Security and Privacy Advice

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

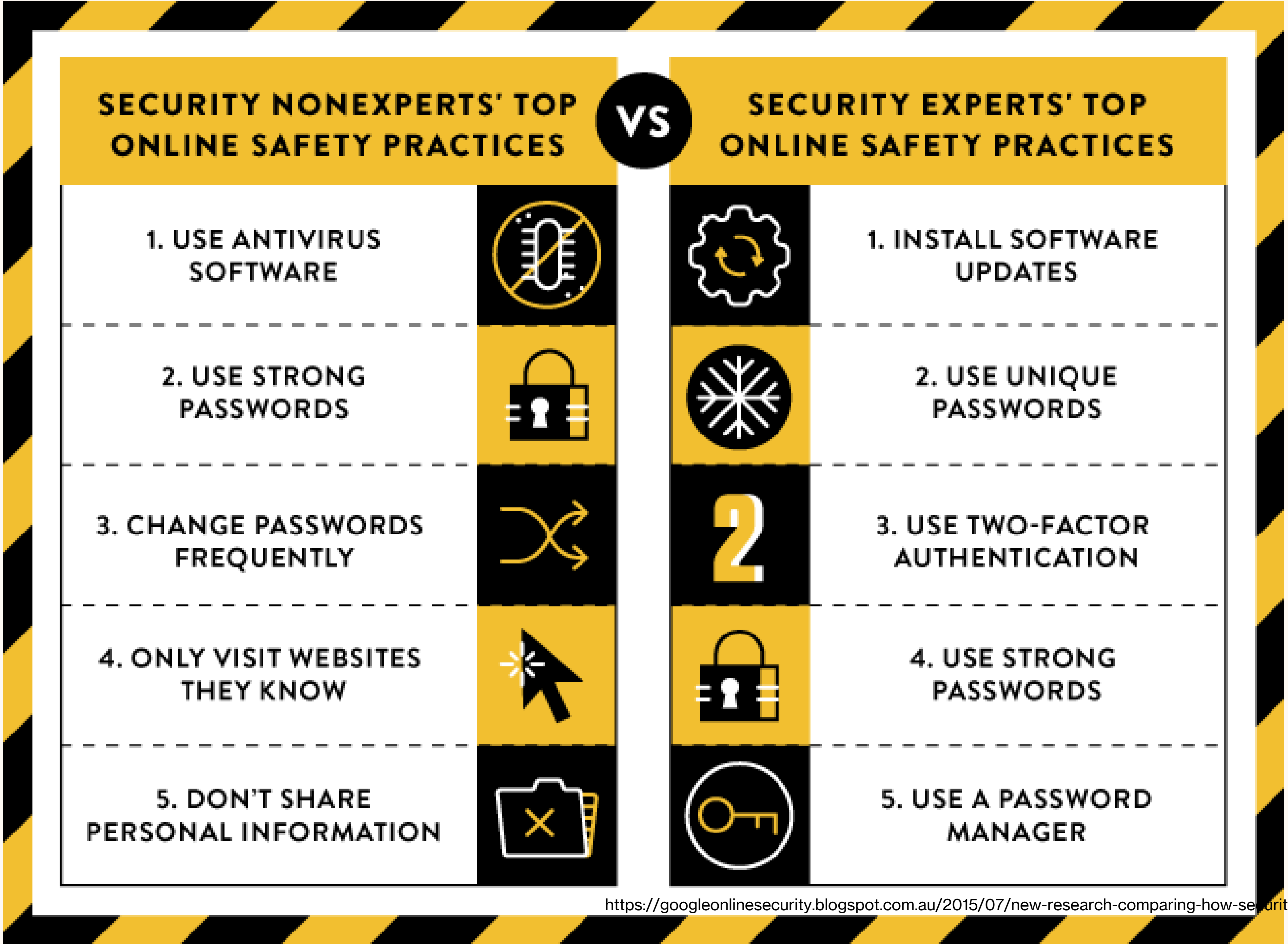
27/02/2024

THE UNIVERSITY *of* EDINBURGH

Overview

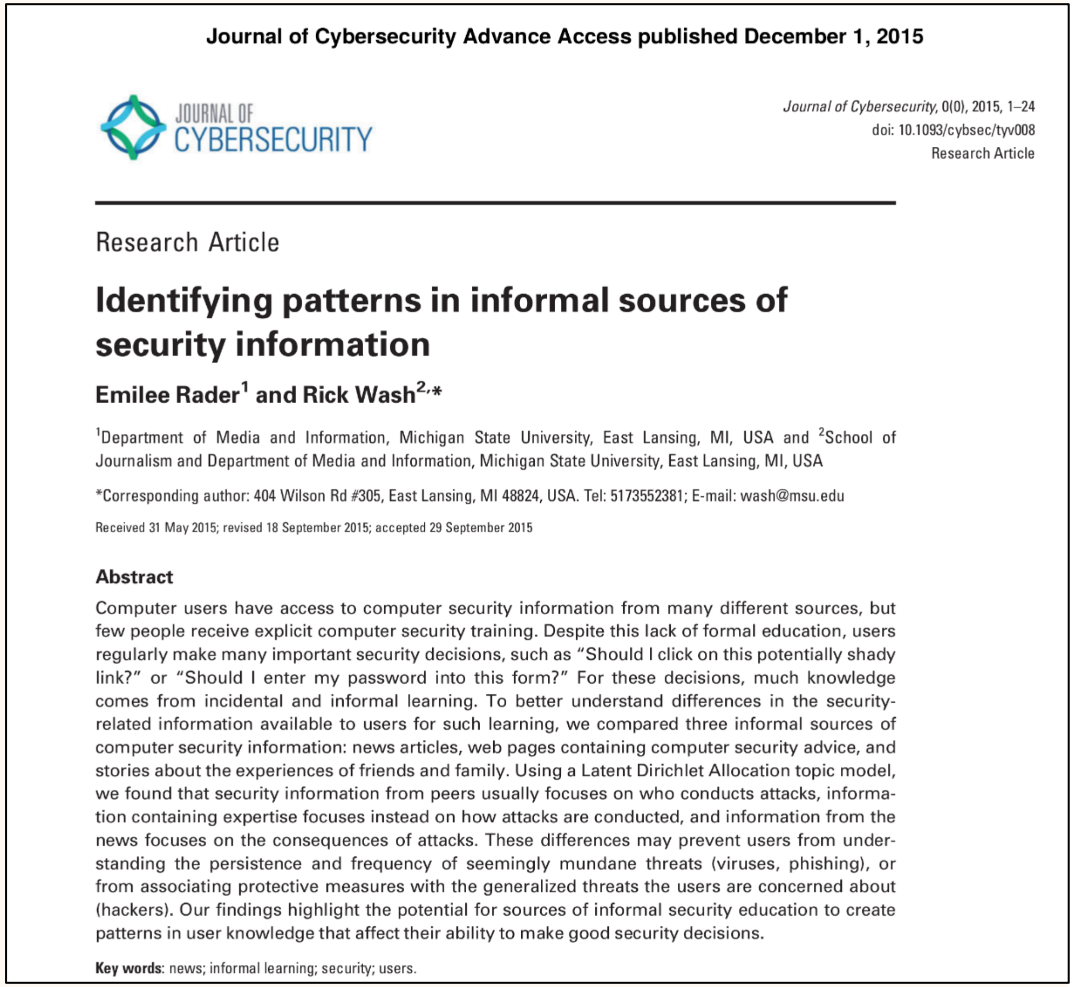
- Warm-up
- Security and privacy advice: why challenging?
- Framework: NEAT, etc.
- Take-home

https://www.youtube.com/watch?v=twTeOWLPRa4



SECURITY NONEXPERTS' TOP ONLINE SAFETY PRACTICES	VS	SECURITY EXPERTS' TOP ONLINE SAFETY PRACTICES
1. USE ANTIVIRUS SOFTWARE		1. INSTALL SOFTWARE UPDATES
2. USE STRONG PASSWORDS		2. USE UNIQUE PASSWORDS
3. CHANGE PASSWORDS FREQUENTLY		3. USE TWO-FACTOR AUTHENTICATION
4. ONLY VISIT WEBSITES THEY KNOW		4. USE STRONG PASSWORDS
5. DON'T SHARE PERSONAL INFORMATION		5. USE A PASSWORD MANAGER

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



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.

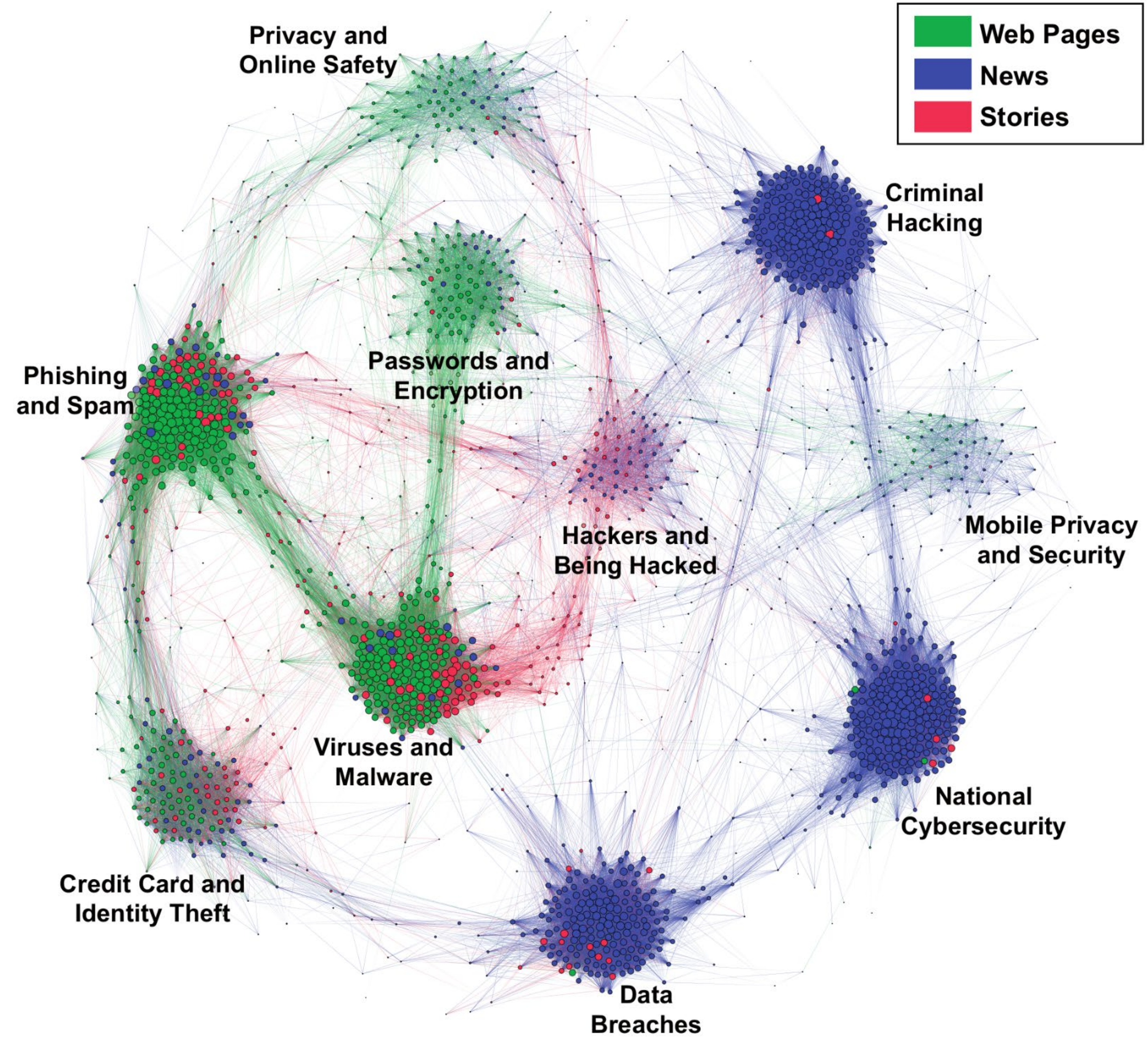
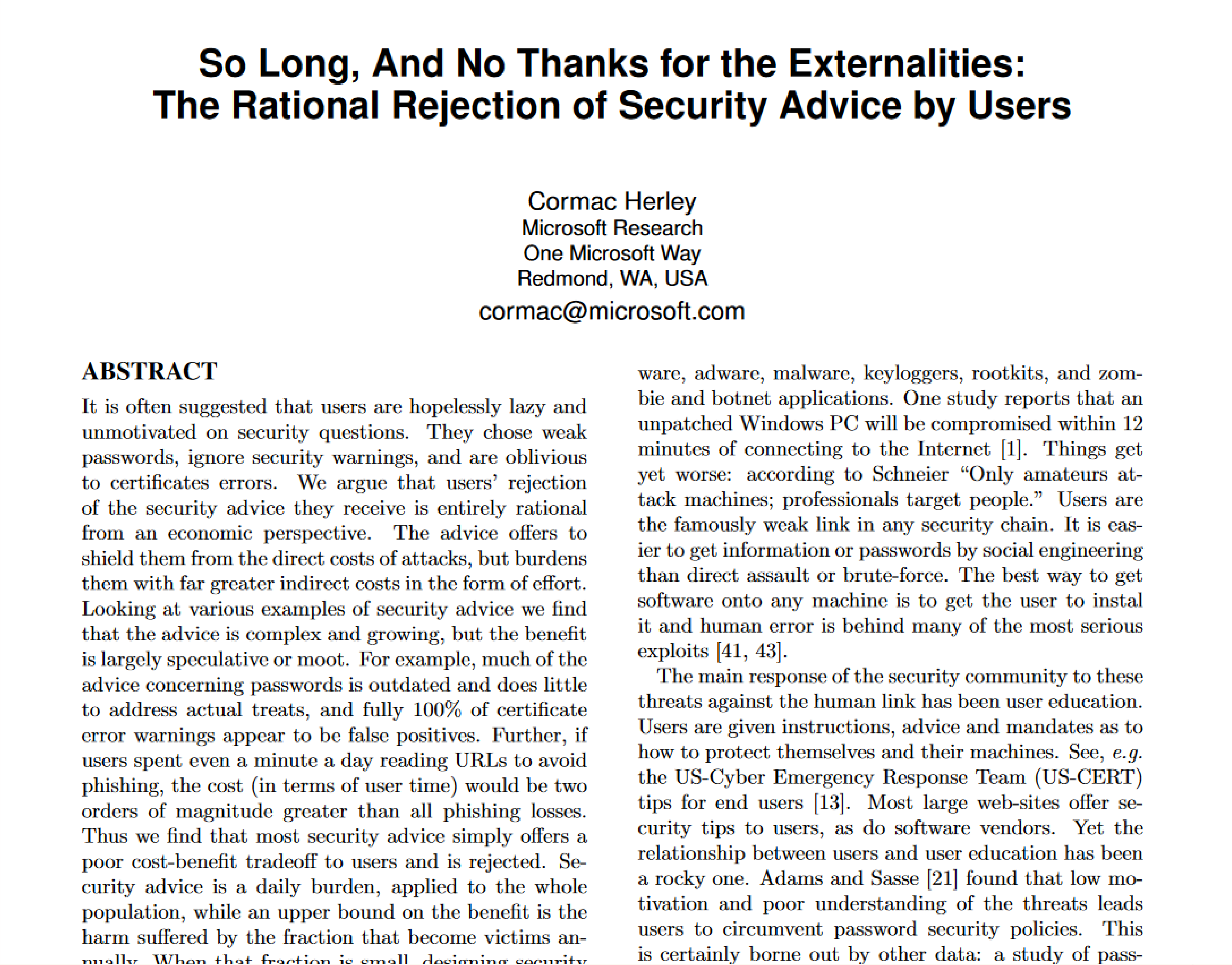


Figure 8. The document similarity graph, with clusters for each topic. There is one node for each document in the dataset. The red nodes are stories, green are web pages, and blue are news articles. Larger nodes are connected to more other documents. Edges represent the Pearson correlation between the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

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].

