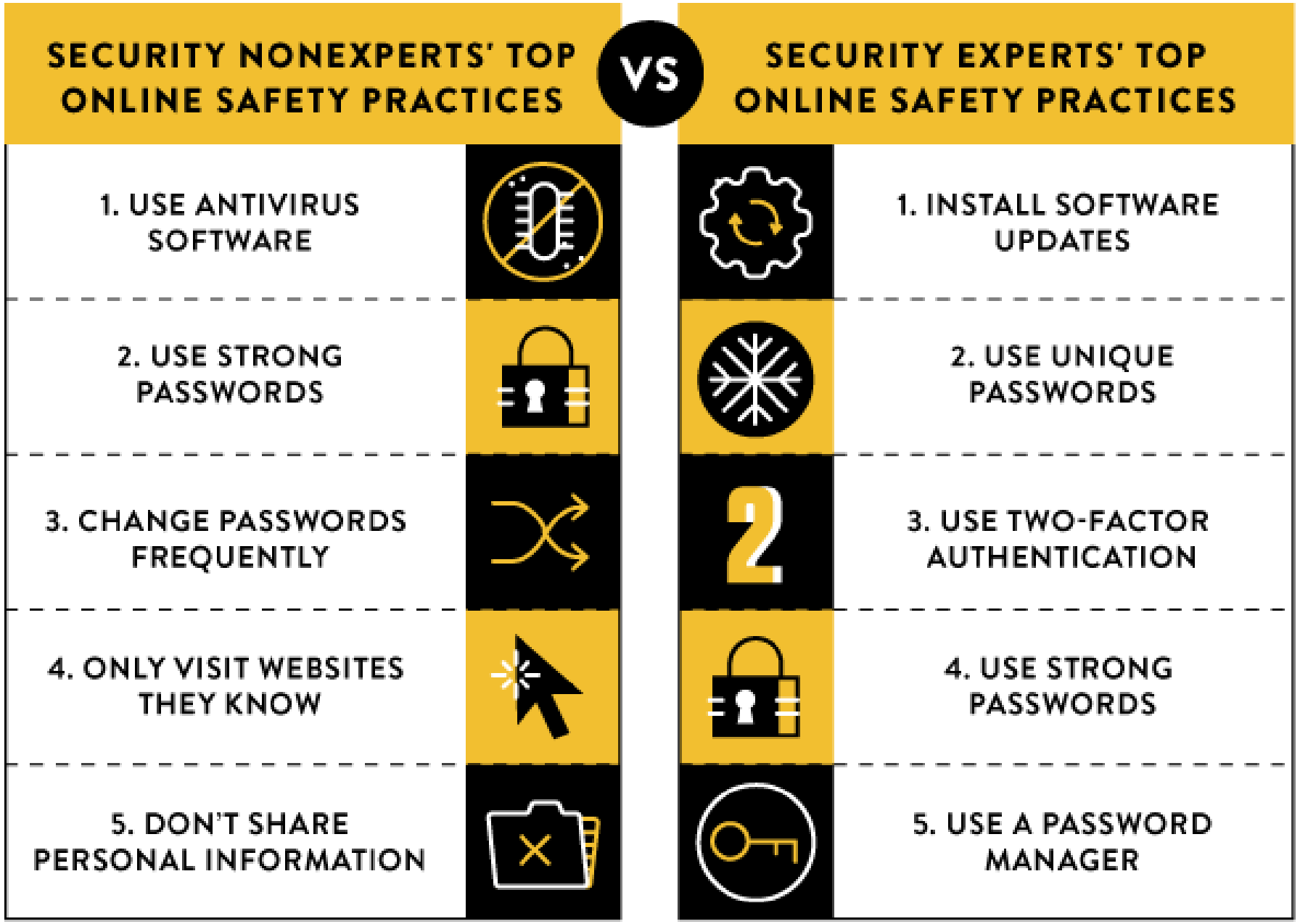
ECE750: Usable Security and Privacy
Advice

Dr. Kami Vaniea,
Electrical and Computer Engineering
kami.vaniea@uwaterloo.ca

First, something random...

- First 5 minutes we talk about something interesting, often from recent events
- You will not be tested on the 5 minutes part of lecture
- This part of lecture will sometimes not be recorded
- Why do this?
    1. Some students show up late
    2. Reward students who show up on time
    3. Important to see real world examples



https://googleonlinesecurity.blogspot.com.au/2015/07/new-research-comparing-how-security.html

In the next few slides I want to make three points:

1. People give other people piles of advice all the time

2. The advice being given out can tell you a lot about what people think is important or what is broken about a situation

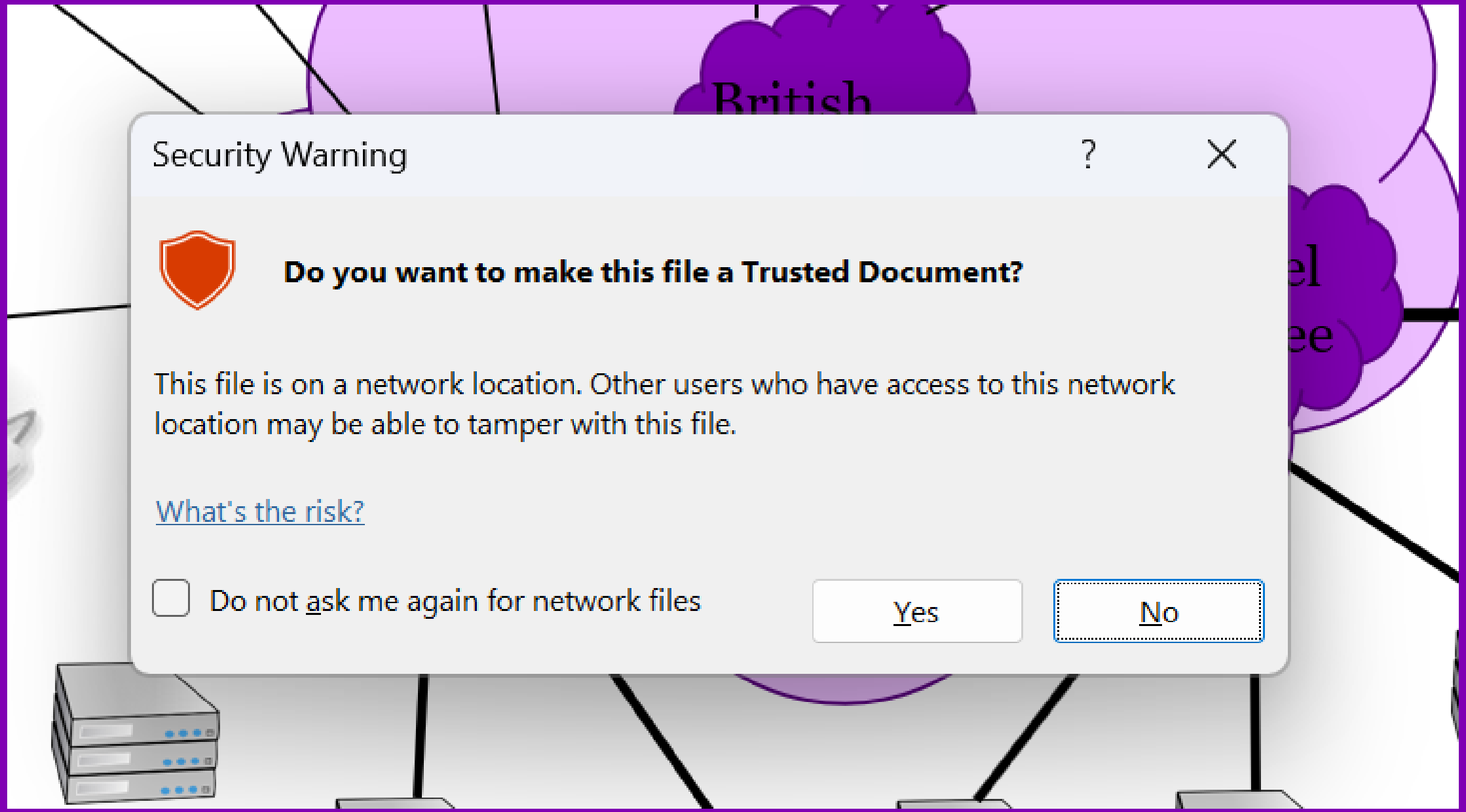
3. Warnings are a type of advice


Windows Security
These files might be harmful to your computer
Your Internet security settings suggest that one or more files may be harmful. Do you want to use it anyway?
C:\Users\kvaniea\Desktop
Hide details
OK
Cancel
How do I decide whether to unblock these files?

Interest-Based Ads Notice

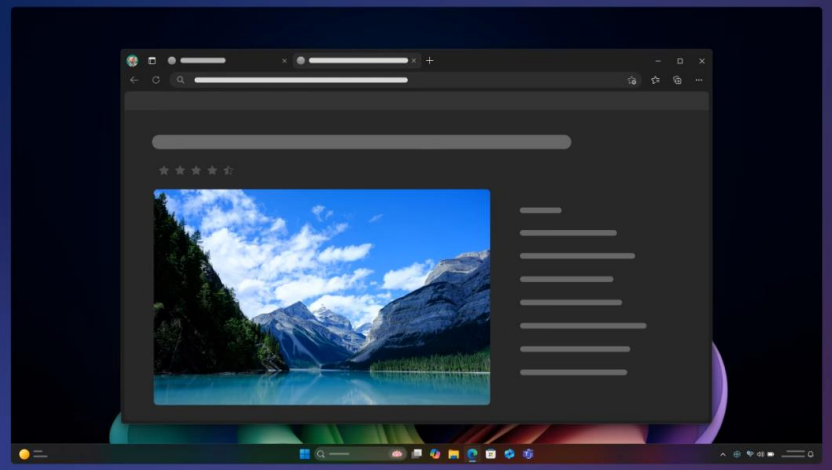
We show interest-based ads (sometimes referred to as personalized or targeted ads) to display features, products, or services that may be of interest to you. To learn more, or to adjust your preferences, please refer to our Interest-Based Ads page.

Continue Shopping


British
Security Warning
?
Do you want to make this file a Trusted Document?
This file is on a network location. Other users who have access to this network location may be able to tamper with this file.
What's the risk?
Do not ask me again for network files
Yes
No

Recall (preview)

Type here to search your history



You're in control of your privacy

You'll see the Recall icon in the system tray when snapshots are being saved:

From here, you can pause snapshots and choose apps and websites to filter out. You'll find more options in Settings, like deleting snapshots.

Snapshots aren't saved when you use private browsing in supported browsers.

Back

Next

https://accounts.google.com/signin/v2/passkeyenrollment?TL=ADBLaQBSIQ3coe8H8bodUyZDzoYGenjC

accounts.google.com is requesting extended information about your security key, which may affect your privacy.

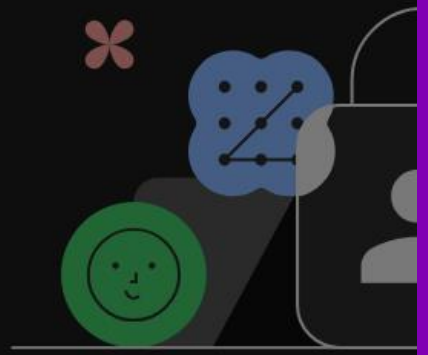
Firefox can anonymize this for you, but the website might decline this key. If declined, you can try again.

Learn more

Allow Block

Simplify your sign-in

kami.vaniea@gmail.com



With passkeys you can now use you

Wacom Experience Program

Wacom Experience Program for Tablet Driver

Help us improve our products!

When you participate in the Wacom Experience Program for Tablet Driver, the Tablet Driver will automatically send us diagnostics and usage data for your Wacom product.

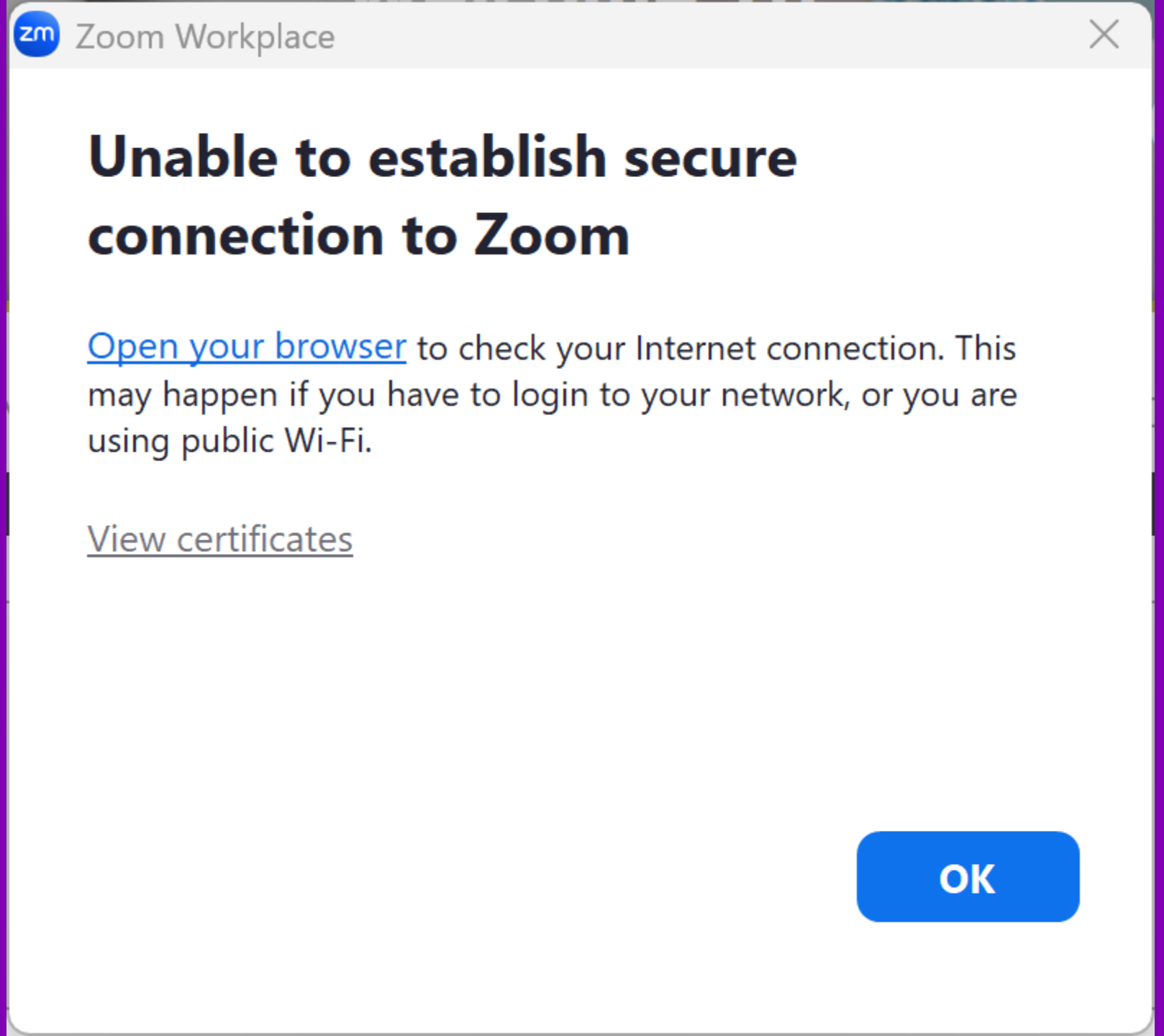
Information on the Wacom Experience Program for Tablet Driver can be found here:

