1/3 of participants:]
When you complete the following section in full, you will be entered for a chance to win a gift card in the amount of 100 euros.

[no persuasion technique will be applied to 1/3 of participants:]

d. What is your full name (first, middle and last)?

[] I'd rather not say

e. What is your email address?

[] I'd rather not say

f. Please provide an email address for one of your acquaintances, friends or family members (*we will contact them solely in order to ask them to take part in this study*).

[] I'd rather not say

g. What is your date of birth?

[] I'd rather not say

h. What is your postal code (for example: 1234AA)?

[] I'd rather not say

i. What is your house number?

[] I'd rather not say

j. Here below, please enter the missing digits of your bank account number. Note: for privacy reasons, we are only asking for a few digits.

xxxxxxxxxxxxxx□□ □

[] I'd rather not say

63. At the start of this questionnaire, we asked you to create an account. Is the password you entered similar to the passwords you usually create in order to protect your personal data?

- No, I chose a <u>simpler</u> password than I usually would
- No, I chose a <u>more complex</u> password than I usually would
- Yes, I chose a password in the same way I usually do

[Disclosure]

This is the end of this questionnaire. First of all, we would like to thank you for taking part in this survey.

We would also like to share with you some additional information about the questionnaire you have just completed. At the start of the questionnaire, we indicated that this survey would be about people's online activities. In reality, the survey was also aimed at another topic: safe internet usage. Using the results of this survey, the researchers will be able to map out the online behaviour of people in the Netherlands, with our ultimate goal being to help Dutch citizens to better protect themselves from internet criminals.

In order to conduct effective research on this topic, it was necessary (at several points in the survey) to avoid telling you the real reason why we were asking you certain questions. Below, we will explain at which points this was the case, along with how and why we did this.

Creating an account:
At the very beginning of the survey, you were asked to create an account. The purpose of this question was to determine whether Dutch people know what constitutes a strong password and whether they actually put this knowledge into practice in their lives. A special program that analyses how strong passwords are will be used to determine the strength of your password. Your password itself will not be retained by the panel company and will not be shared with the researchers or other parties in any form. Only the strength of your password will be shared with the researchers.

Clicking on a link:
Next, you were asked to clink a link in order to install a file, with the explanation that this was necessary because a video would not play otherwise. The purpose of this question was to investigate whether participants in this study would click on a link to install software when there were indications that the software in question was from a suspicious source. Regardless of your answer, no software was actually installed on your device in any way, shape or form. You were also told that you had 5 minutes to complete this section. A number of participants were asked to complete this portion quickly. This was intended to help researchers see whether participants were more likely to download software when facing time pressure.

Sharing personal information:
At the end of the survey, you were asked to share personal information with us, such as a portion of your bank account number. The purpose of this question was to study whether respondents would in fact share such personal information with third parties. The panel company will not retain or store the data you entered in any form and the researchers will be told only *whether* you entered an answer, not what that answer was.

We hope you understand and thank you once again for your participation.

For more information or if you have any questions, you may contact the panel company's help desk.

The researchers