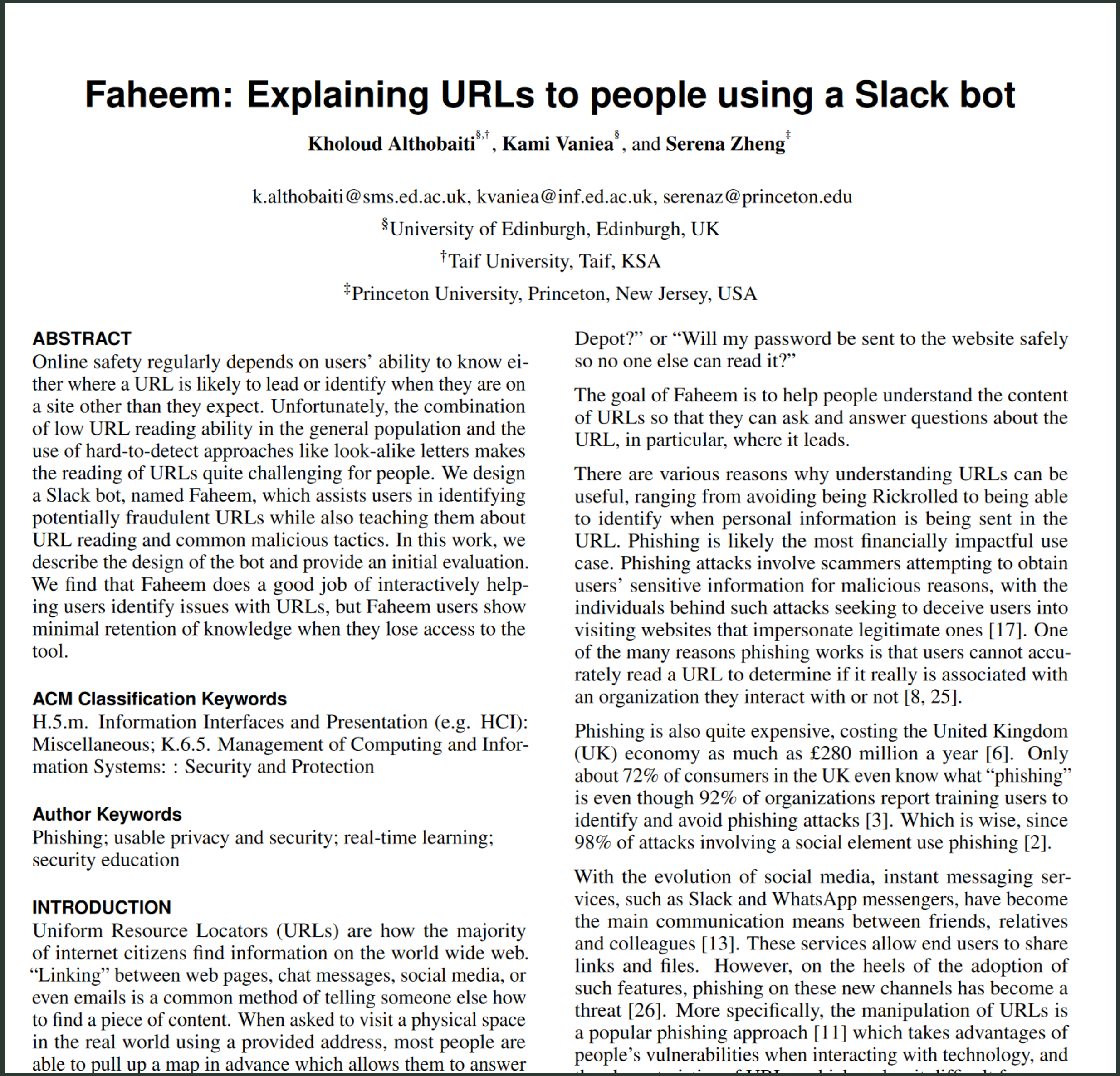
The main response of the security community to these threats against the human link has been user education. Users are given instructions, advice and mandates as to how to protect themselves and their machines. See, *e.g.* the US-Cyber Emergency Response Team (US-CERT) tips for end users [13]. Most large 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-

Externalities vs Internalities

Externality – The costs or benefits of an activity affect other groups or people.

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

Lets look at the example of URL reading given by Herley.



Faheem: Explaining URLs to people using a Slack bot

Kholoud Althobaiti[§,†], **Kami Vaniea**[§], and **Serena Zheng**[‡]

k.althobaiti@sms.ed.ac.uk, kvaniea@inf.ed.ac.uk, serenaz@princeton.edu

[§]University of Edinburgh, Edinburgh, UK

[†]Taif University, Taif, KSA

[‡]Princeton University, Princeton, New Jersey, USA

ABSTRACT

Online safety regularly depends on users' ability to know either where a URL is likely to lead or identify when they are on a site other than they expect. Unfortunately, the combination of low URL reading ability in the general population and the use of hard-to-detect approaches like look-alike letters makes the reading of URLs quite challenging for people. We design a Slack bot, named Faheem, which assists users in identifying potentially fraudulent URLs while also teaching them about URL reading and common malicious tactics. In this work, we describe the design of the bot and provide an initial evaluation. We find that Faheem does a good job of interactively helping users identify issues with URLs, but Faheem users show minimal retention of knowledge when they lose access to the tool.

ACM Classification Keywords

H.5.m. Information Interfaces and Presentation (e.g. HCI): Miscellaneous; K.6.5. Management of Computing and Information Systems: : Security and Protection

Author Keywords

Phishing; usable privacy and security; real-time learning; security education

INTRODUCTION

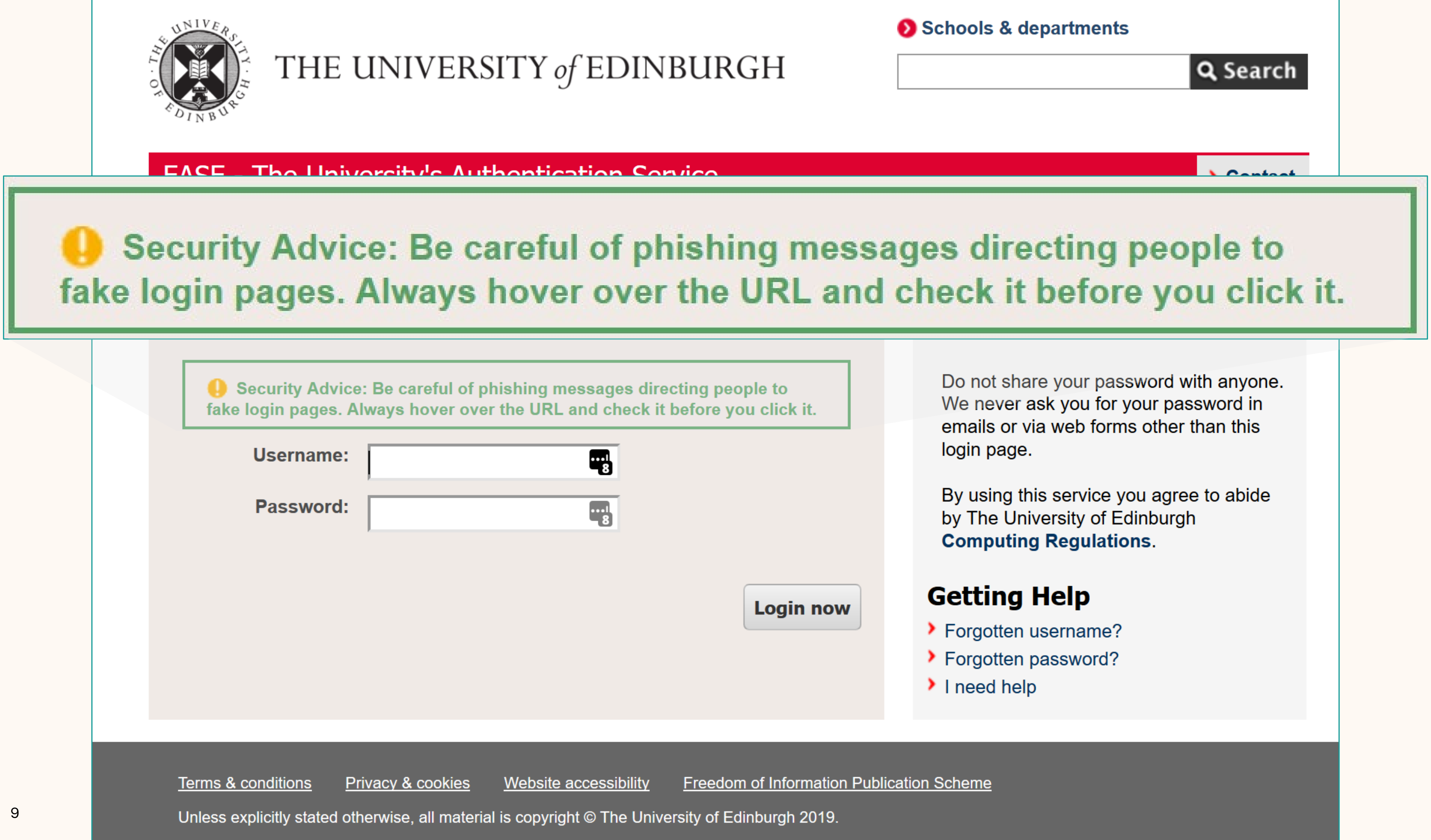
Uniform Resource Locators (URLs) are how the majority of internet citizens find information on the world wide web. "Linking" between web pages, chat messages, social media, or even emails is a common method of telling someone else how to find a piece of content. When asked to visit a physical space in the real world using a provided address, most people are able to pull up a map in advance which allows them to answer Depot?" or "Will my password be sent to the website safely so no one else can read it?"

The goal of Faheem is to help people understand the content of URLs so that they can ask and answer questions about the URL, in particular, where it leads.

There are various reasons why understanding URLs can be useful, ranging from avoiding being Rickrolled to being able to identify when personal information is being sent in the URL. Phishing is likely the most financially impactful use case. Phishing attacks involve scammers attempting to obtain users' sensitive information for malicious reasons, with the individuals behind such attacks seeking to deceive users into visiting websites that impersonate legitimate ones [17]. One of the many reasons phishing works is that users cannot accurately read a URL to determine if it really is associated with an organization they interact with or not [8, 25].

Phishing is also quite expensive, costing the United Kingdom (UK) economy as much as £280 million a year [6]. Only about 72% of consumers in the UK even know what "phishing" is even though 92% of organizations report training users to identify and avoid phishing attacks [3]. Which is wise, since 98% of attacks involving a social element use phishing [2].

With the evolution of social media, instant messaging services, such as Slack and WhatsApp messengers, have become the main communication means between friends, relatives and colleagues [13]. These services allow end users to share links and files. However, on the heels of the adoption of such features, phishing on these new channels has become a threat [26]. More specifically, the manipulation of URLs is a popular phishing approach [11] which takes advantages of people's vulnerabilities when interacting with technology, and


Schools & departments
Search
THE UNIVERSITY of EDINBURGH
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.