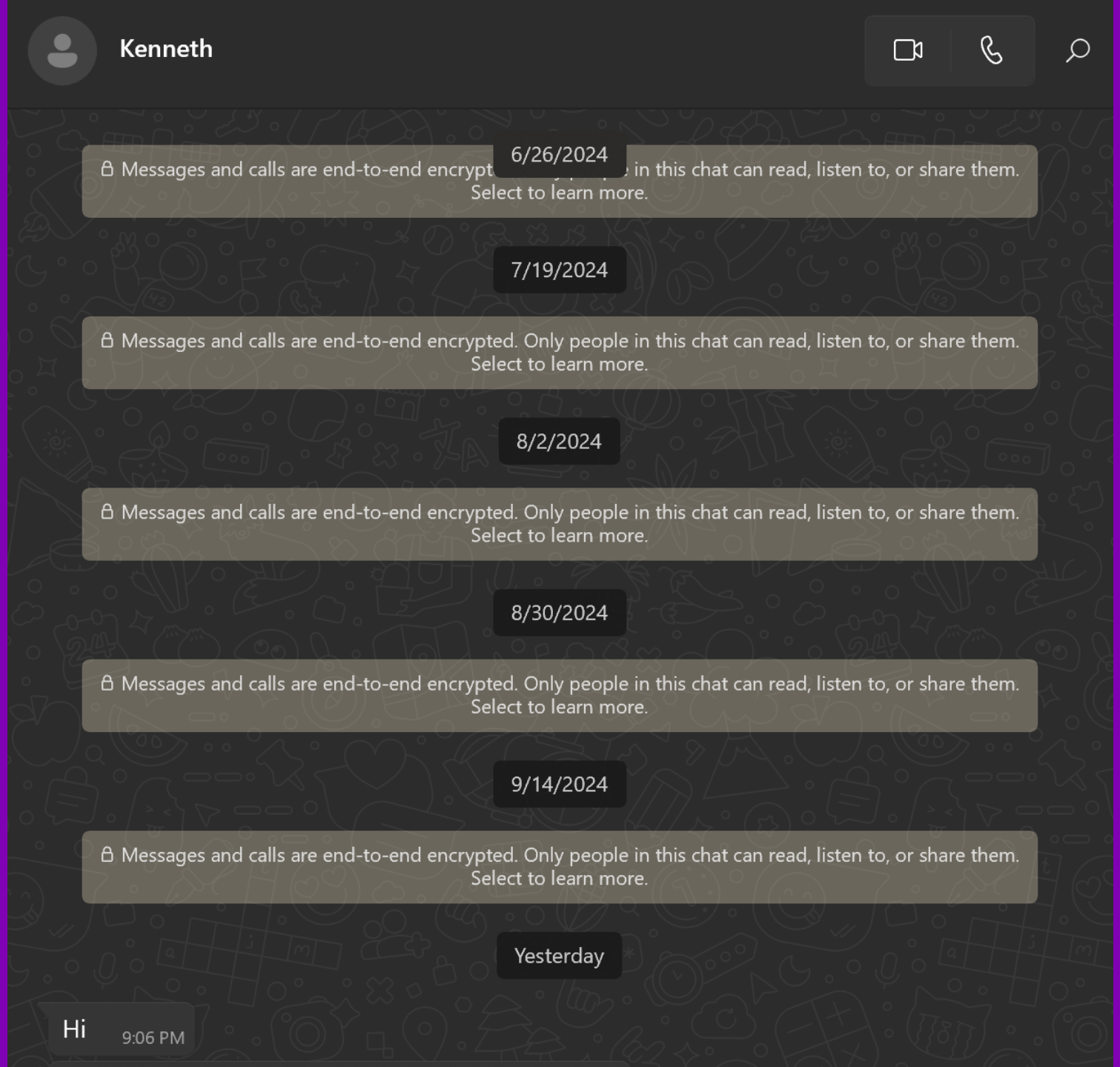
Tablet Driver Privacy Notice

You can change your preference at any time from Wacom Center.

☐ By checking the box, you opt-in to participate in the Wacom Experience Program for Tablet Driver that helps Wacom to improve its tablet driver and products. Participation is optional.

OK


Zoom Workplace
Unable to establish secure connection to Zoom
Open your browser to check your Internet connection. This may happen if you have to login to your network, or you are using public Wi-Fi.
View certificates
OK


Kenneth
6/26/2024
Messages and calls are end-to-end encrypt in this chat can read, listen to, or share them. Select to learn more.
7/19/2024
Messages and calls are end-to-end encrypted. Only people in this chat can read, listen to, or share them. Select to learn more.
8/2/2024
Messages and calls are end-to-end encrypted. Only people in this chat can read, listen to, or share them. Select to learn more.
8/30/2024
Messages and calls are end-to-end encrypted. Only people in this chat can read, listen to, or share them. Select to learn more.
9/14/2024
Messages and calls are end-to-end encrypted. Only people in this chat can read, listen to, or share them. Select to learn more.
Yesterday
Hi
9:06 PM

Welcome to your free Wi-Fi

Enjoy free Wi-Fi on Great Northern trains. Enter your email address to log in.

New user? **Register to use the Wi-Fi**.

Email *

I accept the terms and conditions. *

Connect

If you experience any issues with this Wi-Fi service, please **Contact Us**.

Visit our website

Head to **our website** for latest customer information and updates, plus travel inspiration to help you plan your next journey.

In today’s lecture we will learn how to create useful communications with users on security topics.

Study of where US internet users get advice and what advice they trust

How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior

Elissa M. Redmiles, Sean Kross†, and Michelle L. Mazurek
University of Maryland †Johns Hopkins University

ABSTRACT

Few users have a single, authoritative, source from whom they can request digital-security advice. Rather, digital-security skills are often learned haphazardly, as users filter through an overwhelming quantity of security advice. By understanding the factors that contribute to users' advice sources, beliefs, and security behaviors, we can help to pare down the quantity and improve the quality of advice provided to users, streamlining the process of learning key behaviors. This paper rigorously investigates how users' security beliefs, knowledge, and demographics correlate with their sources of security advice, and how all these factors influence security behaviors. Using a carefully pretested, U.S.-census-representative survey of 526 users, we present an overview of the prevalence of respondents' advice sources, reasons for accepting and rejecting advice from those sources, and the impact of these sources and demographic factors on security behavior. We find evidence of a "digital divide" in security: the advice sources of users with higher skill levels and socioeconomic status differ from those with fewer resources. This digital security divide may add to

users collect digital-security advice haphazardly from a variety of sources including workplaces, the media, and stories of negative experiences that have happened to family and friends [9, 47, 48]. While a plethora of security advice is available from seemingly authoritative sources such as US CERT and Microsoft [1,2], and yet more is provided casually by friends and acquaintances, users adopt only a fraction of it. Further, it is unclear how useful and effective advice from these various sources may be, or whether the advice that is accepted is the most valuable.

Little effort, however, has gone toward understanding how and why users opt to adopt some recommended behaviors but reject others. Most prior research has instead focused on teaching users individual security-promoting behaviors such as phishing awareness [7, 11, 18, 21, 41, 50, 53, 56, 63]. A smaller set of prior work has hypothesized general models for understanding how security behaviors develop, but these models either have not been empirically validated [26] or have been based on small samples of 25 users or fewer [9,48].

In this work, we present the first large-scale empirical analysis of how users' security beliefs, knowledge, and de-

Census-representative means that they selected people to match a given population's demographics, in this case the USA.

Metric	Sample	Census
Male	49%	49%
Female	50%	51%
Caucasian	69%	64%
Hispanic	11%	16%
African American	12%	12%
Other	8%	8%
Some HS	3%	8%
Completed HS	23%	28%
Completed Some College	25%	18%
Associates Degree	10%	9%
College Degree	26%	26%
Master's	10%	7%
Doctoral	4%	4%
18-29 years	22%	23%
30-39 years	20%	17%
40-49 years	19%	17%
50-59 years	16%	18%
60-69 years	15%	14%
70+ years	8%	11%
<$30k	26%	32%
$30k-$50k	19%	19%
$50k-$75k	17%	18%
$75k-$100k	13%	11%
$100k-$150k	14%	12%
$150k+	9%	8%

Table 2: Demographics of participants in our sample. Some percentages may not add to 100% due to item non-response. Census statistics from the American Community Survey [3].

E. Redmiles, S. Kross, and M.L. Mazurek. "How I learned to be secure: a census-representative survey of security advice sources and behavior." *In SIGSAC* 2016.

Where people learn security behaviors

- Notable:
  - Prompt – 81%
  - Auto/Forced – 52%
    - Automatic update caused them to update
  - Family/Friends – 42%
  - Work – 29%

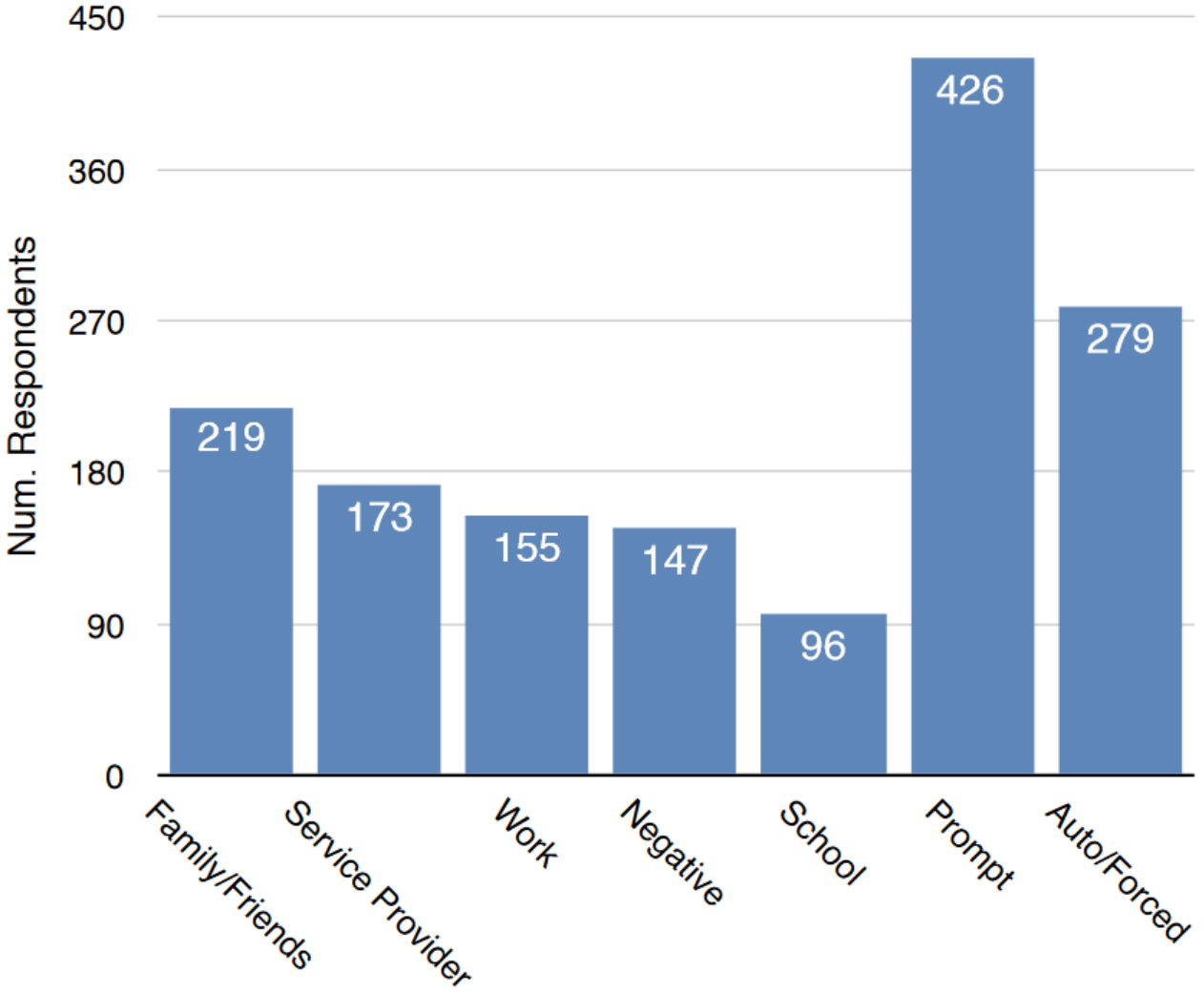


Figure 1: Prevalence of advice sources.

E. Redmiles, S. Kross, and M.L. Mazurek. "How I learned to be secure: a census-representative survey of security advice sources and behavior." *In SIGSAC* 2016.

Advice sources

- Focus on 4 security behaviors

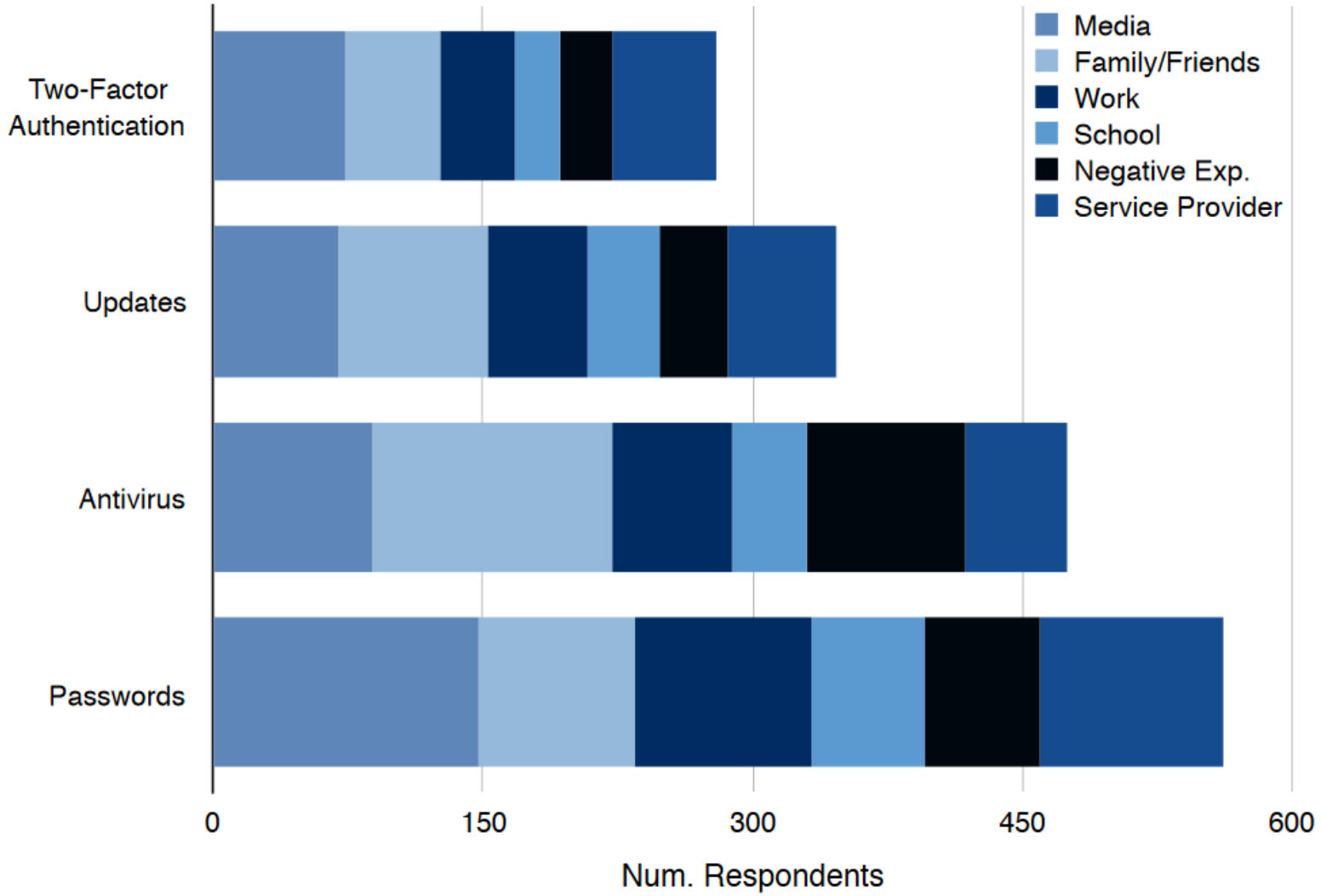


Figure 4: Advice source prevalence by behavior.

E. Redmiles, S. Kross, and M.L. Mazurek. "How I learned to be secure: a census-representative survey of security advice sources and behavior." *In SIGSAC* 2016.

Reasons for accepting advice

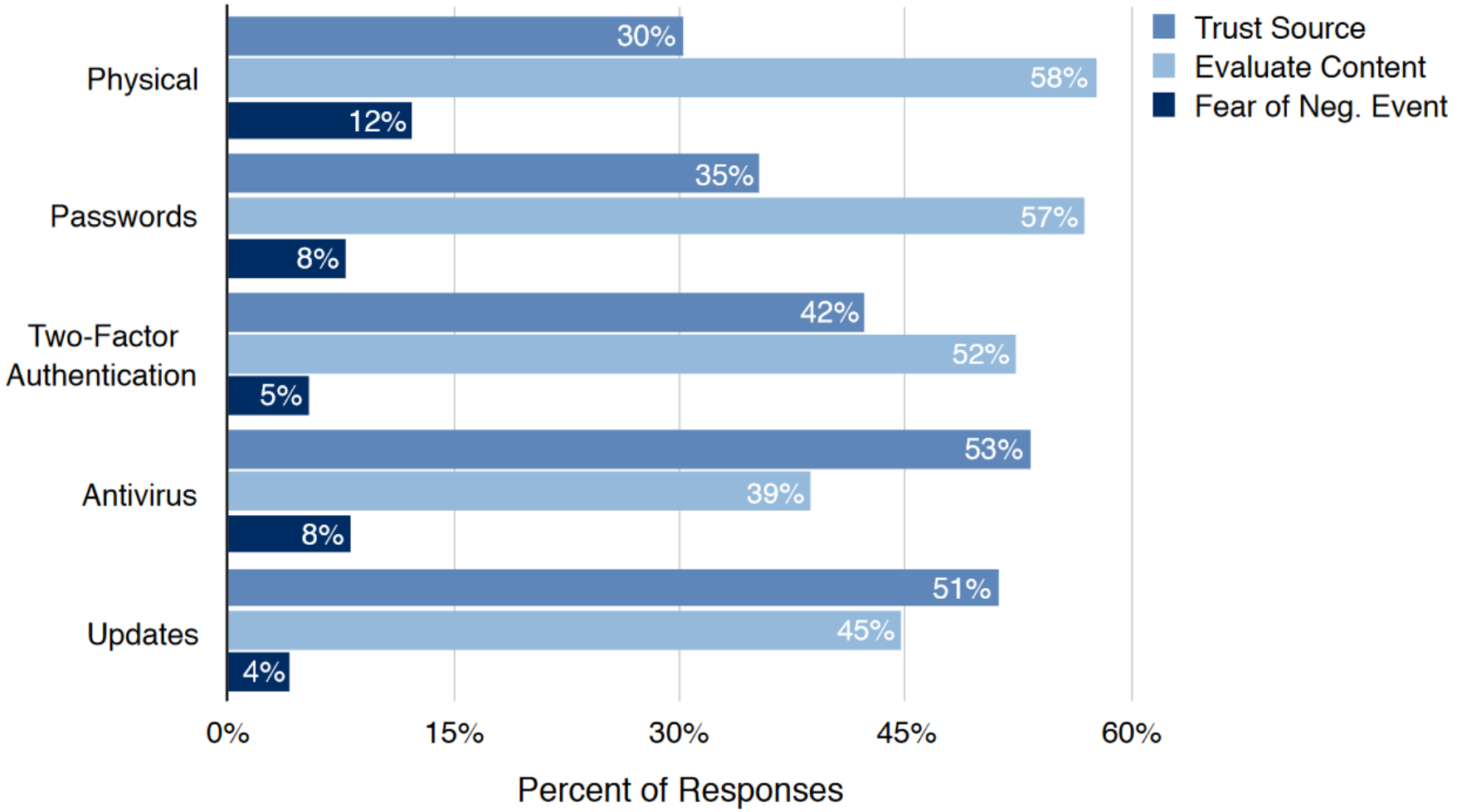


Figure 2: Reasons for accepting digital-security advice. Percentage per behavior.

E. Redmiles, S. Kross, and M.L. Mazurek. "How I learned to be secure: a census-representative survey of security advice sources and behavior." *In SIGSAC* 2016.

Reasons for rejecting

- 43% rejected at least one of the three behaviors
- *Lack* of negative experience – 13%
  - As in: "nothing bad has happened so I don't really need X."
- "They were trying to sell me something" – 33% rejected anti-virus software

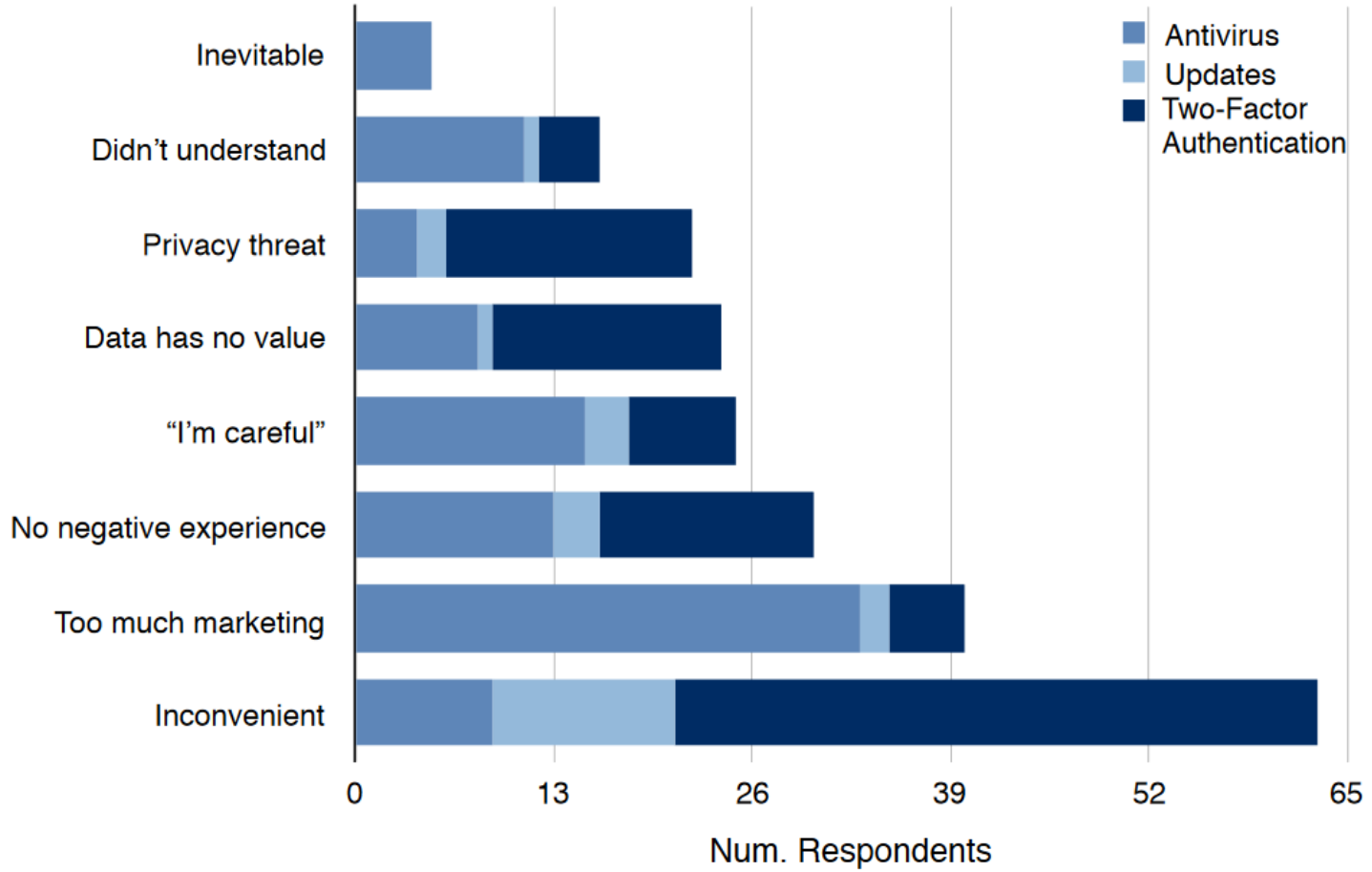
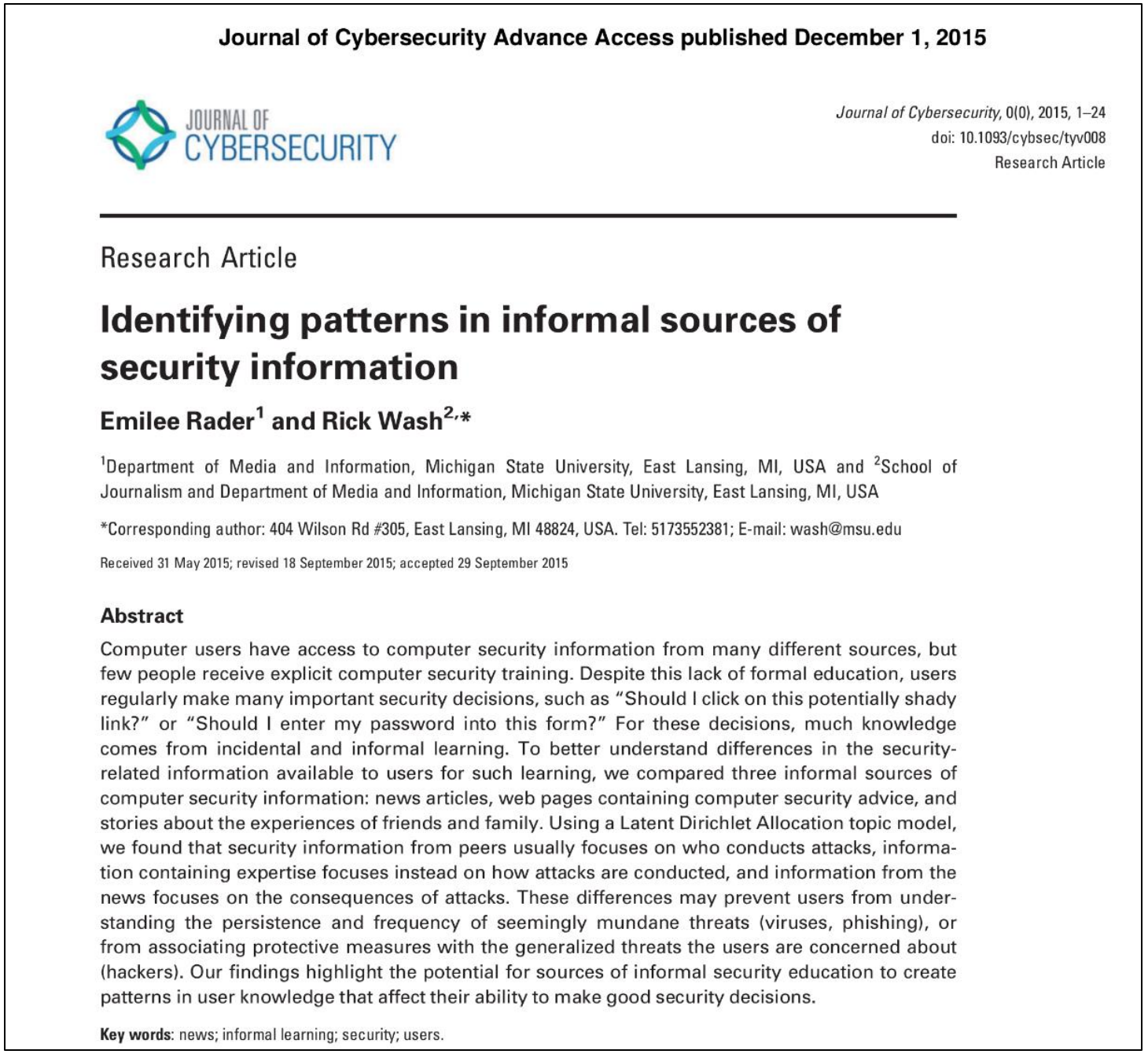


Figure 3: Reasons for rejecting digital-security advice. Total per behavior, multiple responses possible. This question was not asked for passwords, as not using them is rarely, if ever, an option.