Username:

Password:

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

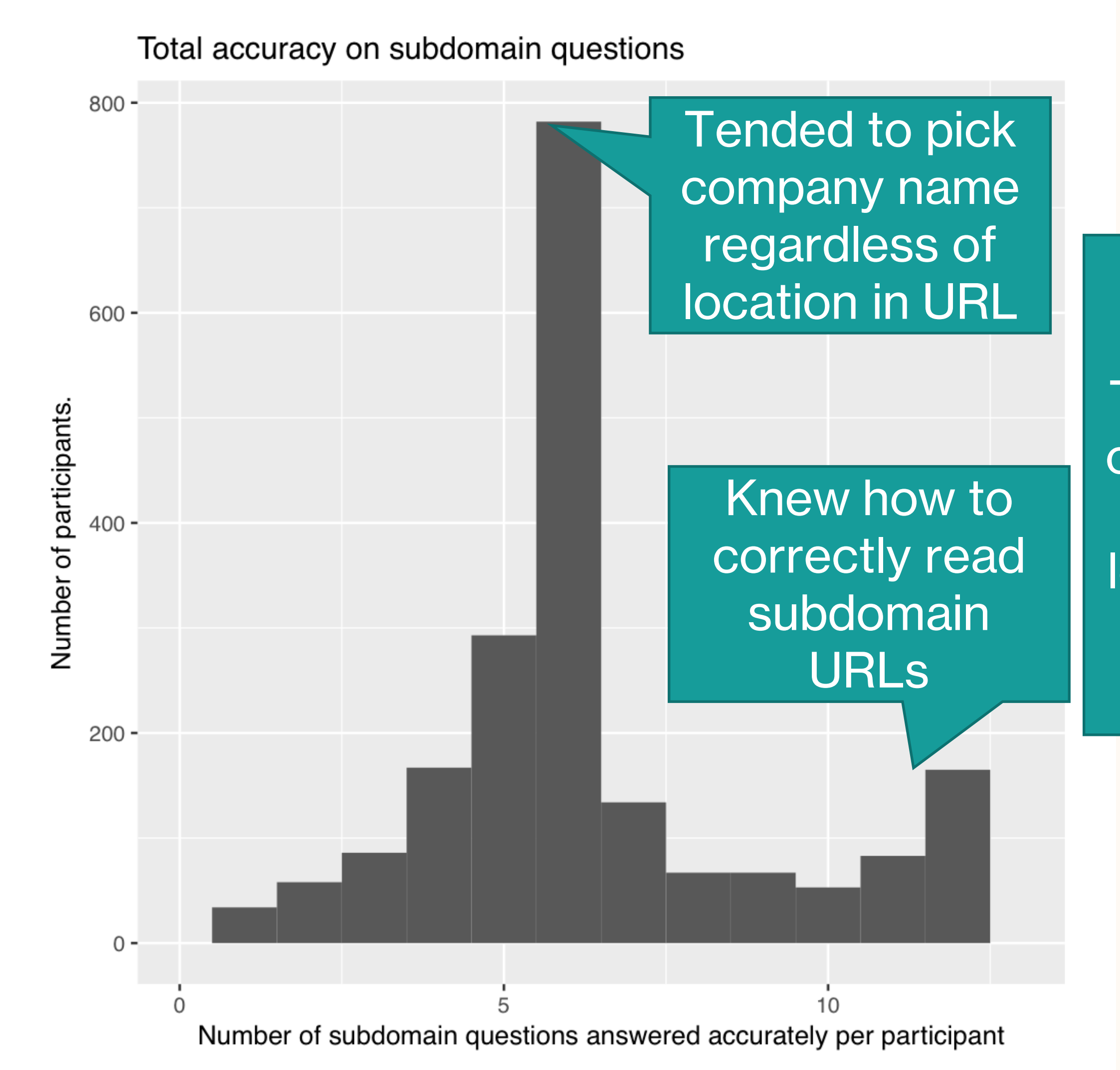
- Forgotten username?
- Forgotten password?
- I need help

Which of these URLs goes to Facebook?

✗ https://facebook.profile.com

https://profile.facebook.com

✓

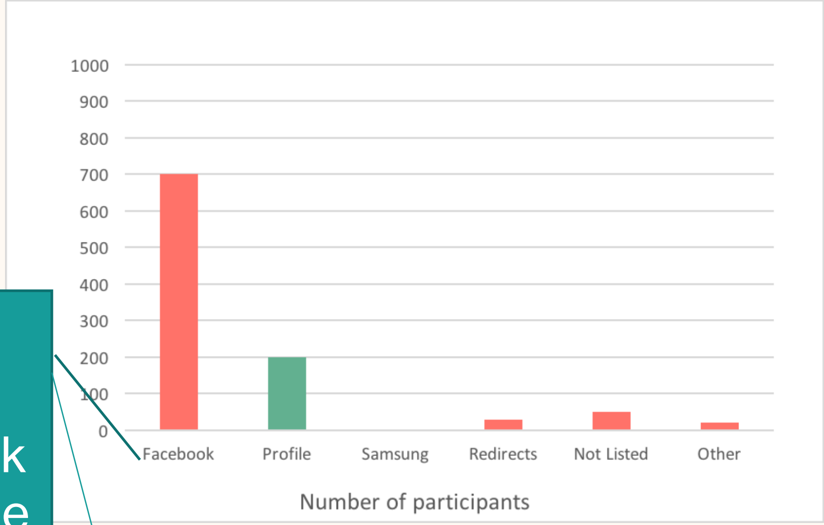


Tended to pick company name regardless of location in URL

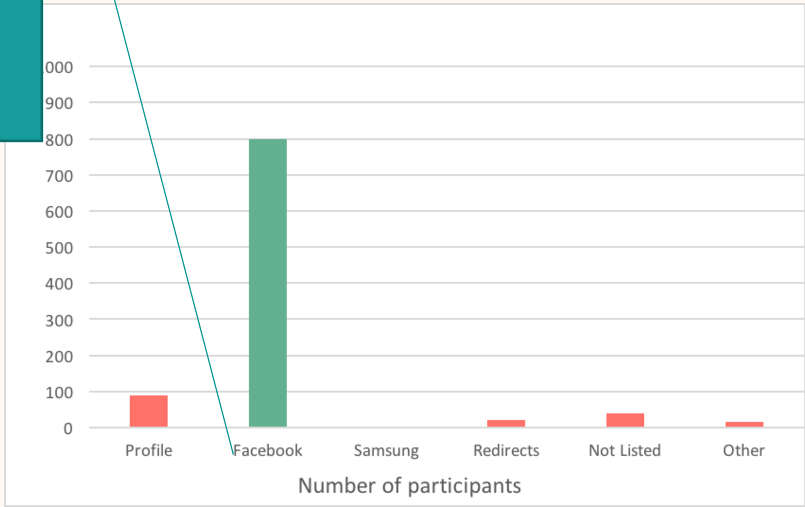
Knew how to correctly read subdomain URLs

Tended to pick company name regardless of location in URL

https://facebook.profile.com

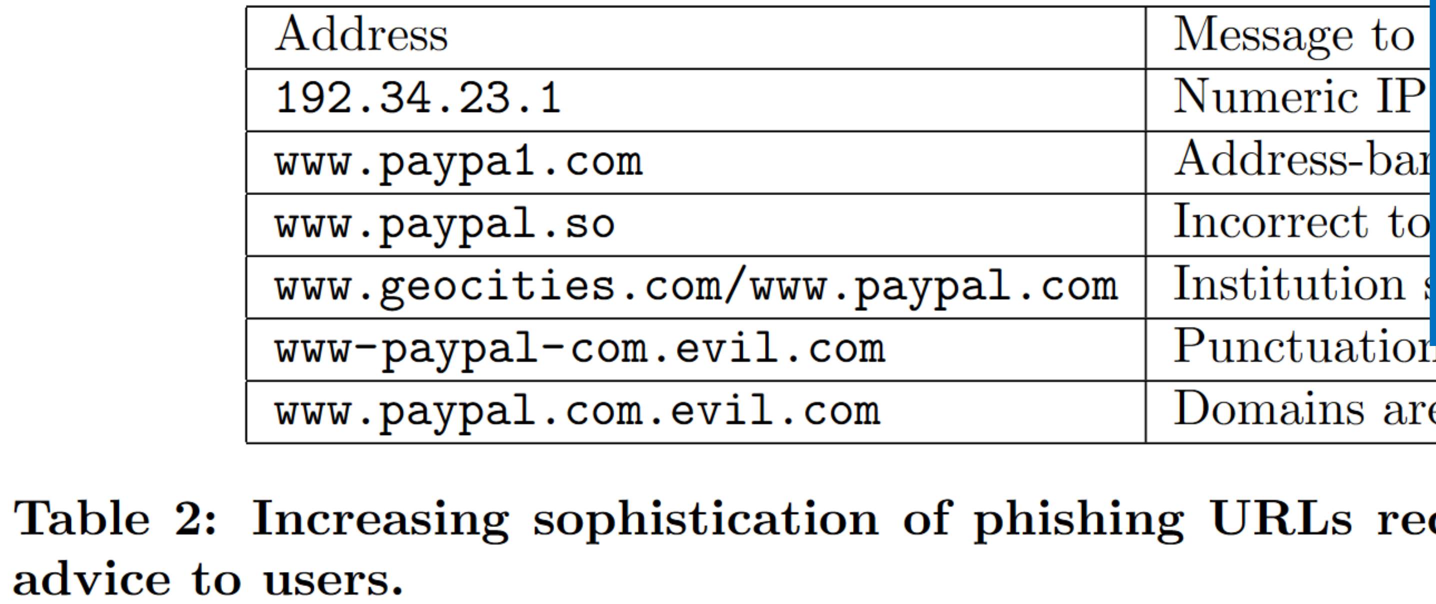


https://profile.facebook.com



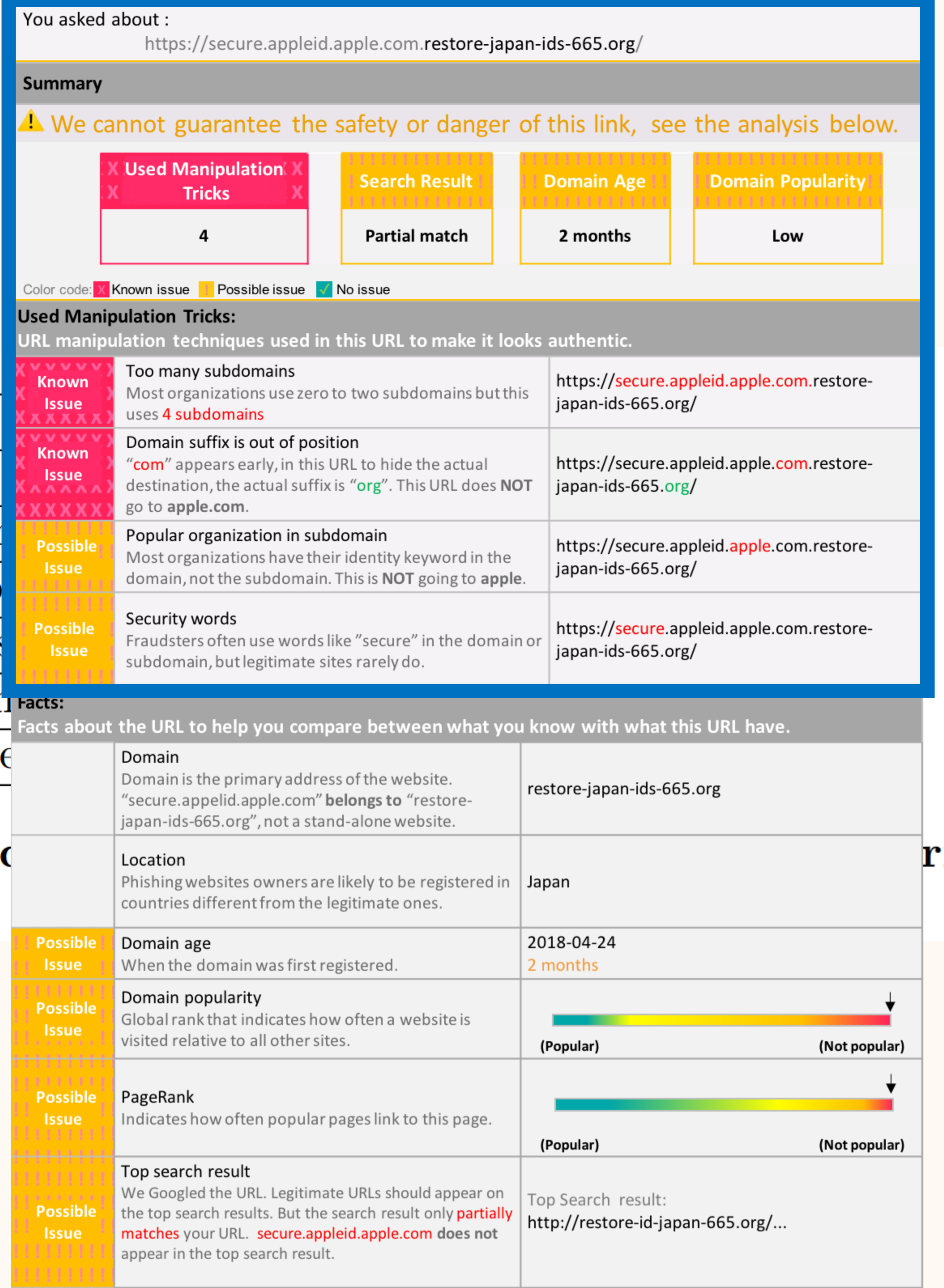
February 26, 2024

URLs can get very complicated



Address	Message to
192.34.23.1	Numeric IP
www.paypa1.com	Address-bar
www.paypal.so	Incorrect to
www.geocities.com/www.paypal.com	Institution s
www-paypal-com.evil.com	Punctuation
www.paypal.com.evil.com	Domains are

Table 2: Increasing sophistication of phishing URLs rec rity advice to users.



You asked about :

https://secure.appleid.apple.com.restore-japan-ids-665.org/

Summary

⚠ We cannot guarantee the safety or danger of this link, see the analysis below.