E. Redmiles, S. Kross, and M.L. Mazurek. "How I learned to be secure: a census-representative survey of security advice sources and behavior." *In SIGSAC* 2016.

Study of the content of different information sources



Journal of Cybersecurity Advance Access published December 1, 2015

JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 0(0), 2015, 1–24
doi: 10.1093/cybsec/tyv008
Research Article

Research Article

Identifying patterns in informal sources of security information

Emilee Rader[1] and Rick Wash[2,*]

[1]Department of Media and Information, Michigan State University, East Lansing, MI, USA and [2]School of Journalism and Department of Media and Information, Michigan State University, East Lansing, MI, USA

*Corresponding author: 404 Wilson Rd #305, East Lansing, MI 48824, USA. Tel: 5173552381; E-mail: wash@msu.edu

Received 31 May 2015; revised 18 September 2015; accepted 29 September 2015

Abstract

Computer users have access to computer security information from many different sources, but few people receive explicit computer security training. Despite this lack of formal education, users regularly make many important security decisions, such as "Should I click on this potentially shady link?" or "Should I enter my password into this form?" For these decisions, much knowledge comes from incidental and informal learning. To better understand differences in the security-related information available to users for such learning, we compared three informal sources of computer security information: news articles, web pages containing computer security advice, and stories about the experiences of friends and family. Using a Latent Dirichlet Allocation topic model, we found that security information from peers usually focuses on who conducts attacks, information containing expertise focuses instead on how attacks are conducted, and information from the news focuses on the consequences of attacks. These differences may prevent users from understanding the persistence and frequency of seemingly mundane threats (viruses, phishing), or from associating protective measures with the generalized threats the users are concerned about (hackers). Our findings highlight the potential for sources of informal security education to create patterns in user knowledge that affect their ability to make good security decisions.

Key words: news; informal learning; security; users.

Rader, E. and Wash, R., 2015. Identifying patterns in informal sources of security information. *Journal of Cybersecurity*.

Compared:

- Websites
  - Advice posted on websites like Universities, government sites, companies
- News
  - Security information in news articles
- Stories
  - Stories people tell each other, info drawn from an earlier survey study

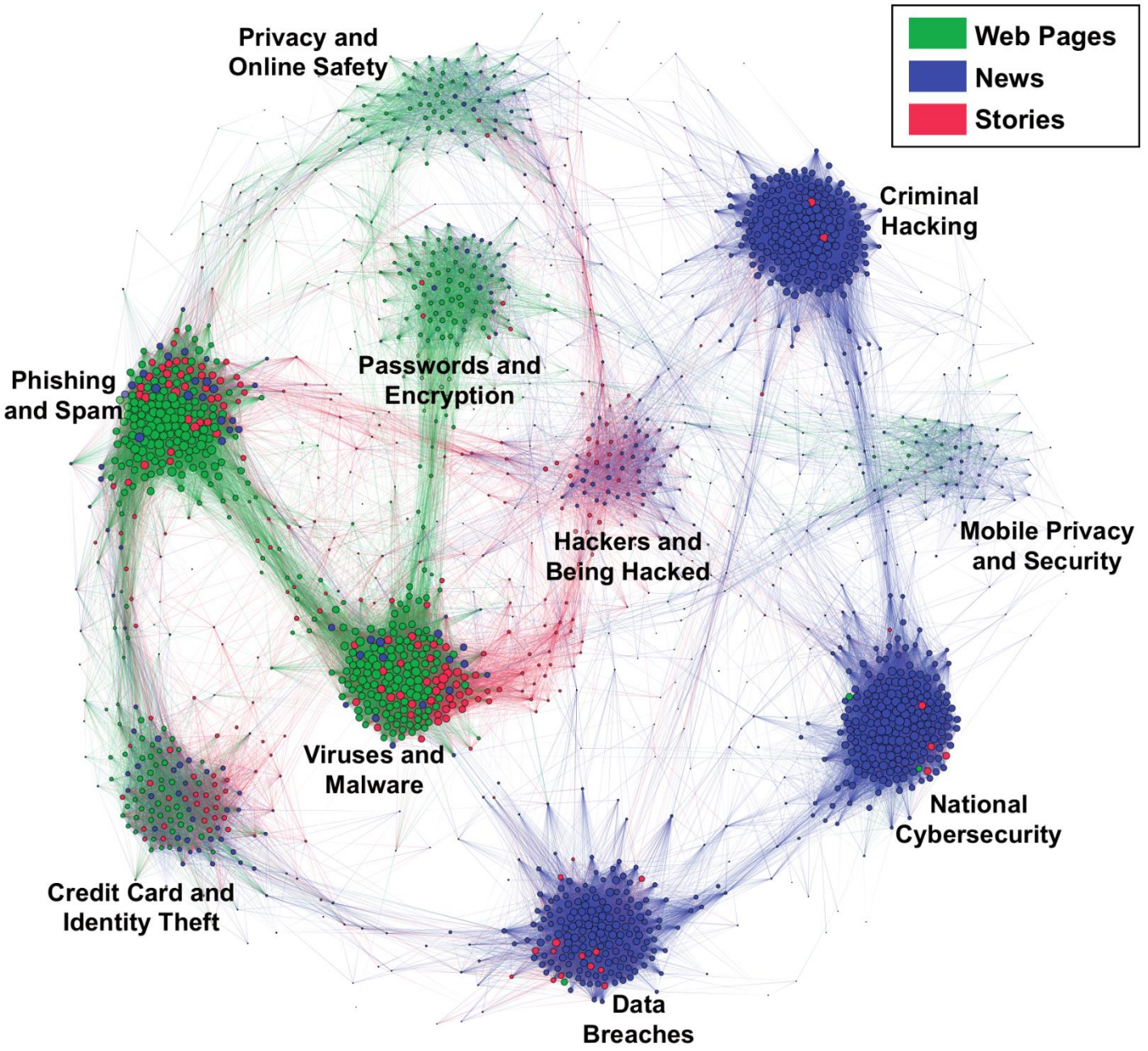


Figure 8. The document similarity graph, with clusters for each topic. There is one node for each document in the dataset. The red nodes are stories, green are web pages, and blue are news articles. Larger nodes are connected to more other documents. Edges represent the Pearson correlation between the topic vectors for a pair of documents.

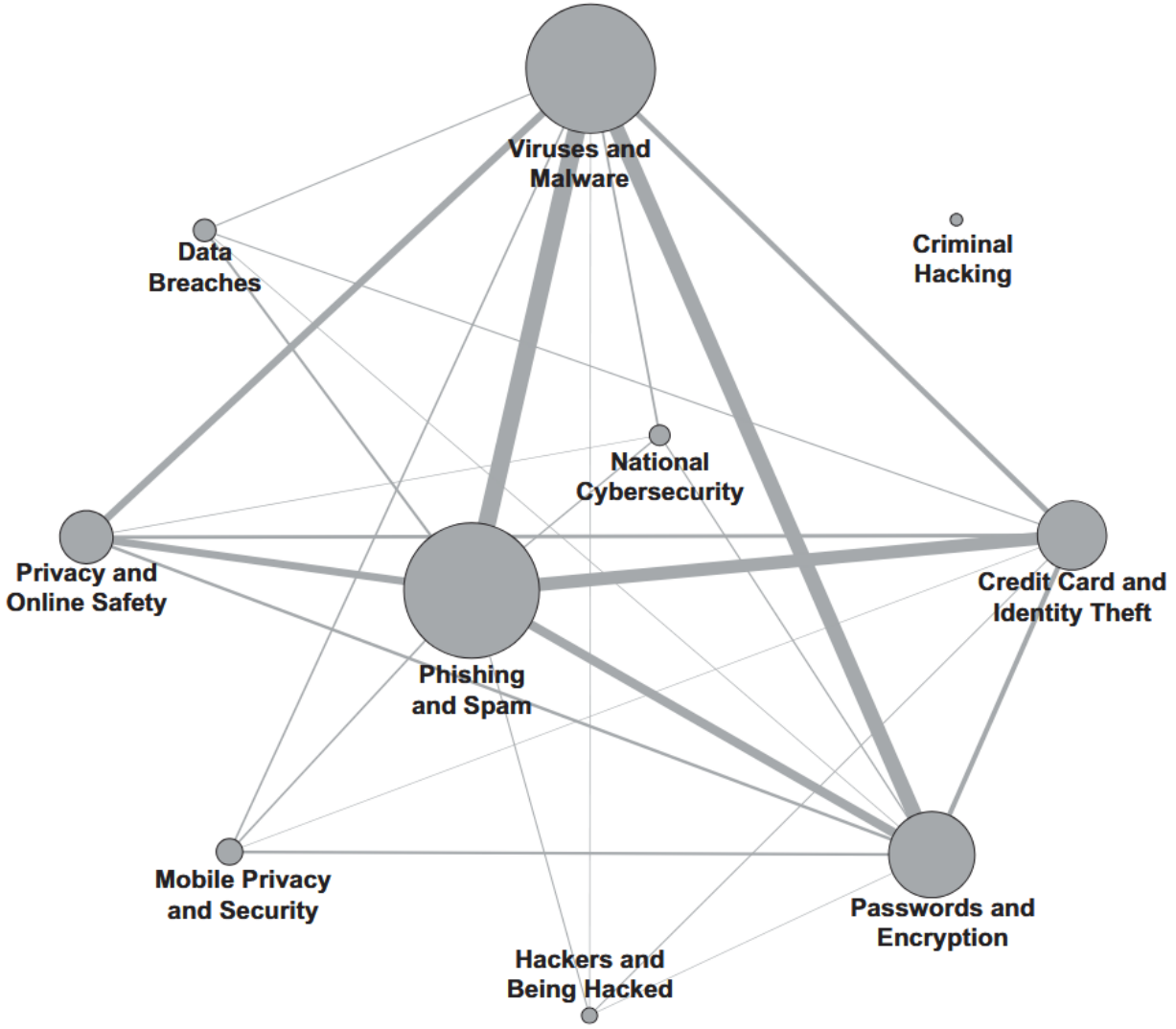
Rader, E. and Wash, R., 2015. Identifying patterns in informal sources of security information. *Journal of Cybersecurity*.

Topic co-occurrence

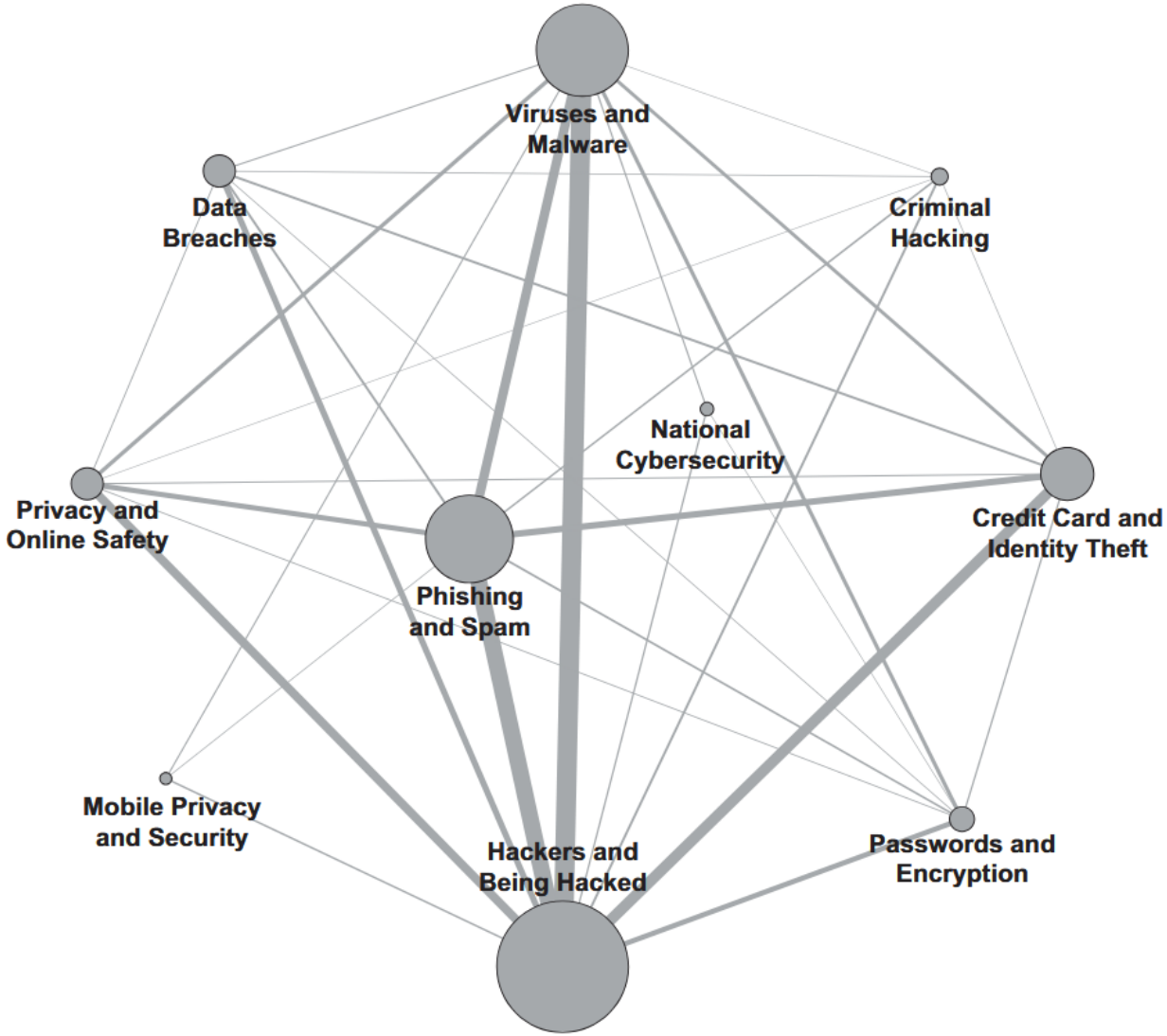
- The lines show frequencies of two topics both appearing in the same story
- Hackers, for example, often co-occur with Viruses and with Phishing
- National Cybersecurity rarely occurs

Rader, E. and Wash, R., 2015. Identifying patterns in informal sources of security information. *Journal of Cybersecurity*.

Education websites

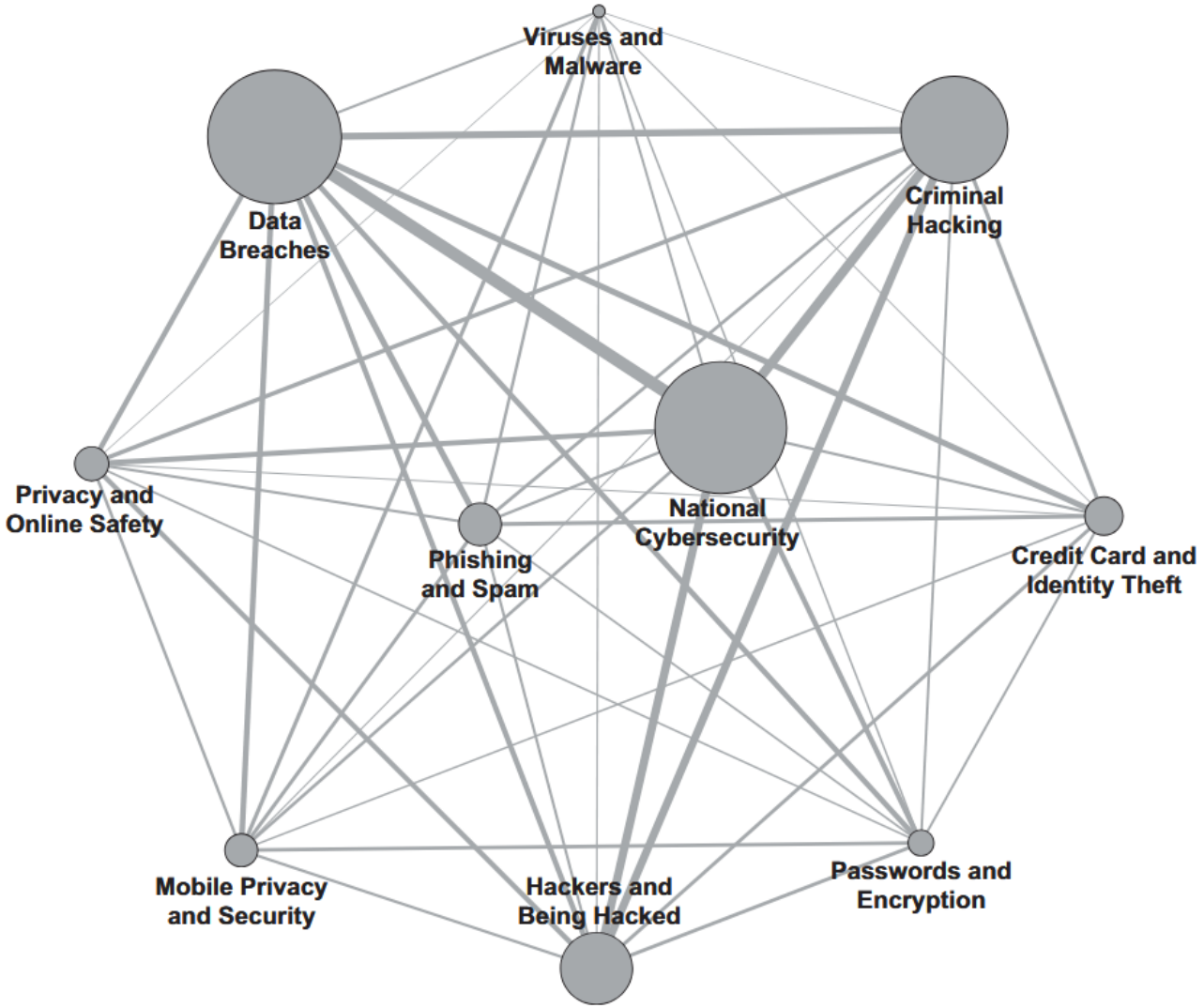


Stories told by people

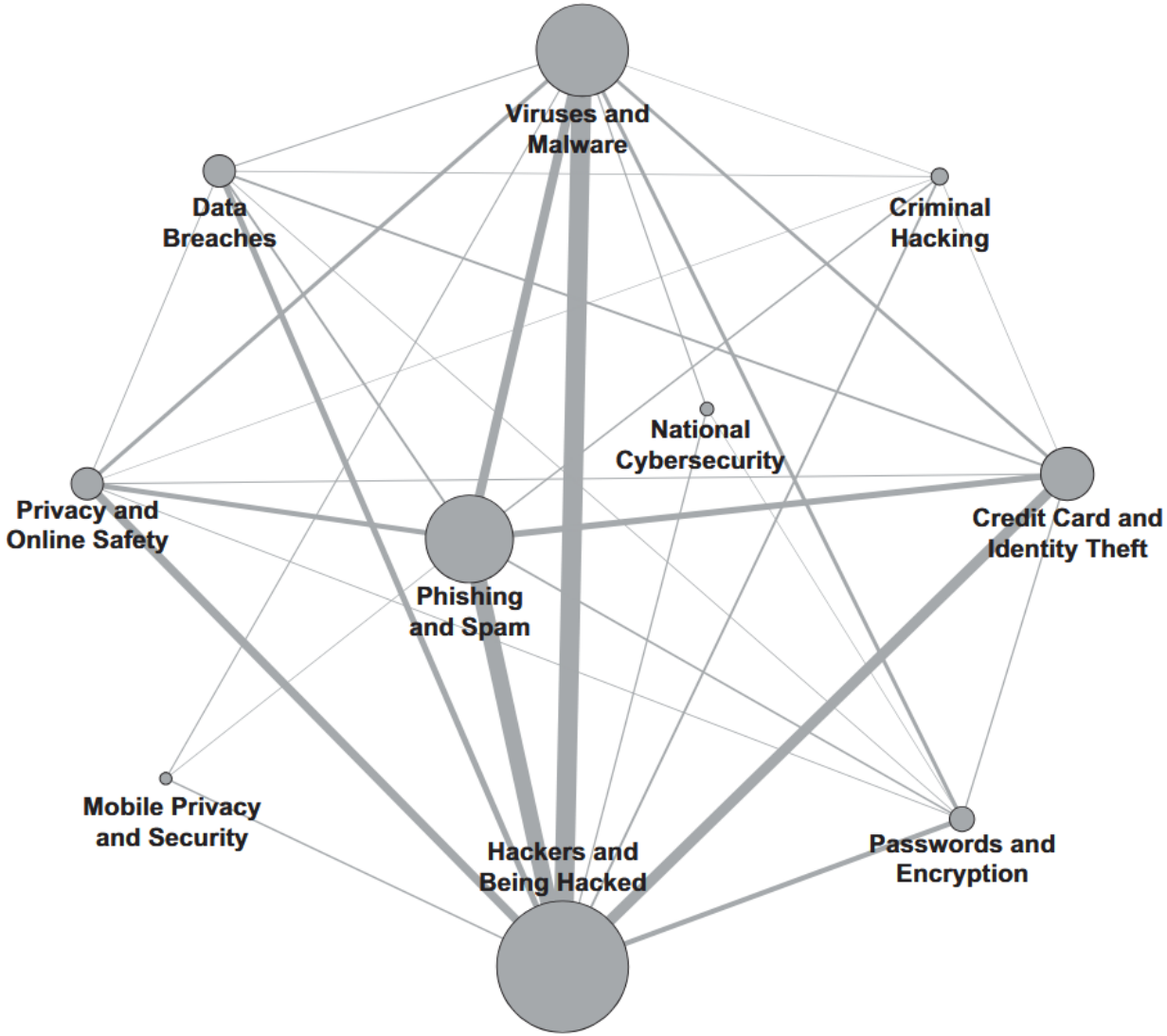


Rader, E. and Wash, R., 2015. Identifying patterns in informal sources of security information. *Journal of Cybersecurity*.

News articles



Stories told by people



Rader, E. and Wash, R., 2015. Identifying patterns in informal sources of security information. *Journal of Cybersecurity*.

Study of online advice aimed at Black Lives Matter protesters

Understanding the Security and Privacy Advice Given to Black Lives Matter Protesters

Maia J. Boyd
University of Chicago
mboyd6@uchicago.edu

Jamar L. Sullivan Jr.
University of Chicago
jlsullivan2@uchicago.edu

Marshini Chetty
University of Chicago
marshini@uchicago.edu

Blase Ur
University of Chicago
blase@uchicago.edu

ABSTRACT

In 2020, there were widespread Black Lives Matter (BLM) protests in the U.S. Because many attendees were novice protesters, organizations distributed guides for staying safe at a protest, often including security and privacy advice. To understand what advice novice protesters are given, we collected 41 safety guides distributed during BLM protests in spring 2020. We identified 13 classes of digital security and privacy advice in these guides. To understand whether this advice influences protesters, we surveyed 167 BLM protesters. Respondents reported an array of security and privacy concerns, and their concerns were magnified when considering fellow protesters. While most respondents reported being aware of, and following, certain advice (e.g., choosing a strong phone passcode), many were unaware of key advice like using end-to-end encrypted messengers and disabling biometric phone unlocking. Our results can guide future advice and technologies to help novice protesters protect their security and privacy.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**.

KEYWORDS

BlackLivesMatter, Activism, Security, Black Lives Matter, BLM, Security Advice, Privacy

ACM Reference Format:
Maia J. Boyd, Jamar L. Sullivan Jr., Marshini Chetty, and Blase Ur. 2021. Understanding the Security and Privacy Advice Given to Black Lives Matter Protesters. In *CHI Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3411764.3445061

in May. These events led to widespread protests in the US and internationally. An estimated 15–26 million Americans participated in these protests for the Black Lives Matter (**BLM**) movement to spur change against racial injustice. In turn, these protesters faced privacy and security threats from police and others attempting to surveil or harm the movement [41, 82, 86, 91]. Because many attendees of these protests were novice protesters, numerous organizations distributed **safety guides**, or succinct sets of advice for staying safe at a protest. These guides, such as those shown in Figure 1, often included digital security and privacy advice. Although there have been studies of how users follow security advice in general contexts [28, 39, 63, 65, 67, 68], the degree to which activists are informed about, and take advantage of, privacy and security advice remains an open question. Moreover, most HCI research on the BLM movement has focused on discourse online [2, 59, 76, 78, 81], rather than the role of technology in demonstrations and protests.

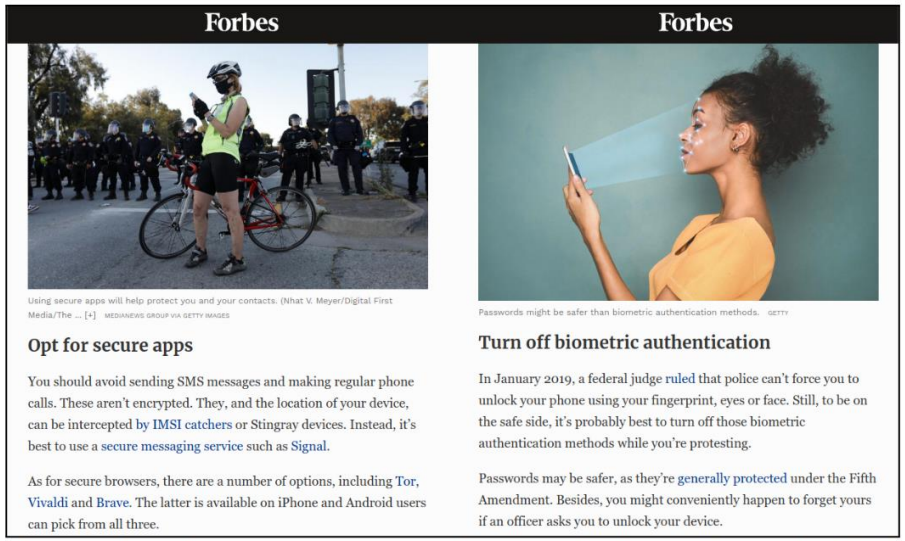
Towards helping activists stay safe at in-person protests, we answer two research questions within the context of the BLM movement.[1] First, we wanted to understand the spectrum of digital security and privacy advice novice BLM protesters are given in widely available safety guides. Second, we wanted to examine whether this advice is understood and used by novice BLM protesters. To answer these questions, we first collected 41 safety guides distributed on social media and the web during the spring 2020 BLM protests, performing content analysis on those guides. To understand whether this advice reaches and influences protesters, we then conducted an online survey of 167 BLM protesters, primarily novice protesters. The survey covered protesters' security and privacy concerns, knowledge of tools and strategies, and actions.

We identified 13 key classes of digital security and privacy advice given to novice protesters. The most common advice included disabling phones' transmission features (e.g., putting them in air-

Lots of advice

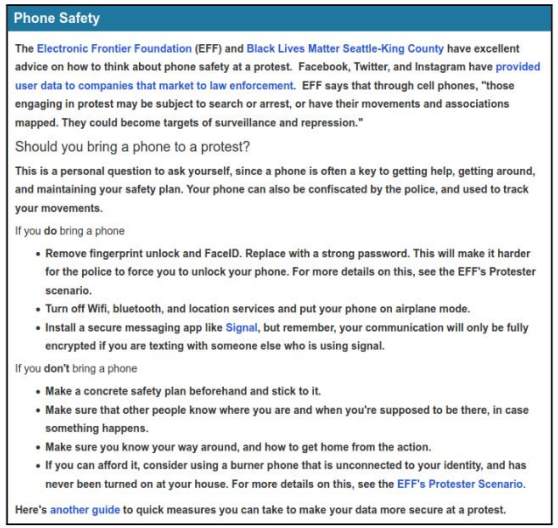
- Interesting user group
- Clear threat model
- Government / police considered to be a threat
- Serious possible consequences if identified

(a) The first and fourth images of a ten-image safety guide posted on Instagram [42], reformatted to be side-by-side.



(b) Two of the eleven privacy tips in a longer guide featured on Forbes [36], reformatted to be side-by-side.

(c) Infographic distributed on Twitter [80].



(d) From Seattle Central College [8].

(e) From BLM Belfast's guide [7].

Figure 1: Excerpts from safety guides for novice protesters distributed during BLM protests in June 2020.

Boyd, Maia J., et al. "Understanding the security and privacy advice given to black lives matter protesters." *In CHI conference on human factors in computing systems*. 2021.