Used Manipulation Tricks	Search Result	Domain Age	Domain Popularity
4	Partial match	2 months	Low

Color code: 🟥 Known issue 🟨 Possible issue ✓ No issue

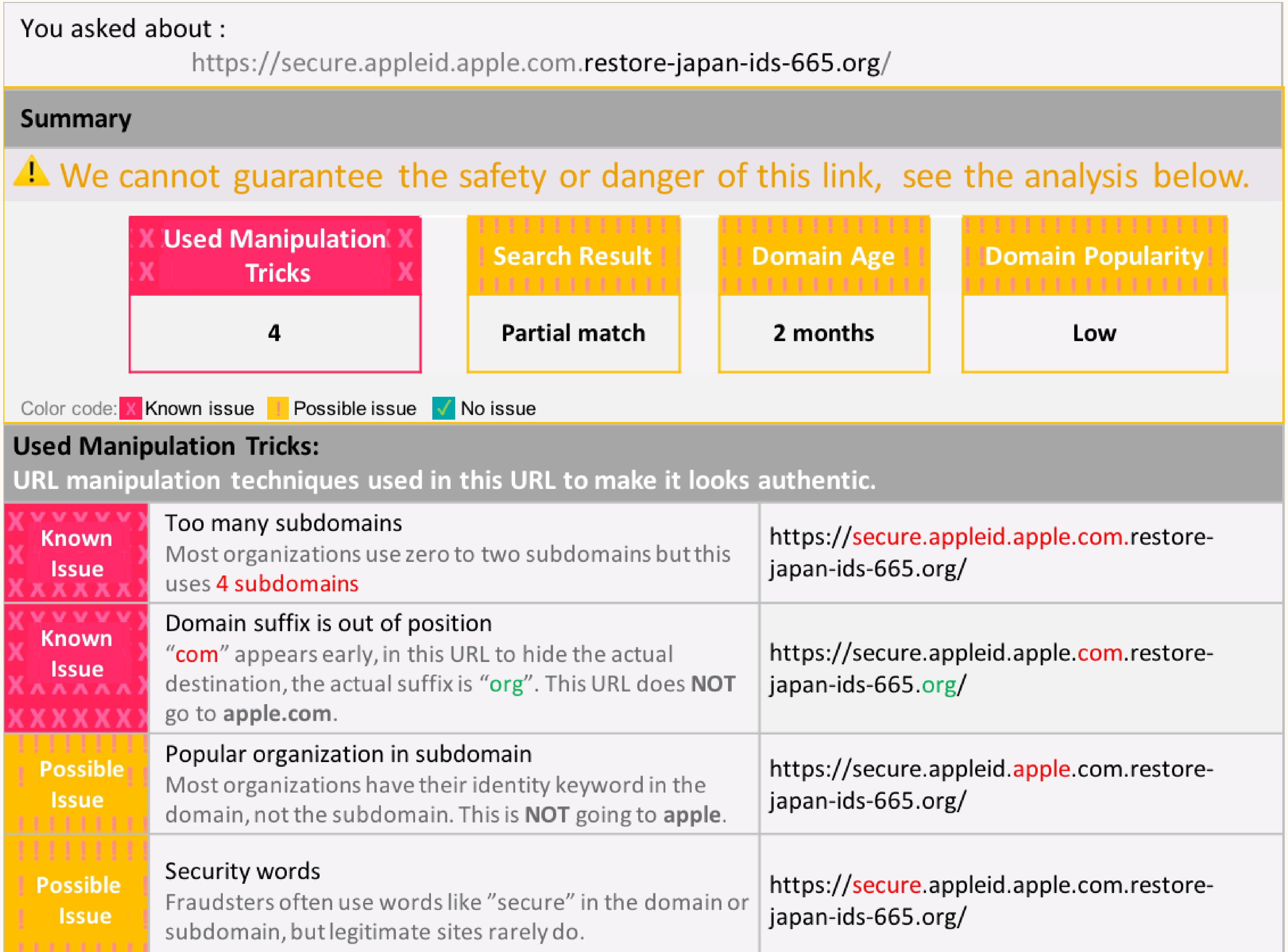
Used Manipulation Tricks:
URL manipulation techniques used in this URL to make it looks authentic.

Known Issue	Too many subdomains Most organizations use zero to two subdomains but this uses 4 subdomains	https://secure.appleid.apple.com.restore-japan-ids-665.org/
Known Issue	Domain suffix is out of position "com" appears early, in this URL to hide the actual destination, the actual suffix is "org". This URL does **NOT** go to **apple.com**.	https://secure.appleid.apple.com.restore-japan-ids-665.org/
Possible Issue	Popular organization in subdomain Most organizations have their identity keyword in the domain, not the subdomain. This is **NOT** going to **apple**.	https://secure.appleid.apple.com.restore-japan-ids-665.org/
Possible Issue	Security words Fraudsters often use words like "secure" in the domain or subdomain, but legitimate sites rarely do.	https://secure.appleid.apple.com.restore-japan-ids-665.org/

Facts:
Facts about the URL to help you compare between what you know with what this URL have.

	Domain Domain is the primary address of the website. "secure.appelid.apple.com" **belongs to** "restore-japan-ids-665.org", not a stand-alone website.	restore-japan-ids-665.org
	Location Phishing websites owners are likely to be registered in countries different from the legitimate ones.	Japan
Possible Issue	Domain age When the domain was first registered.	2018-04-24 2 months
Possible Issue	Domain popularity Global rank that indicates how often a website is visited relative to all other sites.	**(Popular)** **(Not popular)**
Possible Issue	PageRank Indicates how often popular pages link to this page.	**(Popular)** **(Not popular)**
Possible Issue	Top search result We Googled the URL. Legitimate URLs should appear on the top search results. But the search result only partially matches your URL. secure.appleid.apple.com **does not** appear in the top search result.	Top Search result: http://restore-id-japan-665.org/...

rity



You asked about :

https://secure.appleid.apple.com.restore-japan-ids-665.org/

Summary

⚠ We cannot guarantee the safety or danger of this link, see the analysis below.

Used Manipulation Tricks	Search Result	Domain Age	Domain Popularity
4	Partial match	2 months	Low

Color code: ☒ Known issue ! Possible issue ✓ No issue

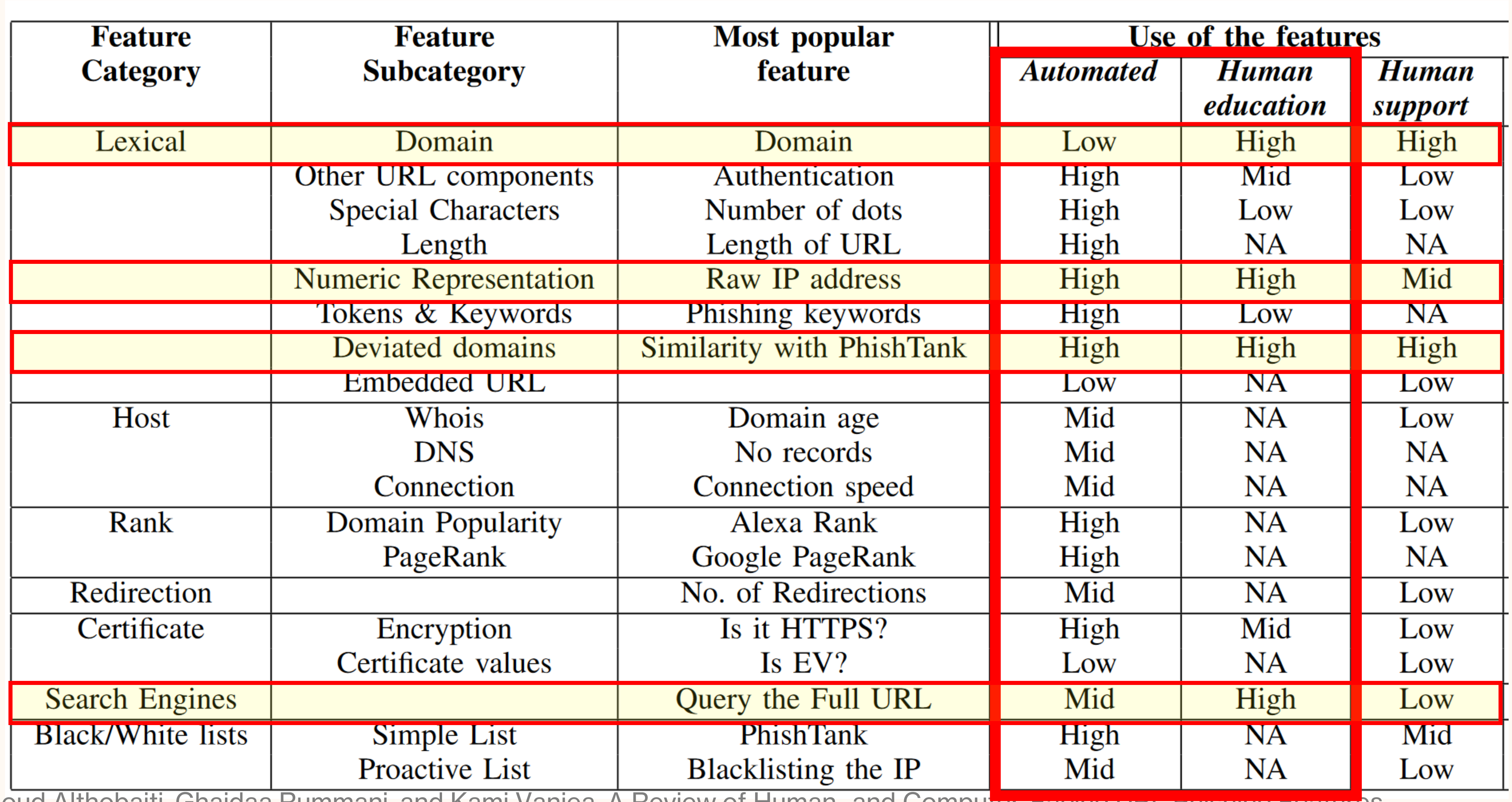
Used Manipulation Tricks:
URL manipulation techniques used in this URL to make it looks authentic.

Known Issue	Too many subdomains Most organizations use zero to two subdomains but this uses 4 subdomains	https://secure.appleid.apple.com.restore-japan-ids-665.org/
Known Issue	Domain suffix is out of position “com” appears early, in this URL to hide the actual destination, the actual suffix is “org”. This URL does **NOT** go to **apple.com**.	https://secure.appleid.apple.com.restore-japan-ids-665.org/
Possible Issue	Popular organization in subdomain Most organizations have their identity keyword in the domain, not the subdomain. This is **NOT** going to **apple**.	https://secure.appleid.apple.com.restore-japan-ids-665.org/
Possible Issue	Security words Fraudsters often use words like ”secure” in the domain or subdomain, but legitimate sites rarely do.	https://secure.appleid.apple.com.restore-japan-ids-665.org/

Herley says...

- Costs
  - Re-training users constantly as the attackers improve
  - Training organizations to behave in a consistent way so the advice is true and makes sense
- Benefits (potential)
  - Falling for (less) phishing attacks
- Benefits (actual)
  - Most large organizations absorb financial loss from phishing so the loss is an externality

Features for phishing URL detection

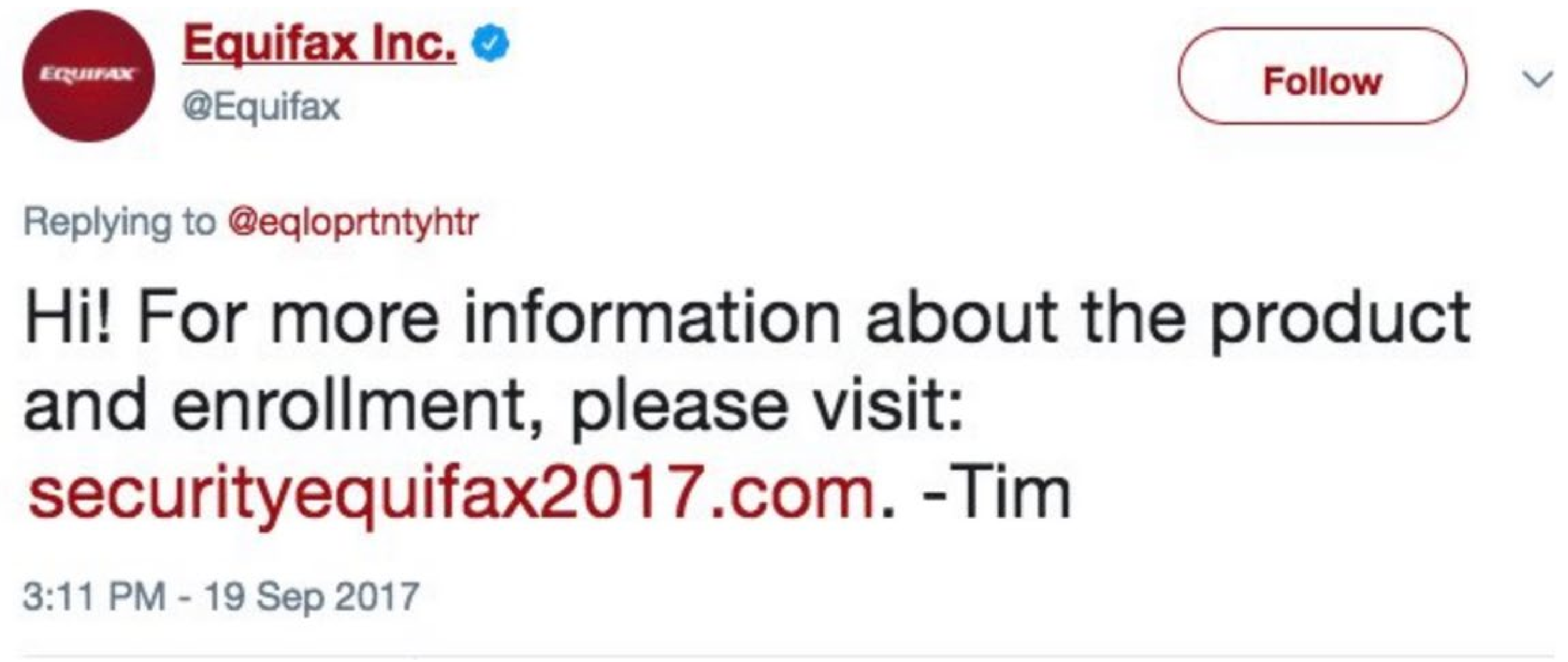


Feature Category	Feature Subcategory	Most popular feature	Use of the features		
			Automated	*Human education*	*Human support*
Lexical	Domain	Domain	Low	High	High
	Other URL components	Authentication	High	Mid	Low
	Special Characters	Number of dots	High	Low	Low
	Length	Length of URL	High	NA	NA
	Numeric Representation	Raw IP address	High	High	Mid
	Tokens & Keywords	Phishing keywords	High	Low	NA
	Deviated domains	Similarity with PhishTank	High	High	High
	Embedded URL		Low	NA	Low
Host	Whois	Domain age	Mid	NA	Low
	DNS	No records	Mid	NA	NA
	Connection	Connection speed	Mid	NA	NA
Rank	Domain Popularity	Alexa Rank	High	NA	Low
	PageRank	Google PageRank	High	NA	NA
Redirection		No. of Redirections	Mid	NA	Low
Certificate	Encryption	Is it HTTPS?	High	Mid	Low
	Certificate values	Is EV?	Low	NA	Low
Search Engines		Query the Full URL	Mid	High	Low
Black/White lists	Simple List	PhishTank	High	NA	Mid
	Proactive List	Blacklisting the IP	Mid	NA	Low

Kholoud Althobaiti, Ghaidaa Rummani, and Kami Vaniea. A Review of Human- and Computer-Facing URL Phishing Features. In the European Workshop on Usable Security (EuroUSEC), June 2019.