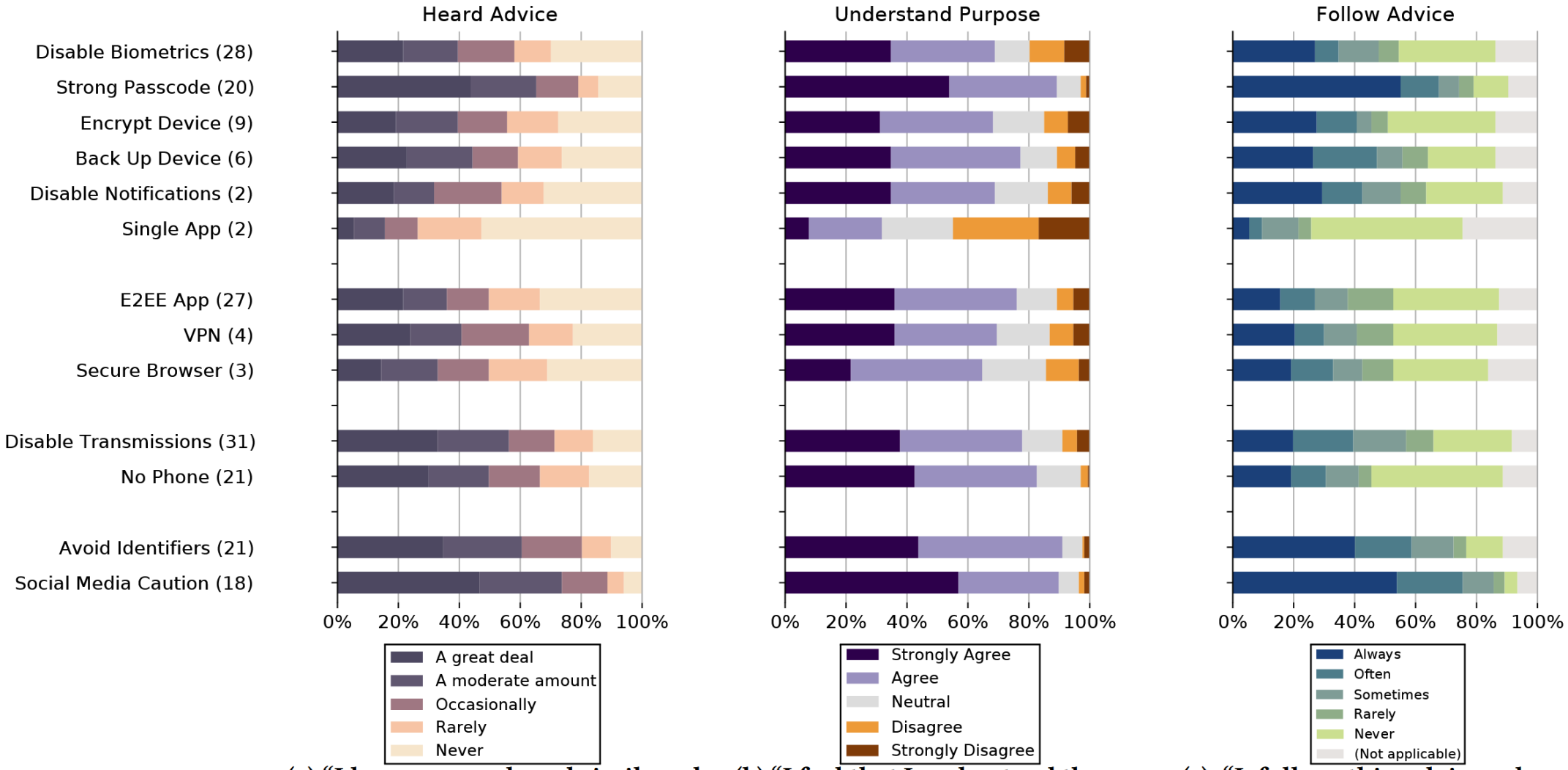
Advice found:

Table 3: The 13 classes of advice we studied and how they were presented to participants. We use the terminology from the left column throughout the rest of the paper.

Advice	Phrasing
Disable Biometrics	*"Disable biometric (face or fingerprint) unlocking for your phone. Use a password/passcode instead."*
Strong Passcode	*"Lock your phone with a strong password/passcode containing 6+ characters/digits."*
Encrypt Device	*"Encrypt your phone, which may require manually changing settings (Android) or setting a passcode (iOS)."*
Back Up Device	*"Back up your phone before attending a protest."*
Disable Notifications	*"Configure your phone not to show notifications when it is locked."*
Single App	*"Use the feature that limits your phone to the use of a single app."*
E2EE App	*"Use an end-to-end encrypted messaging app like Signal instead of sending text messages. Configure messages to disappear automatically."*
VPN	*"Use a VPN (Virtual Private Network)."*
Secure Browser	*"Use a security-focused web browser."*
Disable Transmissions	*"Turn off your phone completely or put it in airplane mode. Be sure to disable location services, turn off WiFi, turn off Bluetooth, and turn off cellular data."*
No Phone	*"Do not bring your primary phone to a protest. Leave it at home or use a burner phone unconnected to your identity."*
Avoid Identifiers	*"For photos and videos, avoid identifying information (people, their faces, their distinguishing features, and locations). Blur such information you capture, potentially with software. Remove photo metadata, such as by sharing screenshots of photos."*
Social Media Caution	*"Be careful about what you post on social media, especially documenting your participation in a protest. Consider how your posts might impact other protesters."*

Boyd, Maia J., et al. "Understanding the security and privacy advice given to black lives matter protesters." *In CHI conference on human factors in computing systems*. 2021.

Survey



(a) "I have seen or heard similar advice about attending a protest."

(b) "I feel that I understand the purpose of this advice about attending a protest."

(c) "I follow this advice when attending a protest."

Figure 3: Whether respondents had (a) heard about, (b) felt they understood the purpose of, and (c) followed particular advice. The number in parentheses for each class of advice indicates how many safety guides (out of 41) mentioned that advice.

Boyd, Maia J., et al. "Understanding the security and privacy advice given to black lives matter protesters." *In CHI conference on human factors in computing systems*. 2021.

Survey

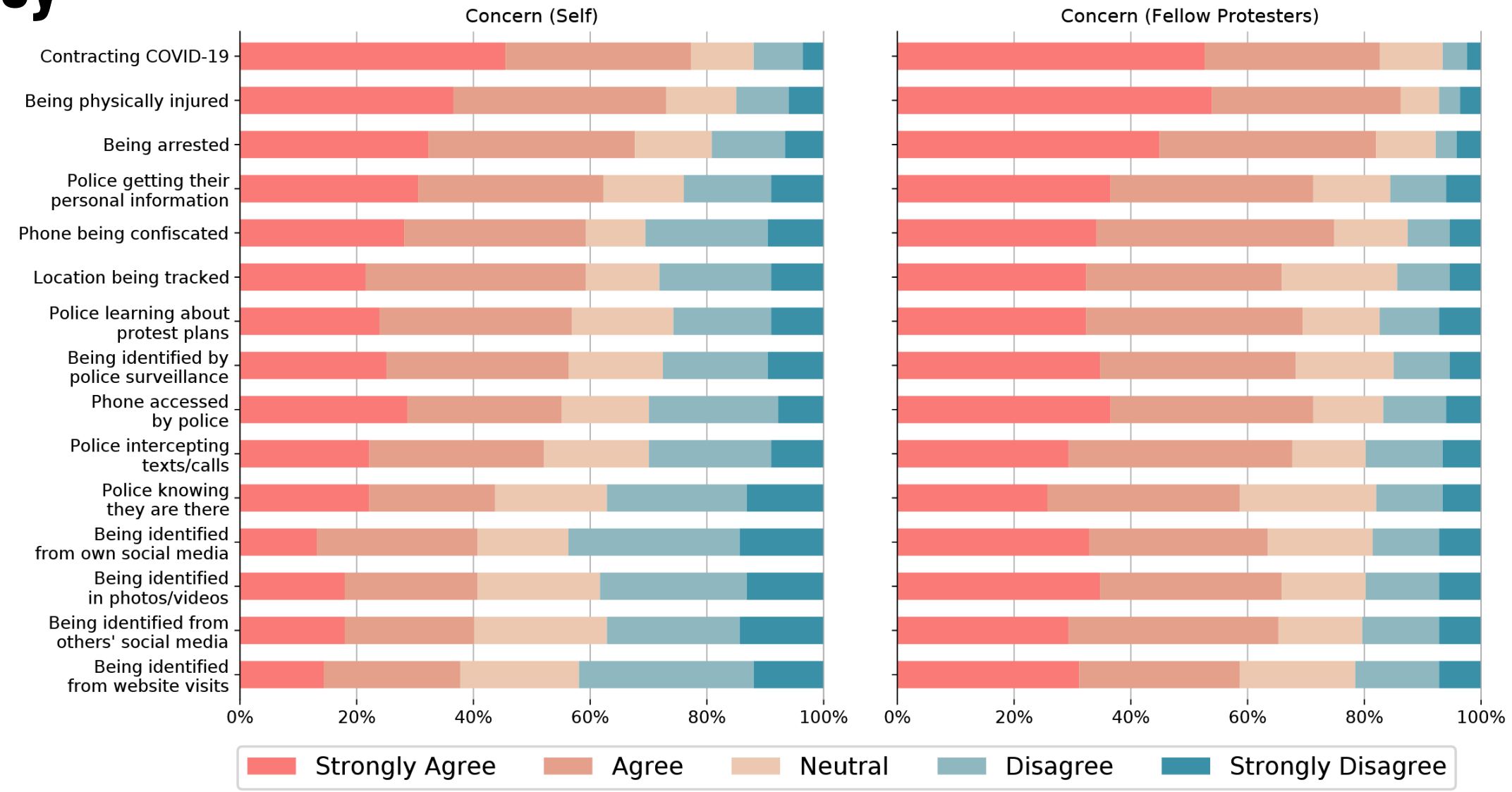


Figure 2: The distribution of respondents' level of concern about their own safety (L) and that of others (R) at BLM protests.

Boyd, Maia J., et al. "Understanding the security and privacy advice given to black lives matter protesters." *In CHI conference on human factors in computing systems*. 2021.

ADVICE SHOULD BE “WORTH IT” FOR PEOPLE

This paper was:

- Authored by a Microsoft employee based in Redmond
- They feel that ignoring security advice is rational but that the community disagrees
- Published in 2009
- Accepted by a top security (not HCI) conference. So top people in the field think this could be true.

So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users

Cormac Herley
Microsoft Research
One Microsoft Way
Redmond, WA, USA
cormac@microsoft.com

ABSTRACT

It is often suggested that users are hopelessly lazy and unmotivated on security questions. They chose weak passwords, ignore security warnings, and are oblivious to certificates errors. We argue that users' rejection of the security advice they receive is entirely rational from an economic perspective. The advice offers to shield them from the direct costs of attacks, but burdens them with far greater indirect costs in the form of effort. Looking at various examples of security advice we find that the advice is complex and growing, but the benefit is largely speculative or moot. For example, much of the advice concerning passwords is outdated and does little to address actual treats, and fully 100% of certificate error warnings appear to be false positives. Further, if users spent even a minute a day reading URLs to avoid phishing, the cost (in terms of user time) would be two orders of magnitude greater than all phishing losses. Thus we find that most security advice simply offers a poor cost-benefit tradeoff to users and is rejected. Security advice is a daily burden, applied to the whole population, while an upper bound on the benefit is the harm suffered by the fraction that become victims annually. When that fraction is small, designing security

ware, adware, malware, keyloggers, rootkits, and zombie and botnet applications. One study reports that an unpatched Windows PC will be compromised within 12 minutes of connecting to the Internet [1]. Things get yet worse: according to Schneier "Only amateurs attack machines; professionals target people." Users are the famously weak link in any security chain. It is easier to get information or passwords by social engineering than direct assault or brute-force. The best way to get software onto any machine is to get the user to instal it and human error is behind many of the most serious exploits [41, 43].

The main response of the security community to these threats against the human link has been user education. Users are given instructions, advice and mandates as to how to protect themselves and their machines. See, *e.g.* the US-Cyber Emergency Response Team (US-CERT) tips for end users [13]. Most large web-sites offer security tips to users, as do software vendors. Yet the relationship between users and user education has been a rocky one. Adams and Sasse [21] found that low motivation and poor understanding of the threats leads users to circumvent password security policies. This is certainly borne out by other data: a study of pass-

Costs and benefits of security advice

- Herley points out that following security advice has costs and benefits. These are modified by users' actual skills, and the relative value of different tasks.
- Theoretical benefits
- Actual benefits
- Costs

	Direct Costs	Indirect costs (*i.e.* externalities)
Attackers	Gain	Don't Care
Banks	Loss	Reputation
Victim Users	Possible Loss	Clean-up Effort
Non-victim Users	None	User Education

Table 1: Costs of online financial fraud. The direct costs are zero-sum: the attackers gain as much as the banks and victims lose. The externalities are indirect costs imposed on banks and non-victim users as they seek to avoid and deal with the consequences of the attacks. For many forms of fraud the externalities are many times greater than the direct costs.

Externalities vs Internalities

Externality – The costs or benefits of an activity are born by other groups or people.

Internality – The costs or benefits of an activity effect the user themselves.

Example: password composition rules

- Costs:
  - Select unique strong passwords for every site, do not write them down, change them periodically. Challenging for users.
- Benefits (potential)
  - Password will not be guessed if it is strong
  - Assuming that web servers lock an account after ~10 failed attempts, a 6 digit numeric pin is enough to protect an account from online attacks
  - In case the hashed password file is lost, a longer password will buy the user only hours, maybe days.
- Benefits (actual)
  - Most common attacks are: phishing, keylogging, and brute-force attack (try all combinations)
  - Stronger passwords only help against brute-force attacks and then only if the website isn't using lockout
- For most people, stronger passwords take more effort and do not protect against the most common attacks – wasted effort

Think-pair-share

- Select one piece of advice from yesterday – or just select one you have heard recently.
- What are the costs, potential benefits, and actual benefits of following that advice?

Study about how security awareness training sold by vendors to companies: “promises align with customers’ needs, …, and what narrative is presented regarding the role of employees”

Selling Satisfaction: A Qualitative Analysis of Cybersecurity Awareness Vendors’ Promises

Jonas Hielscher*
Chair for Human-Centred Security
Ruhr University Bochum
Bochum, Germany

Markus Schöps
Chair for Human-Centred Security
Ruhr University Bochum
Bochum, Germany

Jens Opdenbusch
Chair for Human-Centred Security
Ruhr University Bochum
Bochum, Germany

Felix Reichmann
Developer Centered Security
Ruhr University Bochum
Bochum, Germany

Marco Gutfleisch
Chair for Human-Centred Security
Ruhr University Bochum
Bochum, Germany

Karola Marky
Digital Sovereignty Lab
Ruhr University Bochum
Bochum, Germany

Simon Parkin
TPM Cybersecurity Group
Delft University of Technology
Delft, Netherlands

Abstract

Security awareness and training (SAT) vendors operate in a growing multi-billion dollar market. They publish various marketing promises on their websites to their customers – organizations of all sizes. This paper investigates how these promises align with customers’ needs, how they relate to human-centered security challenges highlighted in prior research, and what narrative is presented regarding the role of employees (as SAT recipients). We also investigate the level of transparency in vendor promises, as to whether it constitutes an information asymmetry. We gathered search terms from $n = 30$ awareness professionals to perform an automated Google search and scraping of SAT vendors’ websites. We then performed a thematic analysis of 2,476 statements on 156 websites from 59 vendors. We found that the messaging from SAT vendors precisely targets customers’ need for easy-to-implement and compliance-fulfilling SAT products; how SAT products are offered also means that some of the impacts of SAT go unmentioned and are transferred to the customer, such as user support. In this vendor-customer relationship, employees are portrayed as a source of weaknesses, needing an indefinite amount of training to be incorporated into the organization’s protection. We conclude with suggestions for SAT vendors and regulators, notably toward an SAT ecosystem that directly links SAT solutions to usable security

Keywords

Security Awareness, Security Market, Human-Centered Security

ACM Reference Format:

Jonas Hielscher, Markus Schöps, Jens Opdenbusch, Felix Reichmann, Marco Gutfleisch, Karola Marky, and Simon Parkin. 2024. Selling Satisfaction: A Qualitative Analysis of Cybersecurity Awareness Vendors’ Promises. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS ’24), October 14–18, 2024, Salt Lake City, UT, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3658644.3690196

1 Introduction

Organizations worldwide invest billions of dollars annually into cybersecurity awareness and training (SAT), and the market is growing [76]. SAT vendors deliver training platforms, campaign material, and simulated phishing attacks to their customers: organizations of all sizes. Numerous studies have investigated how employee-facing SAT products are experienced and how they could be improved (e.g., [12, 47, 49, 54, 61]). Complementing this, there have been studies of how security managers manage the security-related behaviors of the users they serve (e.g., [9, 57, 64]). These prior studies (further detailed in Section 2) have identified a range of misalignments regularly noted from practice over time. These misalignments include users perpetually regarded as needing to

* What do SAT vendors promise their customers?

* Which problems do they claim their products solve?

* What products and services do SAT vendors offer?

* What image of users (employees) do SAT vendors communicate?

Selling Satisfaction: A Qualitative Analysis of Cybersecurity Awareness Vendors' Promises

Jonas Hielscher*
Chair for Human-Centred Security
Ruhr University Bochum
Bochum, Germany

Markus Schöps
Chair for Human-Centred Security
Ruhr University Bochum
Bochum, Germany

Jens Opdenbusch
Chair for Human-Centred Security
Ruhr University Bochum
Bochum, Germany

Felix Reichmann
Developer Centered Security
Ruhr University Bochum
Bochum, Germany

Marco Gutfleisch
Chair for Human-Centred Security
Ruhr University Bochum
Bochum, Germany

Karola Marky
Digital Sovereignty Lab
Ruhr University Bochum
Bochum, Germany

Simon Parkin
TPM Cybersecurity Group
Delft University of Technology
Delft, Netherlands

Abstract

Security awareness and training (SAT) vendors operate in a growing multi-billion dollar market. They publish various marketing promises on their websites to their customers – organizations of all sizes. This paper investigates how these promises align with customers' needs, how they relate to human-centered security challenges highlighted in prior research, and what narrative is presented regarding the role of employees (as SAT recipients). We also investigate the level of transparency in vendor promises, as to whether it constitutes an information asymmetry. We gathered search terms from $n = 30$ awareness professionals to perform an automated Google search and scraping of SAT vendors' websites. We then performed a thematic analysis of 2,476 statements on 156 websites from 59 vendors. We found that the messaging from SAT vendors precisely targets customers' need for easy-to-implement and compliance-fulfilling SAT products; how SAT products are offered also means that some of the impacts of SAT go unmentioned and are transferred to the customer, such as user support. In this vendor-customer relationship, employees are portrayed as a source of weaknesses, needing an indefinite amount of training to be incorporated into the organization's protection. We conclude with suggestions for SAT vendors and regulators, notably toward an SAT ecosystem that directly links SAT solutions to usable security

Keywords

Security Awareness, Security Market, Human-Centered Security

ACM Reference Format:

Jonas Hielscher, Markus Schöps, Jens Opdenbusch, Felix Reichmann, Marco Gutfleisch, Karola Marky, and Simon Parkin. 2024. Selling Satisfaction: A Qualitative Analysis of Cybersecurity Awareness Vendors' Promises. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24), October 14–18, 2024, Salt Lake City, UT, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3658644.3690196

1 Introduction

Organizations worldwide invest billions of dollars annually into cybersecurity awareness and training (SAT), and the market is growing [76]. SAT vendors deliver training platforms, campaign material, and simulated phishing attacks to their customers: organizations of all sizes. Numerous studies have investigated how employee-facing SAT products are experienced and how they could be improved (e.g., [12, 47, 49, 54, 61]). Complementing this, there have been studies of how security managers manage the security-related behaviors of the users they serve (e.g., [9, 57, 64]). These prior studies (further detailed in Section 2) have identified a range of misalignments regularly noted from practice over time. These misalignments include users perpetually regarded as needing to

KnowBe4
309,583 followers
1d •

+ Follow ···

Personalized. Relevant. Adaptive.

This is how we do Human Risk Management. 💯 ...more

Easy learning for employees, 1 click for Security Managers

- Vendors clearly understand that security departments have tight budgets
- They also emphasize that employee involvement is needed but that involvement can be “fun” and “engaged”.

“Free up IT time to focus on big projects.”

“All our e-learning courses and challenge games provide interactivity and engagement to impart knowledge effectively.”

“[…] your training content must be fun, informative, and, above all else, consistently engaging.”

Hielscher, Jonas, et al. “Selling Satisfaction: A Qualitative Analysis of Cybersecurity Awareness Vendors’ Promises.” In Conference on Computer and Communications Security. 2024.

Stakeholders: management and compliance

- Vendors clearly understand that security departments have tight budgets
- They also emphasize that employee involvement is needed but that involvement can be “fun” and “engaged”.

“Track progress and run reports on completion for auditing purposes”

“Many compliance regulations such as HIPAA, PCI, SOX, GDPR, and CCPA, and even some insurance requirements, require cybersecurity training for all employees..”

Hielscher, Jonas, et al. “Selling Satisfaction: A Qualitative Analysis of Cybersecurity Awareness Vendors’ Promises.” In Conference on Computer and Communications Security. 2024.

Success: poorly expressed

- 11/59 vendors talked about success of their product
- Most in general terms or via case studies

- "Fortunately, the data showed that this 33.2% can be brought down to just 18.5% within 90 days of deploying new-school security awareness training. The one-year results show that by following these best practices, the final [Phishing] Percentage can be minimized to 5.4% on average."

Human time

7.1.1 Time for Training. 30 vendors explained in 63 statements how much time employees should spend on training and how long the completion of their training modules would take. The differences were enormous: 2-3min (4 vendors), 5min (1), 8min (1), 10min (3), 15min (3), 30min (3), 45-90min (5). Employees should be trained daily (1 vendor), weekly (4), every few weeks (3), monthly (6), every few months (3), annually (1), or "regulary" (9). The smallest amount a vendor suggested was *"less than 20 minutes of employee training per year"* — [V10]. The largest was the employees' engagement every day. Following micro-learning principles, most vendors stated that training should be delivered regularly but in small doses. While

Employees: Vulnerability or Shield?

- Shield - 9 Vendors
- Vulnerability – 15 Vendors

- “Human Firewall”
- “First line of defense”

- “Employees are the weakest link”
- “Easy prey”
- “Attackers go for the low-hanging fruit: humans”
- “All it takes is one click”

NEAT and SPRUCE

- Developed at Microsoft Research
- Guidance on how to create effective security messaging for end users

NEAT

Necessary – Can you change the architecture to eliminate or defer this user decision?

Explained - Does your user experience present all the information the user needs to make this decision? (See SPRUCE)

Actionable – Have you determined a set of steps the user will realistically be able to take to make the decision correctly?

Tested – Have you checked that your user experience is NEAT for all scenarios, both benign and malicious? Have you tested it on a human who is not a member of your team?

Encryption properties we want:

Cryptography magic sorts this one out for us: Confidentiality, Integrity.

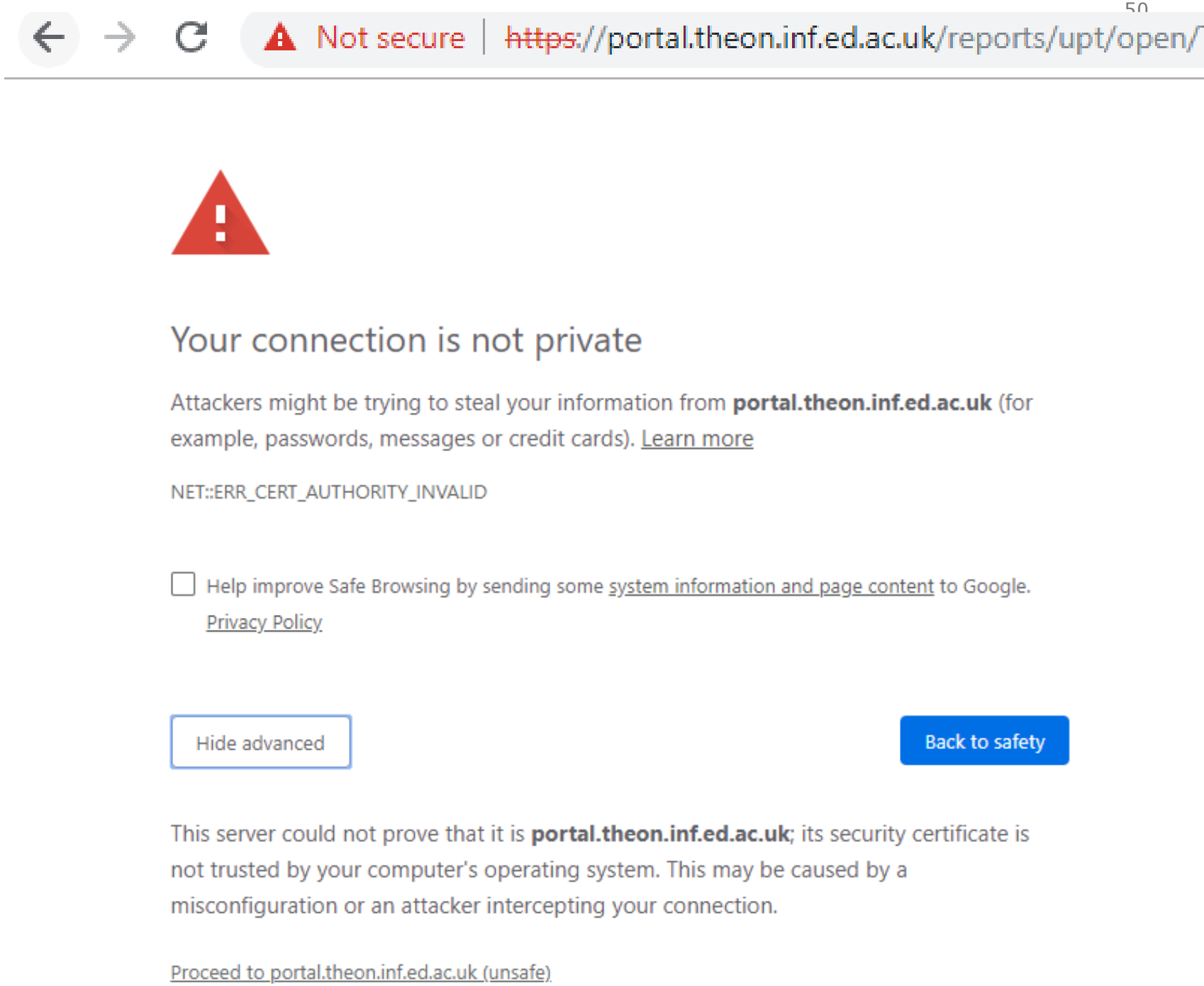
1. The communication between you and the other party is **confidential** and has **not been changed**
   - No one can read what you sent
   - No one can change what you sent

This one is a bit harder. Cryptography can verify you are speaking to the same person, but not identity.

2. **Knowing who** you are communicating with
   - You are talking to who you think you are talking to and not someone else

This error is saying that property (1) is held and that there is an encrypted connection.

But property (2) is not held in that it cannot determine who the browser is talking to.