EQUIPHISH

On Tuesday, the official Equifax account on Twitter replied to a tweet requesting the Web address of the site that the company set up to give away its free one-year of credit monitoring service. That site is https://www.equifaxsecurity2017.com, but the company's Twitter account told users to instead visit securityequifax2017[dot]com, which is currently blocked by multiple browsers as a phishing site.



Equifax Inc.
@Equifax

Follow

Replying to @eqloprtntyhtr

Hi! For more information about the product and enrollment, please visit: securityequifax2017.com. -Tim

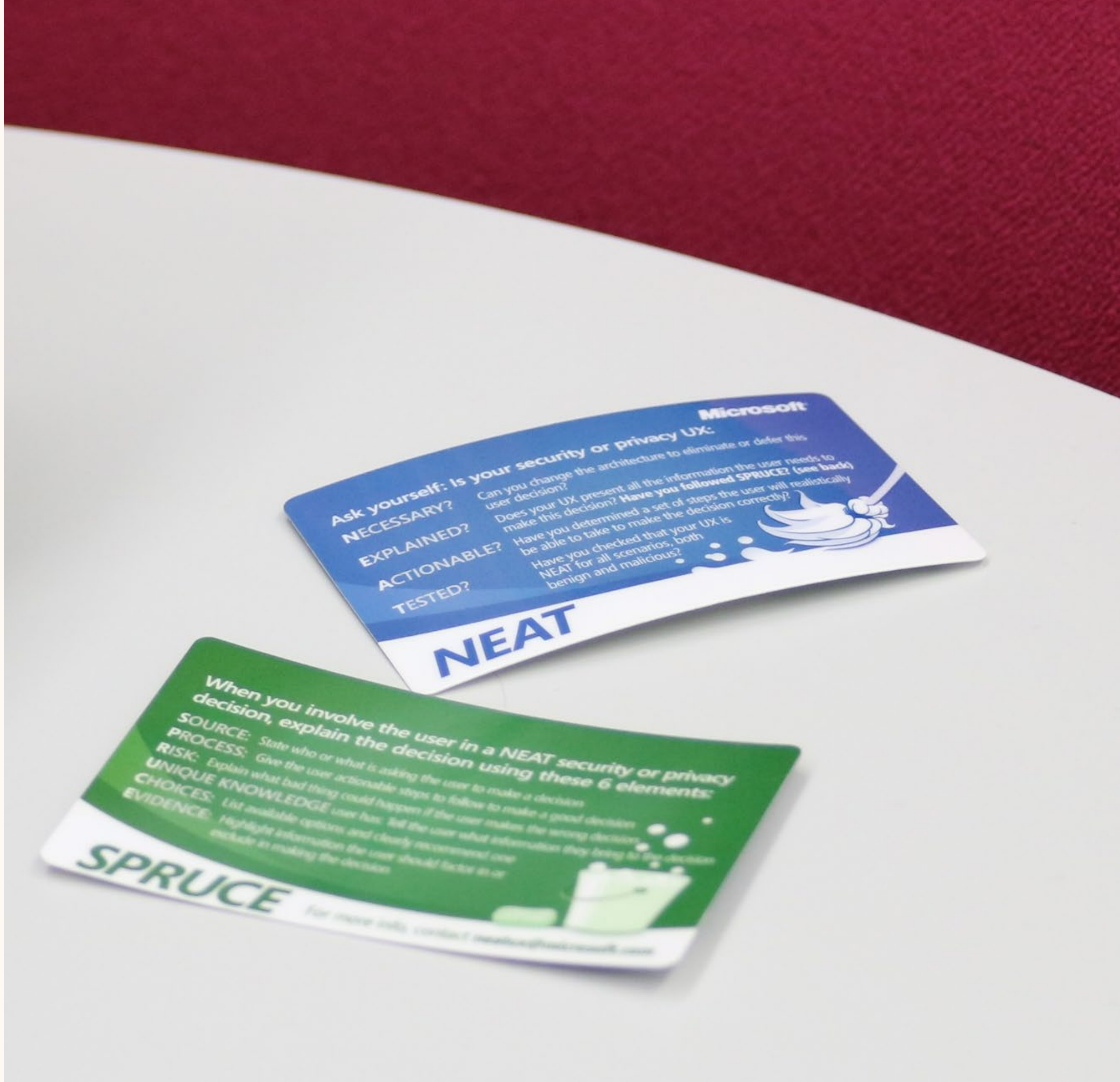
3:11 PM - 19 Sep 2017

Think-pair-share

- Select one piece of advice from the handout
- What are the costs, potential benefits, and actual benefits of following that advice?

NEAT and SPRUCE

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



Microsoft

Ask yourself: Is your security or privacy UX:

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

EXPLAINED? Does your UX present all the information the user needs to make this decision? **Have you followed SPRUCE? (see back)**

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 UX is NEAT for all scenarios, both benign and malicious?

NEAT

When you involve the user in a NEAT security or privacy decision, explain the decision using these 6 elements:

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 the user makes the wrong decision*

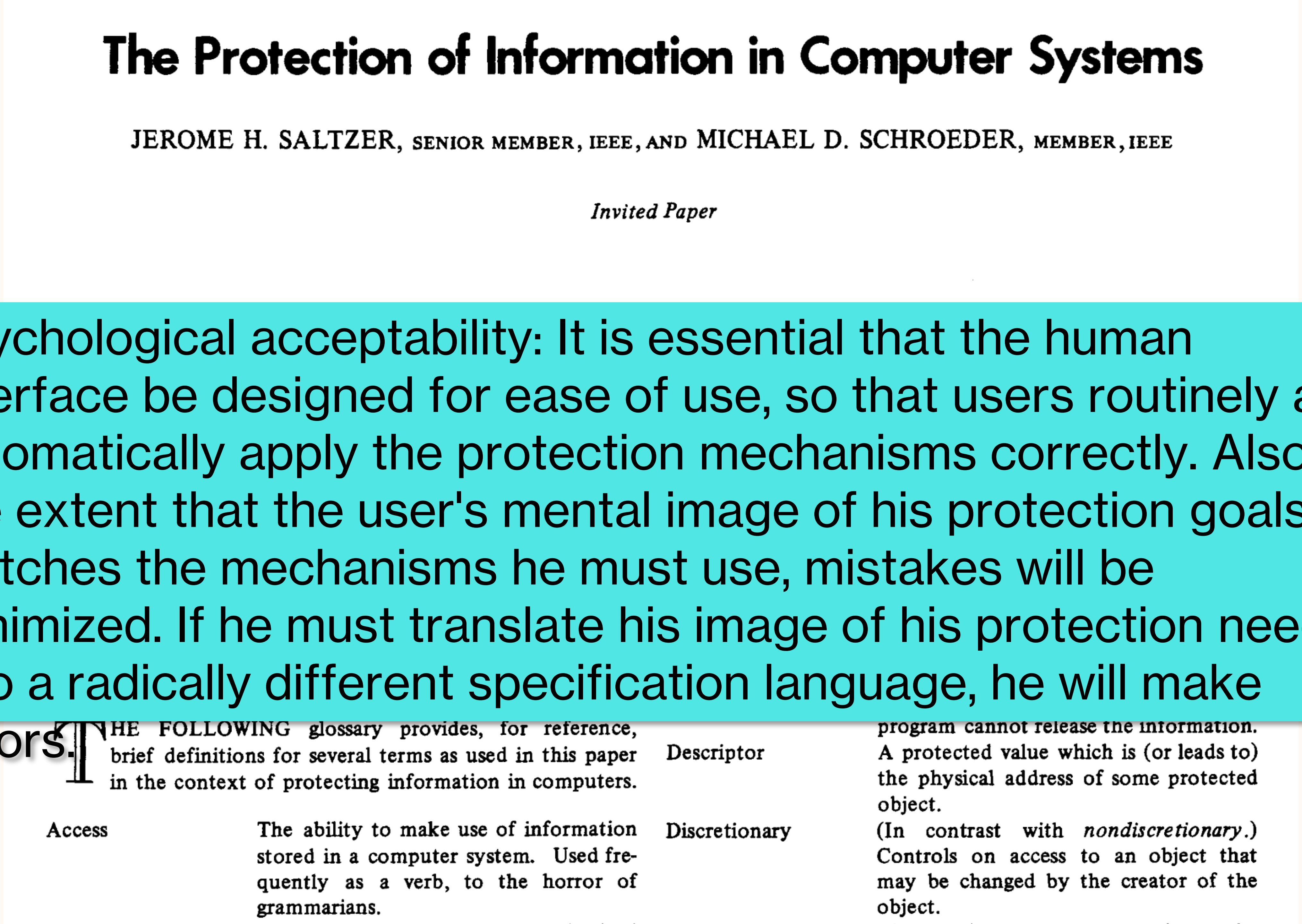
UNIQUE KNOWLEDGE *user has: Tell the user what information they bring to the decision*

CHOICES: *List available options and clearly recommend one*

EVIDENCE: *Highlight information the user should factor in or exclude in making the decision*

SPRUCE

For more info, contact [illegible]



The Protection of Information in Computer Systems

JEROME H. SALTZER, SENIOR MEMBER, IEEE, AND MICHAEL D. SCHROEDER, MEMBER, IEEE

Invited Paper

Psychological acceptability: It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized. If he must translate his image of his protection needs into a radically different specification language, he will make errors.

THE FOLLOWING glossary provides, for reference, brief definitions for several terms as used in this paper in the context of protecting information in computers.

Access — The ability to make use of information stored in a computer system. Used frequently as a verb, to the horror of grammarians.

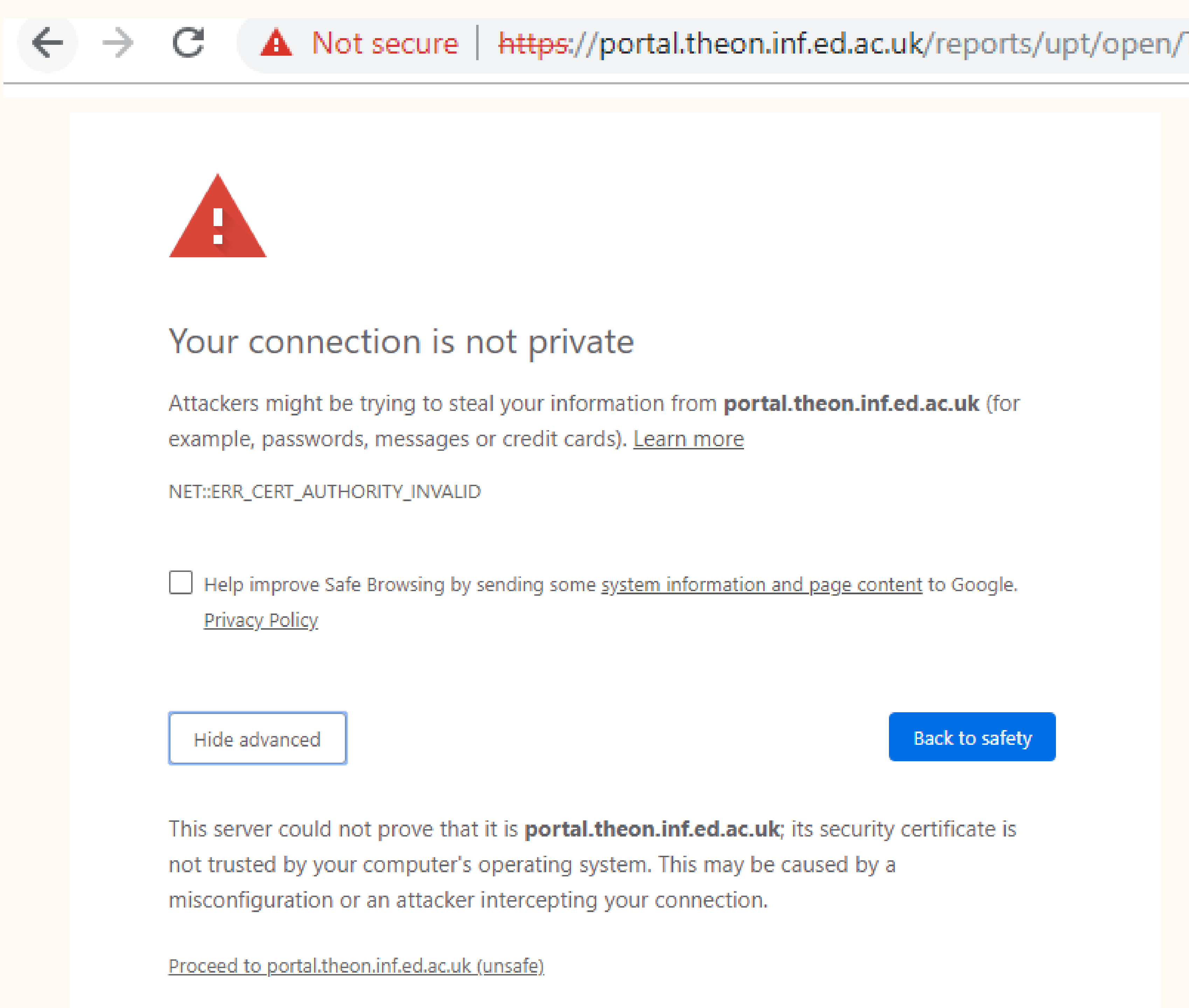
program cannot release the information.

Descriptor — A protected value which is (or leads to) the physical address of some protected object.

Discretionary — (In contrast with *nondiscretionary*.) Controls on access to an object that may be changed by the creator of the object.