Necessary

Explained

Actionable

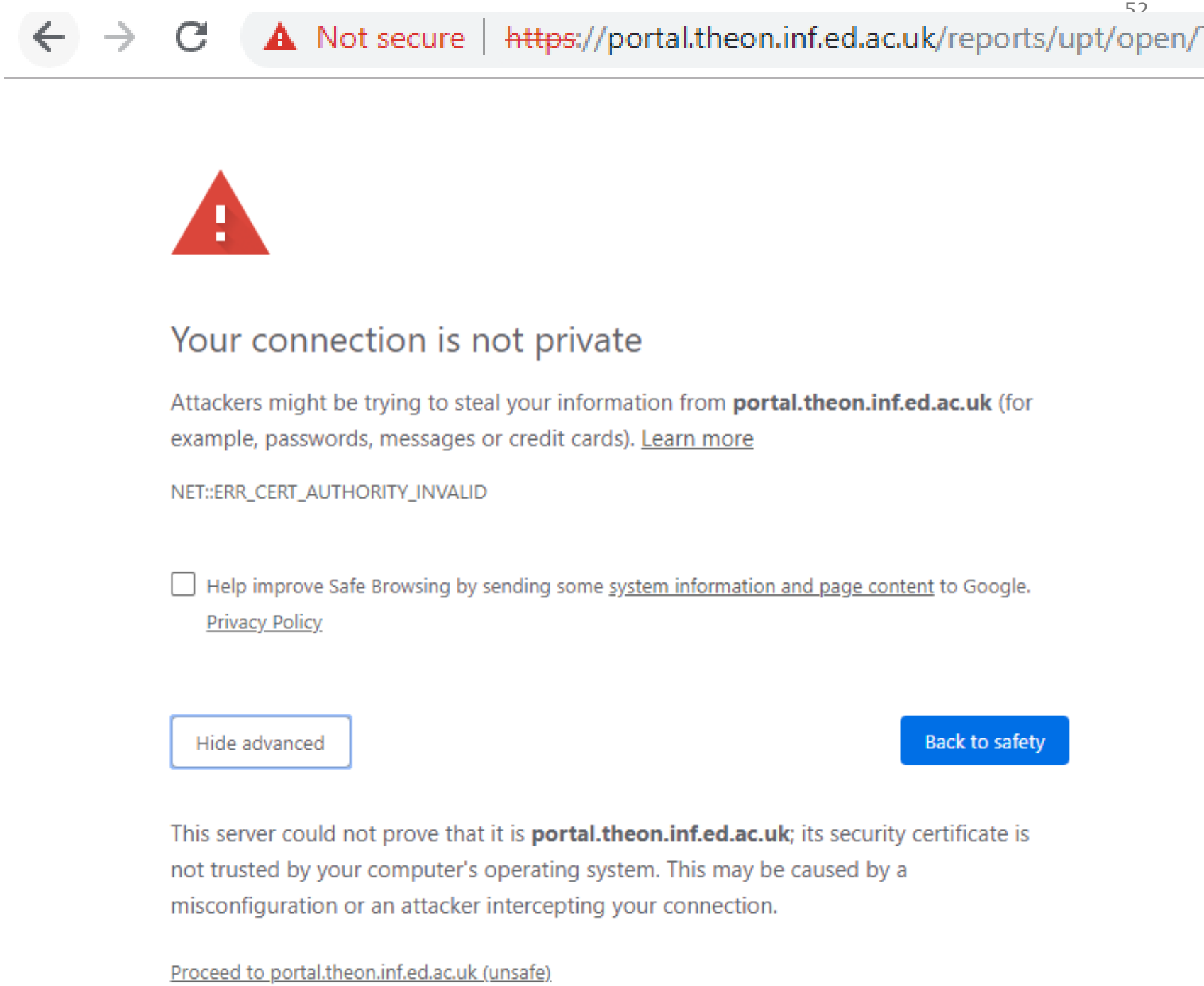
Tested

Necessary

Explained

Actionable

Tested

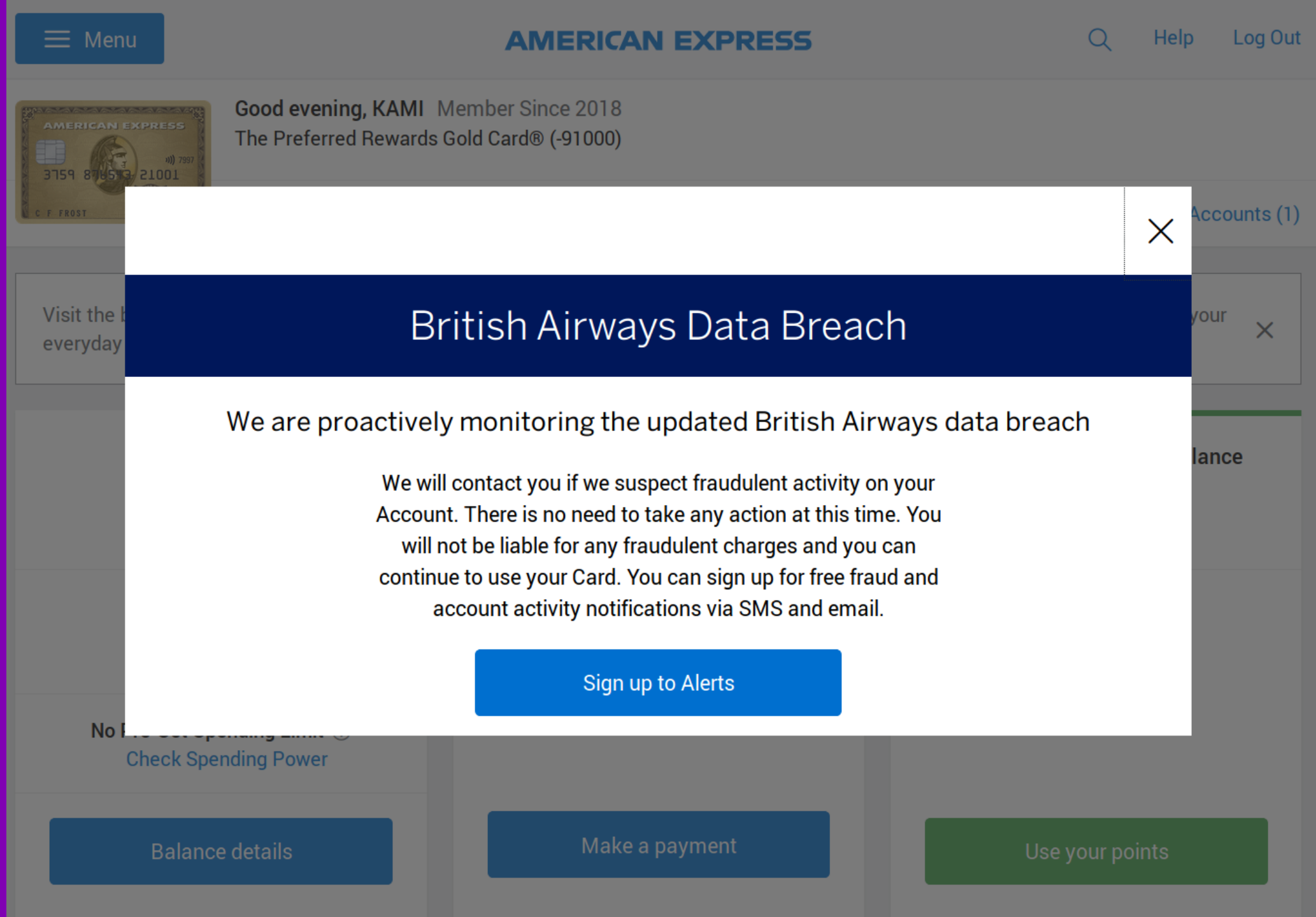


Necessary

Explained

Actionable

Tested



SPRUCE

Source – State who or what is asking the user to make a decision

Process – Give the user actionable steps to follow to make a good decision

Risk – Explain what bad thing could happen if they user makes the wrong decision

Unique – Knowledge the user has – Tell the user what information they bring to the decision

Choices – List available options and clearly recommend one

Evidence – Highlight information the user should factor in or exclude in making a decision

Source

Process

Risk

Unique

Choices

Evidence

Source

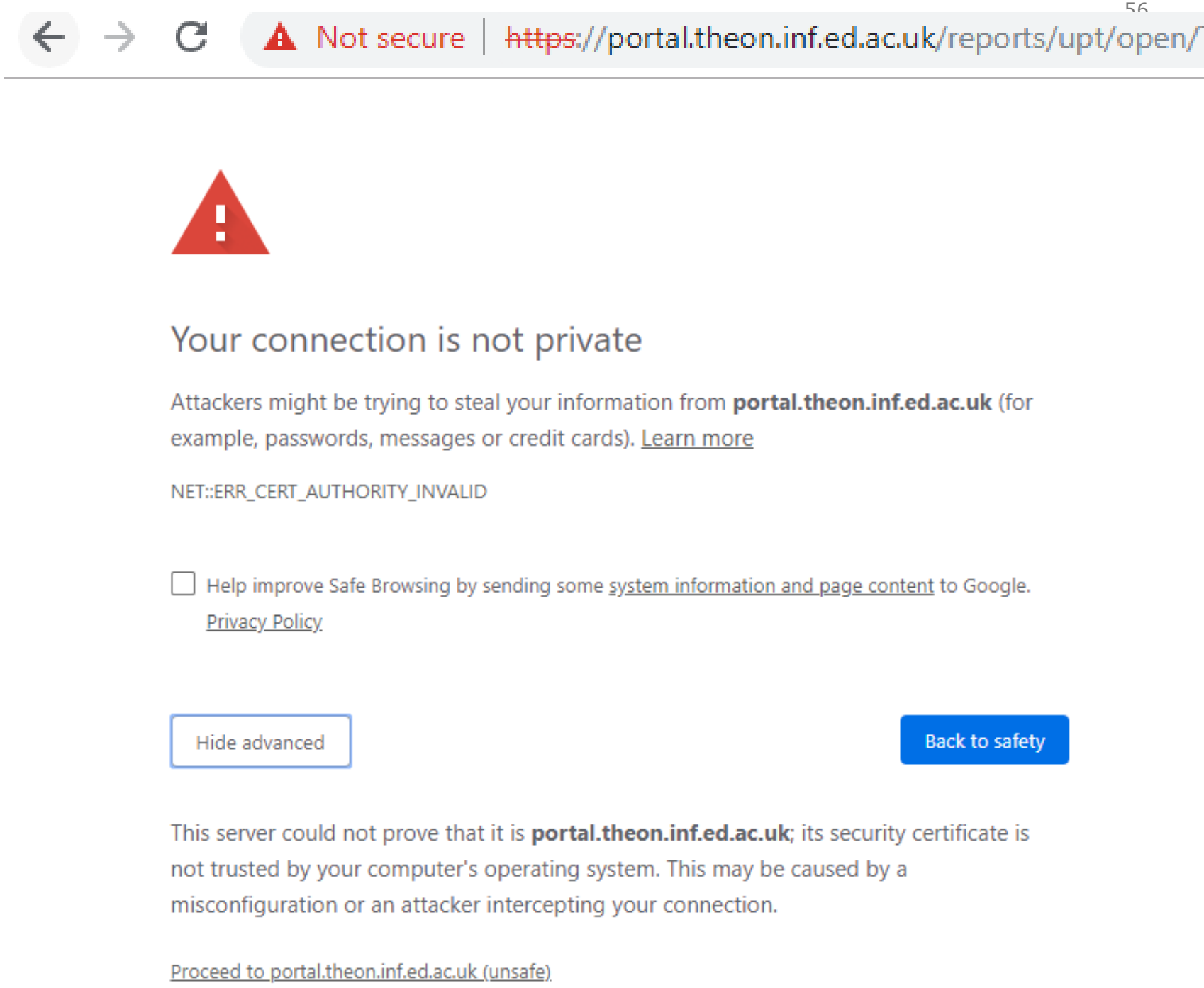
Process

Risk

Unique

Choices

Evidence



Source

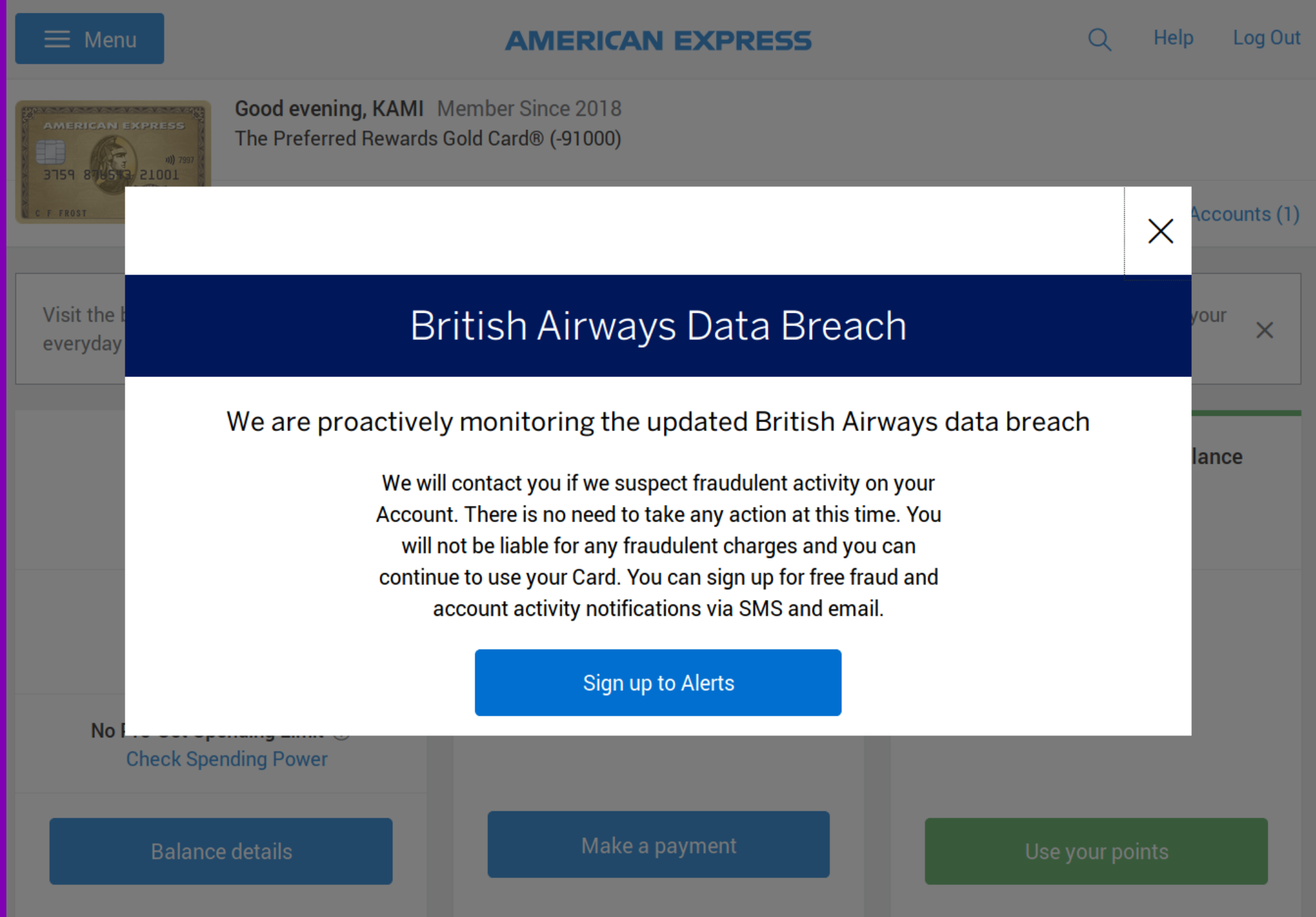
Process

Risk

Unique

Choices

Evidence



THE UNIVERSITY of EDINBURGH

Schools & departments

Search

EASE - The University's Authentication Service

Contact

Security Advice: Be careful of phishing messages directing people to fake login pages. Always hover over the URL and check it before you click it.

Security Advice: Be careful of phishing messages directing people to fake login pages. Always hover over the URL and check it before you click it.

Guidance

Do not share your password with anyone. We never ask you for your password in emails or via web forms other than this login page.

Do not share your password with anyone. We never ask you for your password in emails or via web forms other than this login page.

By using this service you agree to abide by The University of Edinburgh **Computing Regulations**.

Getting Help

- Forgotten username?
- Forgotten password?
- I need help

cation Scheme