I'd like to use this example.

But first you need to understand what this error is talking about.



~~https~~://portal.theon.inf.ed.ac.uk/reports/upt/open/

Your connection is not private

Attackers might be trying to steal your information from **portal.theon.inf.ed.ac.uk** (for example, passwords, messages or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

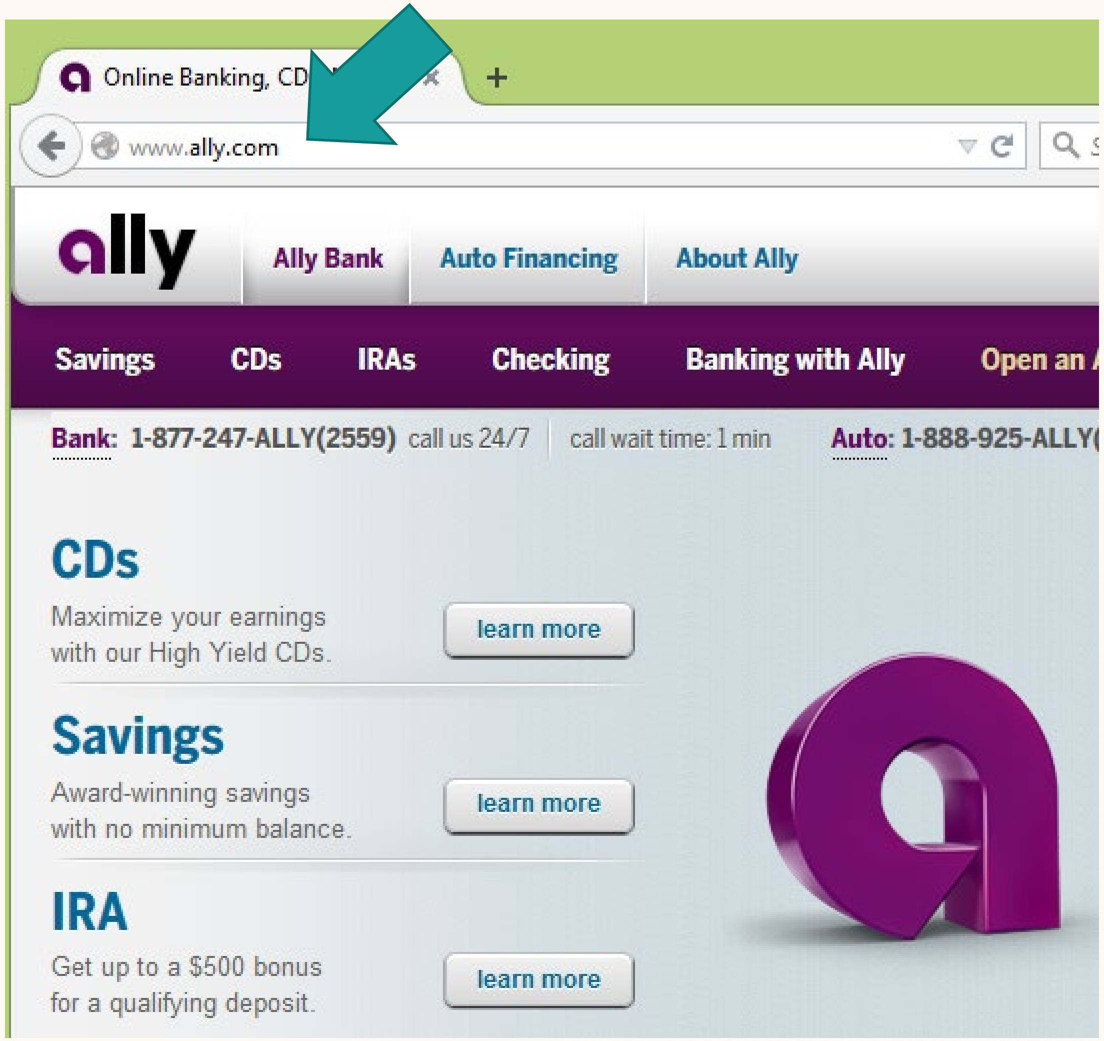
□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy Policy

This server could not prove that it is **portal.theon.inf.ed.ac.uk**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to portal.theon.inf.ed.ac.uk (unsafe)

Short primer on HTTPS

http versus https



Bank: 1-877-247-ALLY(2559) call us 24/7 | call wait time: 1 min Auto: 1-888-925-ALLY(

CDs

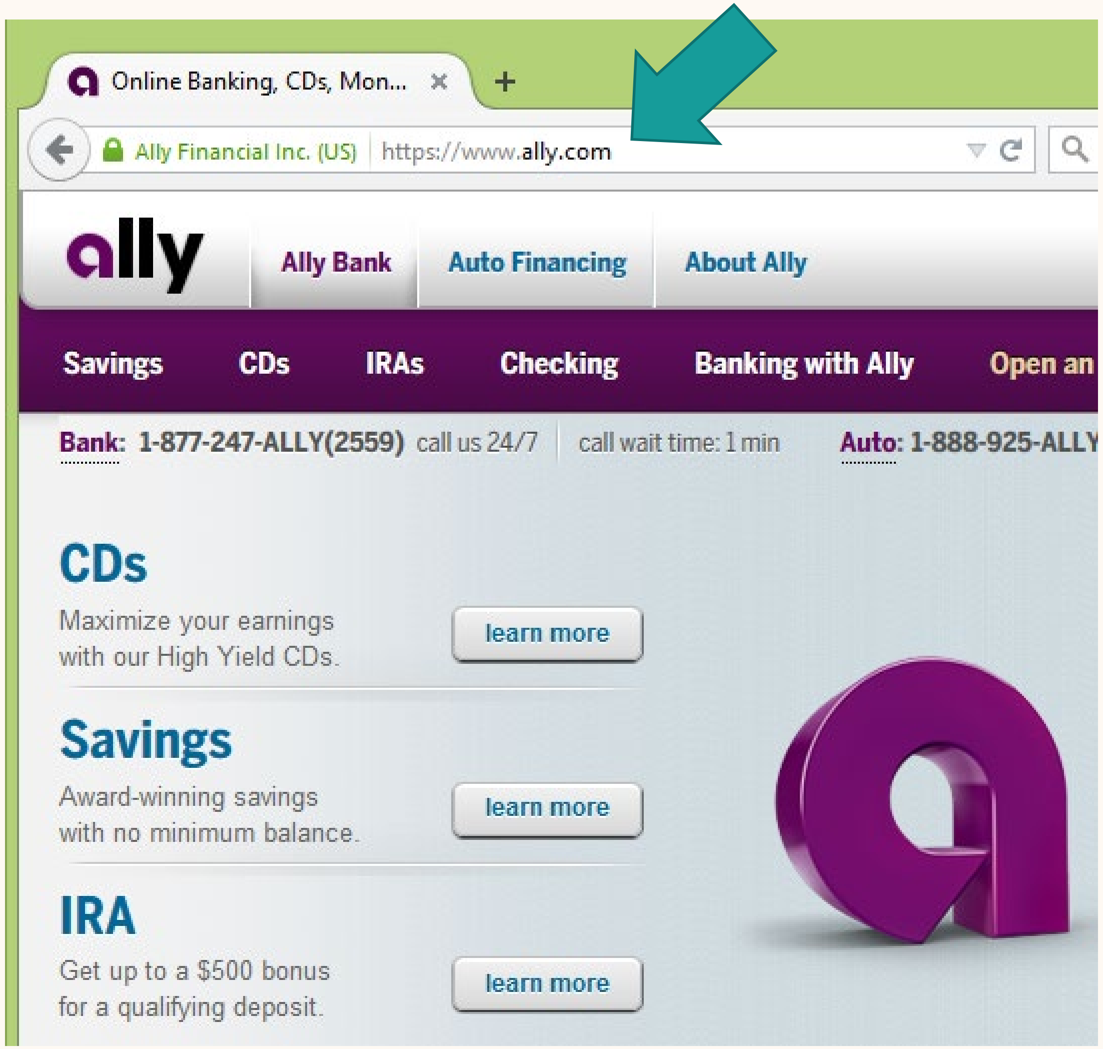
Maximize your earnings with our High Yield CDs.

Savings

Award-winning savings with no minimum balance.

IRA

Get up to a $500 bonus for a qualifying deposit.



Bank: 1-877-247-ALLY(2559) call us 24/7 | call wait time: 1 min Auto: 1-888-925-ALLY

CDs

Maximize your earnings with our High Yield CDs.

Savings

Award-winning savings with no minimum balance.

IRA

Get up to a $500 bonus for a qualifying deposit.

https://ally.com

versus

http://ally.com

Encryption properties we want:

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

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

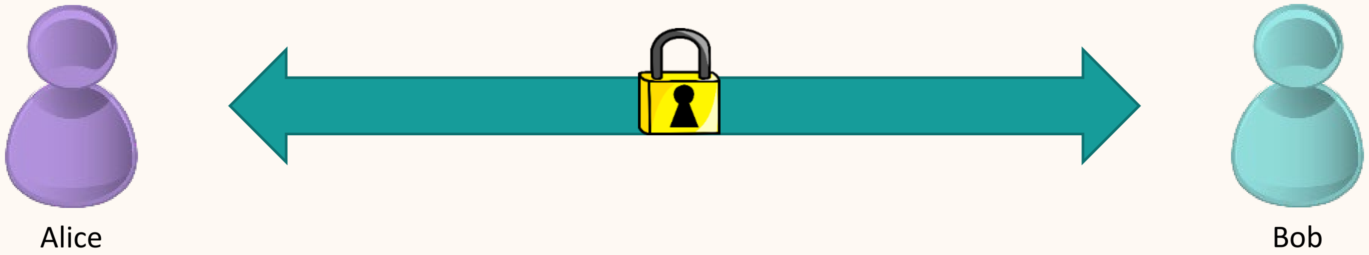
2. **Knowing who** you are communicating with

   You are talking to who you think you are talking to and not someone else

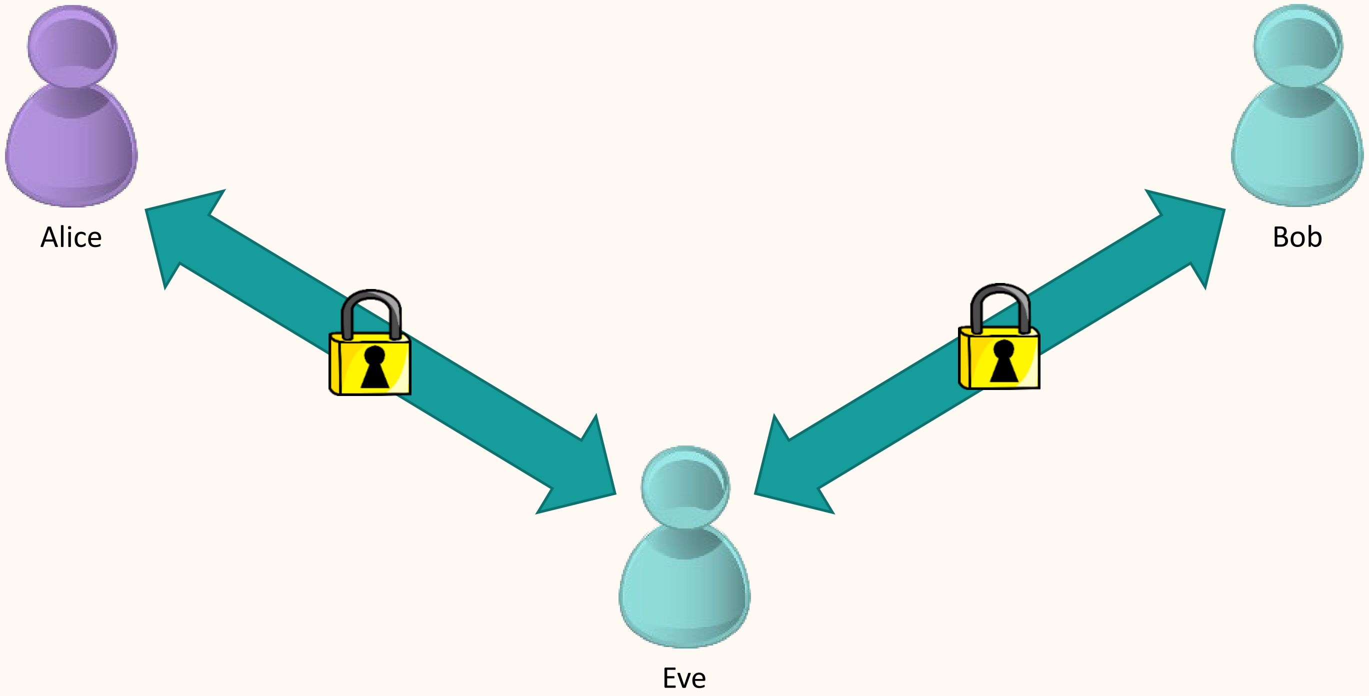
This one is a bit harder. Cryptography can verify you are speaking to the same person, but not identity.

Alice wants to talk securely with Bob

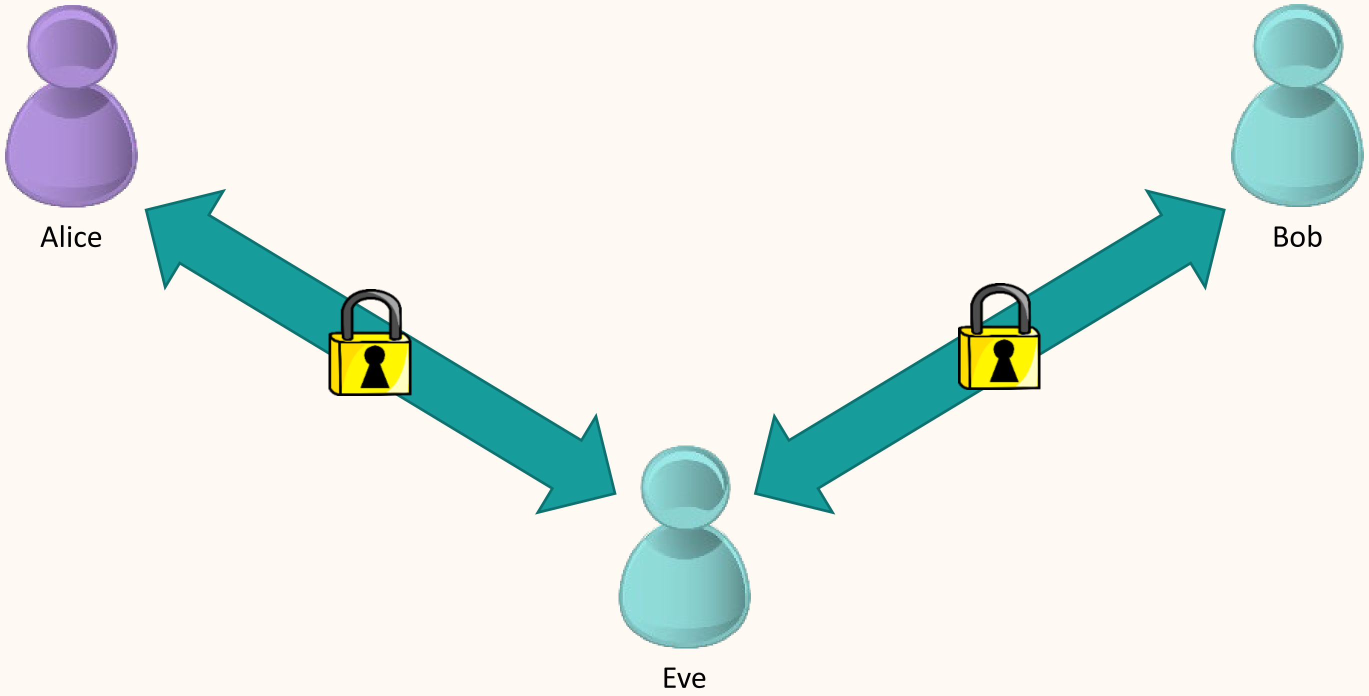
She can encrypt the connection (1)



But how can Alice know she is talking to Bob and not talking to Eve? (2)

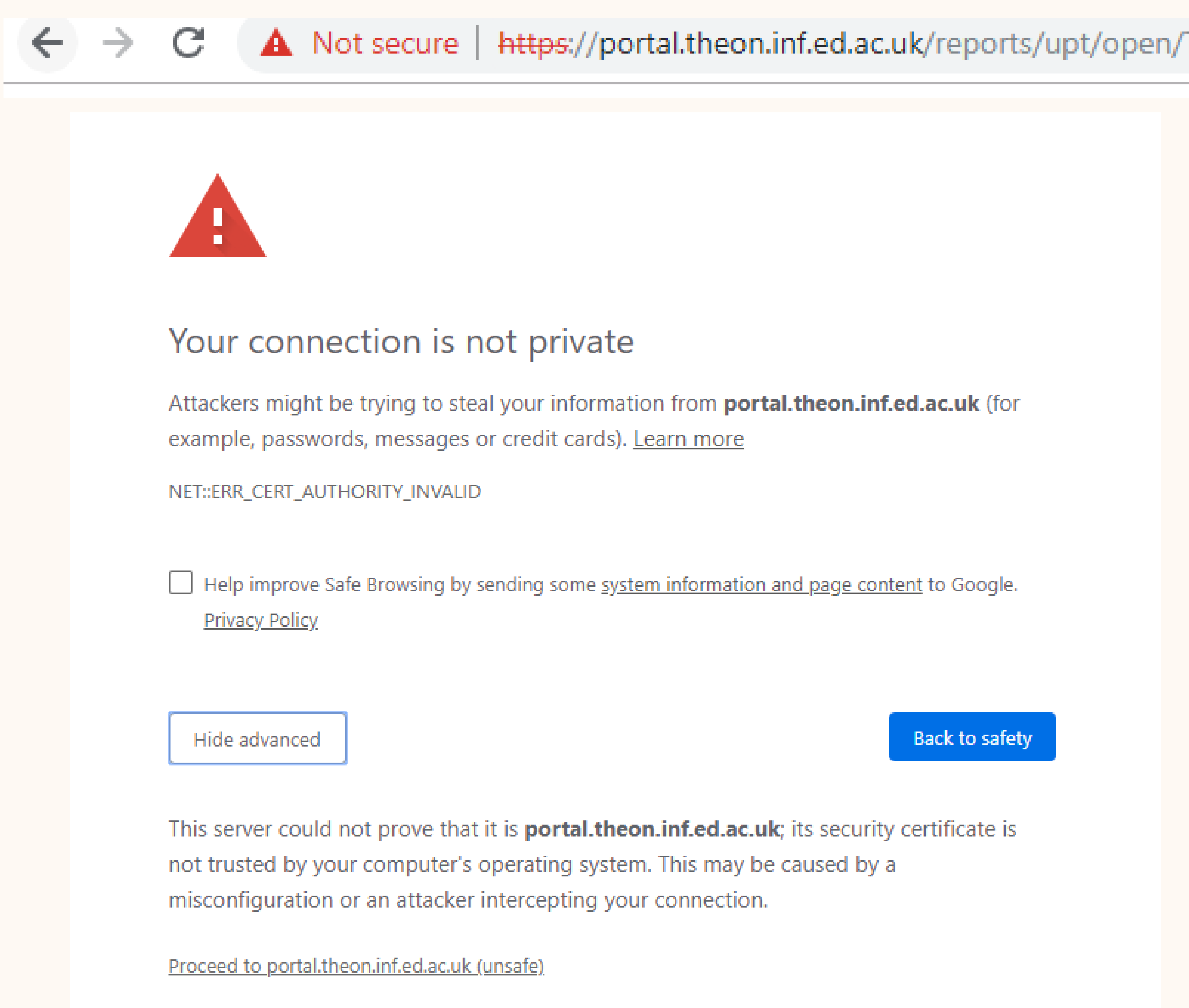


Man in the middle attack



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.



~~https~~://portal.theon.inf.ed.ac.uk/reports/upt/open/

Your connection is not private

Attackers might be trying to steal your information from **portal.theon.inf.ed.ac.uk** (for example, passwords, messages or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

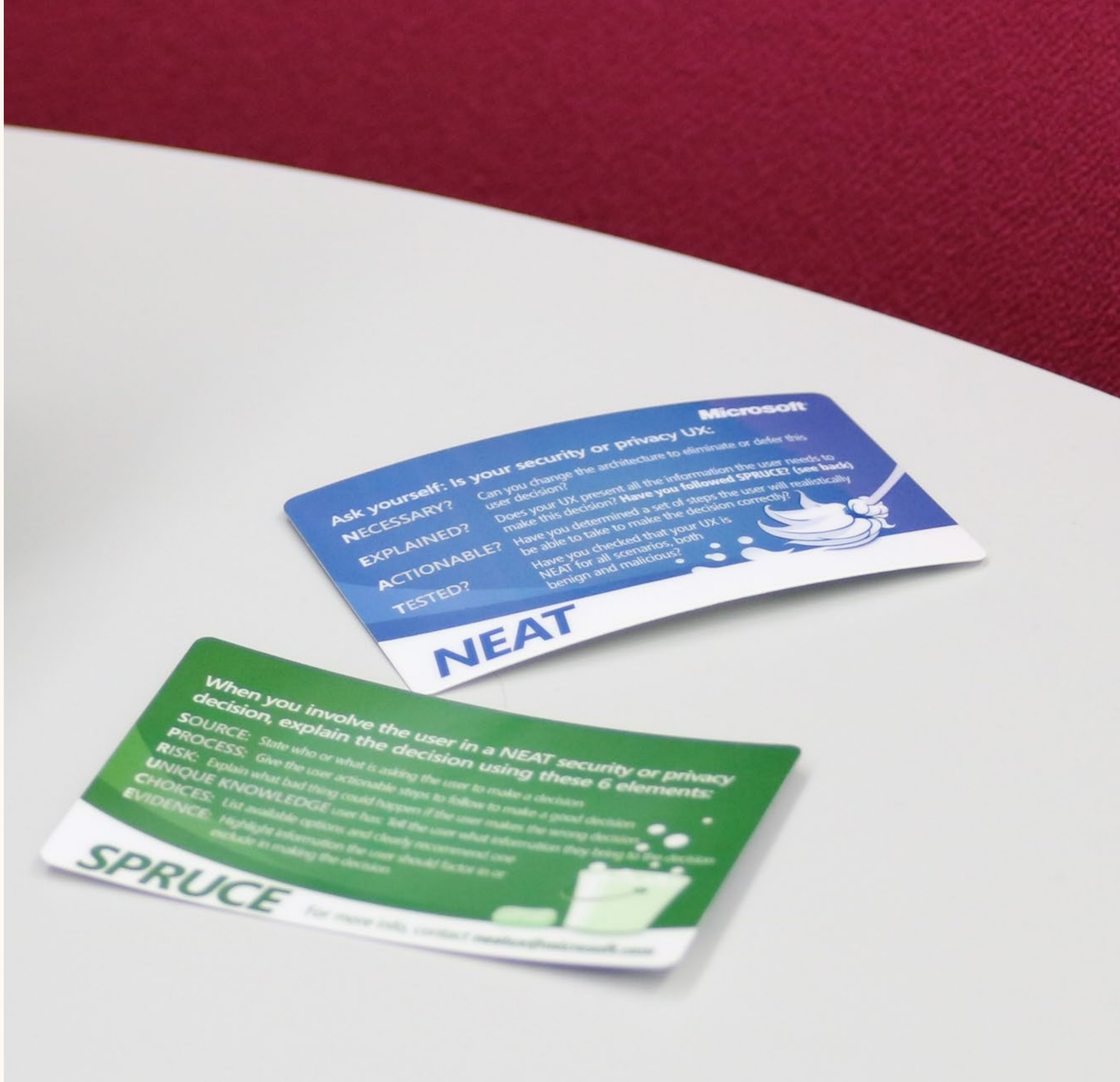
□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy Policy

This server could not prove that it is **portal.theon.inf.ed.ac.uk**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to portal.theon.inf.ed.ac.uk (unsafe)

NEAT and SPRUCE

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



Microsoft

Ask yourself: Is your security or privacy UX:

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

EXPLAINED? Does your UX present all the information the user needs to make this decision? **Have you followed SPRUCE? (see back)**

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 UX is NEAT for all scenarios, both benign and malicious?

NEAT

When you involve the user in a NEAT security or privacy decision, explain the decision using these 6 elements:

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 the user makes the wrong decision

UNIQUE KNOWLEDGE 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 the decision

SPRUCE For more info, contact [illegible]

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?

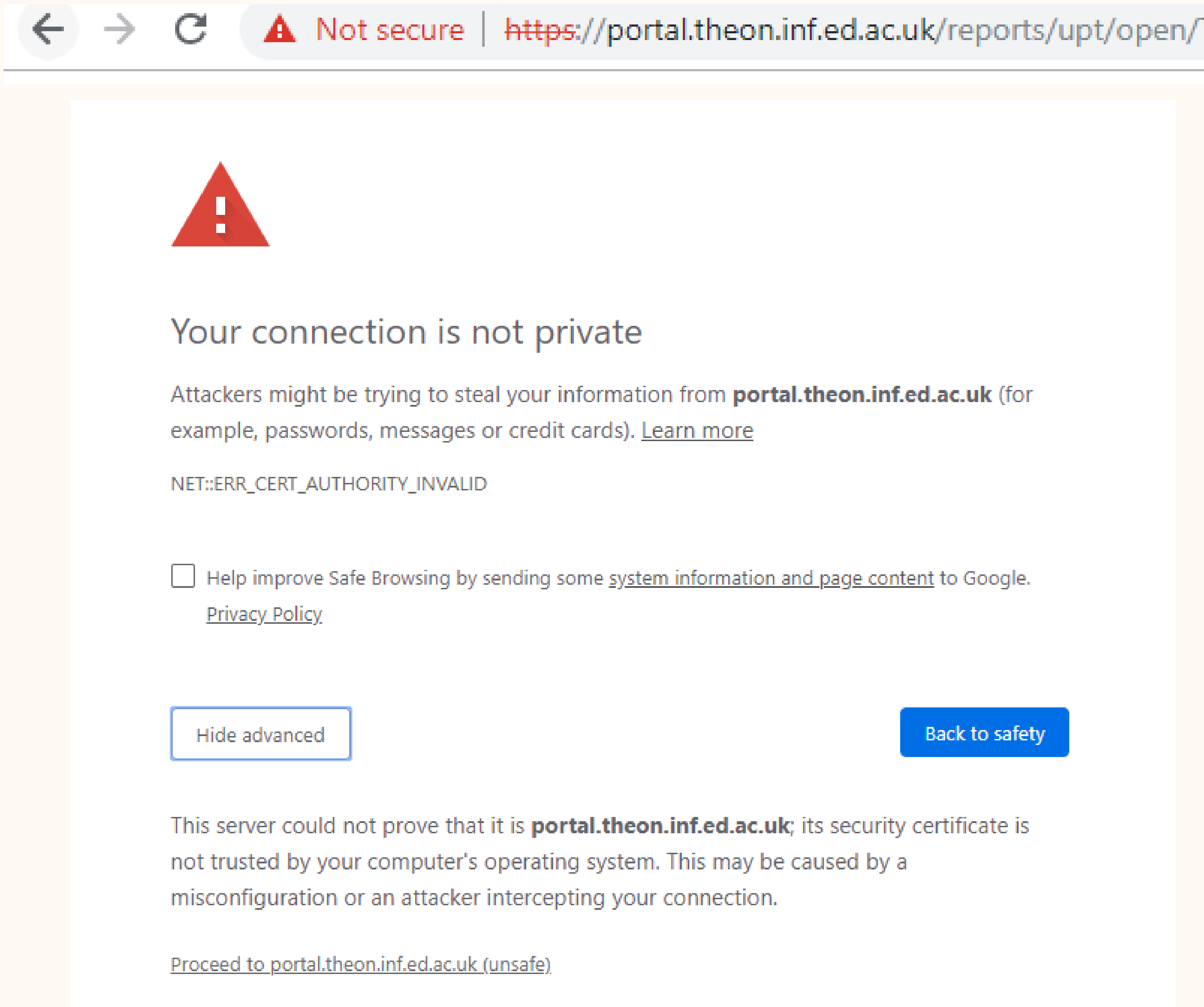
Tested – Have you checked that your user experience is NEAT for all scenarios, both benign and malicious? Have you tested it on a human who is not a member of your team?

Necessary

Explained

Actionable

Tested



Not secure | ~~https~~://portal.theon.inf.ed.ac.uk/reports/upt/open/

Your connection is not private

Attackers might be trying to steal your information from **portal.theon.inf.ed.ac.uk** (for example, passwords, messages or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy Policy

This server could not prove that it is **portal.theon.inf.ed.ac.uk**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to portal.theon.inf.ed.ac.uk (unsafe)

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

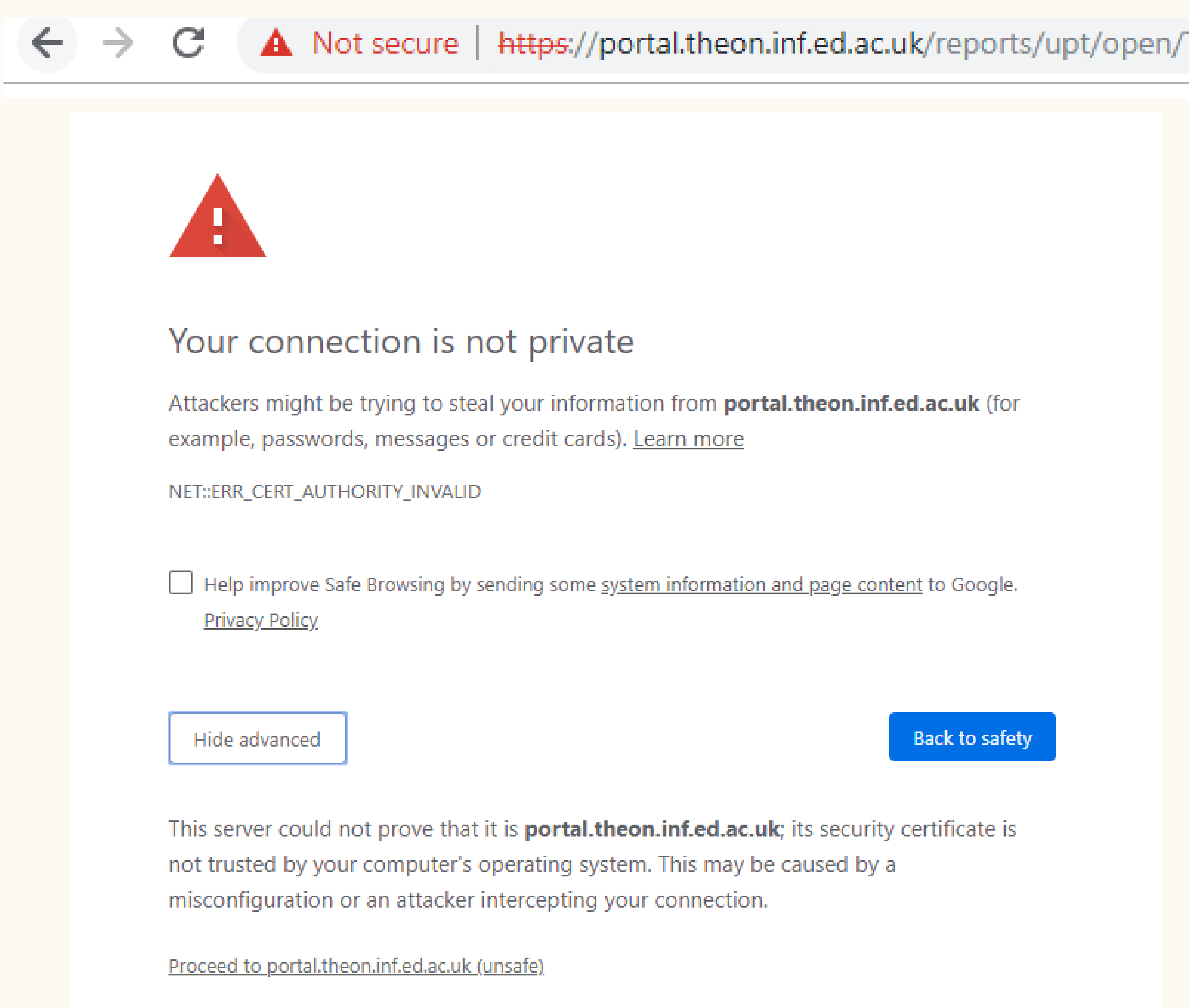
Process

Risk

Unique

Choices

Evidence



Your connection is not private

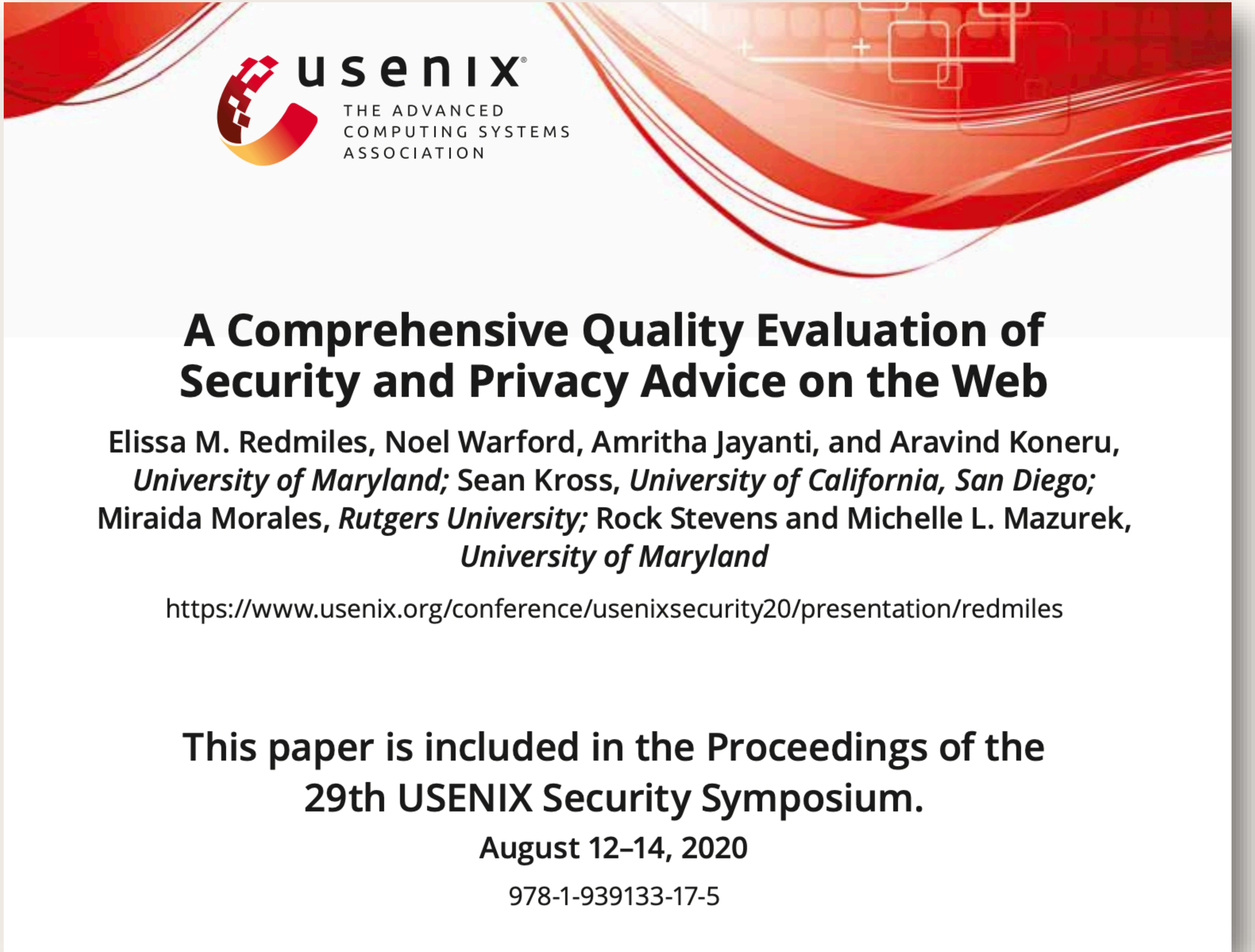
Attackers might be trying to steal your information from **portal.theon.inf.ed.ac.uk** (for example, passwords, messages or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy Policy

This server could not prove that it is **portal.theon.inf.ed.ac.uk**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to portal.theon.inf.ed.ac.uk (unsafe)



A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web

Elissa M. Redmiles, Noel Warford, Amritha Jayanti, and Aravind Koneru, *University of Maryland;* Sean Kross, *University of California, San Diego;* Miraida Morales, *Rutgers University;* Rock Stevens and Michelle L. Mazurek, *University of Maryland*

https://www.usenix.org/conference/usenixsecurity20/presentation/redmiles

This paper is included in the Proceedings of the 29th USENIX Security Symposium.

August 12–14, 2020

978-1-939133-17-5

Contribution

- Taxonomy of security and privacy advice
- Quality evaluation of security and privacy advice

Contribution and method

- Taxonomy of security and privacy advice
  - Online scraping of 2780 pieces of advice; human annotation and analysis
- Quality evaluation of security and privacy advice
  - Survey and evaluation with 1586 User and 41 experts

Identifying advice

- How do people get advice online -> crowdsourcing search queries for security and privacy advice
- Where experts find and recommend advice? -> asking security experts
- Result: 1264 out of 1896 documents after cleaning

Topics of advice

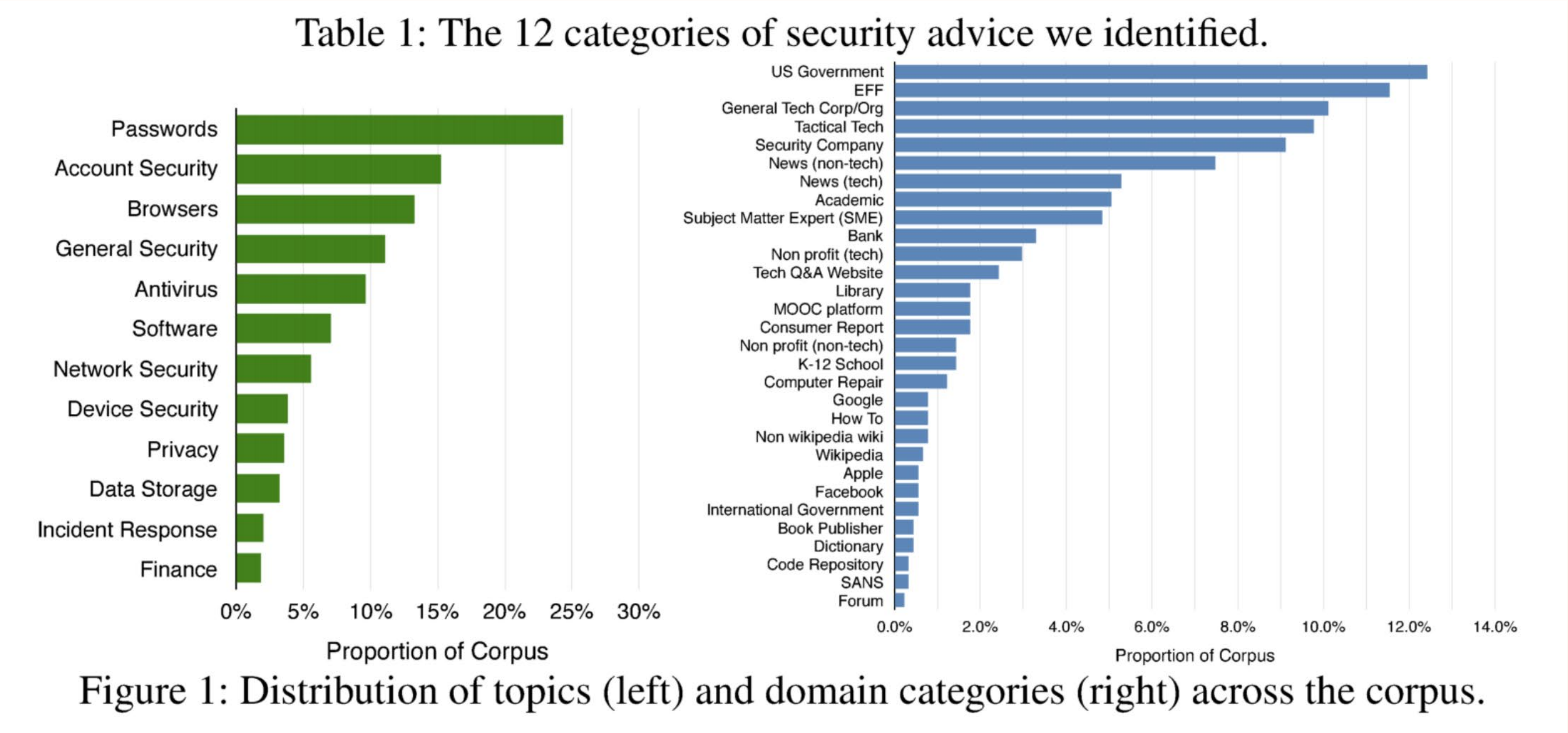


Table 1: The 12 categories of security advice we identified.

Figure 1: Distribution of topics (left) and domain categories (right) across the corpus.

- Qualitative coding and analysis

Evaluating advice: metrics

- Perceived actionability
  - Confidence: how confident users can implement it
  - Time consumption: how time consuming people think it would take to implement
  - Disruption: how disruptive people think when implementing it
  - Difficulty: how difficult people think it is to implement
- Scale: 4-point Likert from “Not at All” to “Very”
- Framework: building on Protection Motivation Theory and Human in the Loop model

Evaluating advice: metrics

- Perceived efficacy: whether the experts believe that a typical user would experience an improvement or not
- Comprehensibility: multiple measures for evaluating text comprehension, e.g., “How easy is this document to read?”

Results

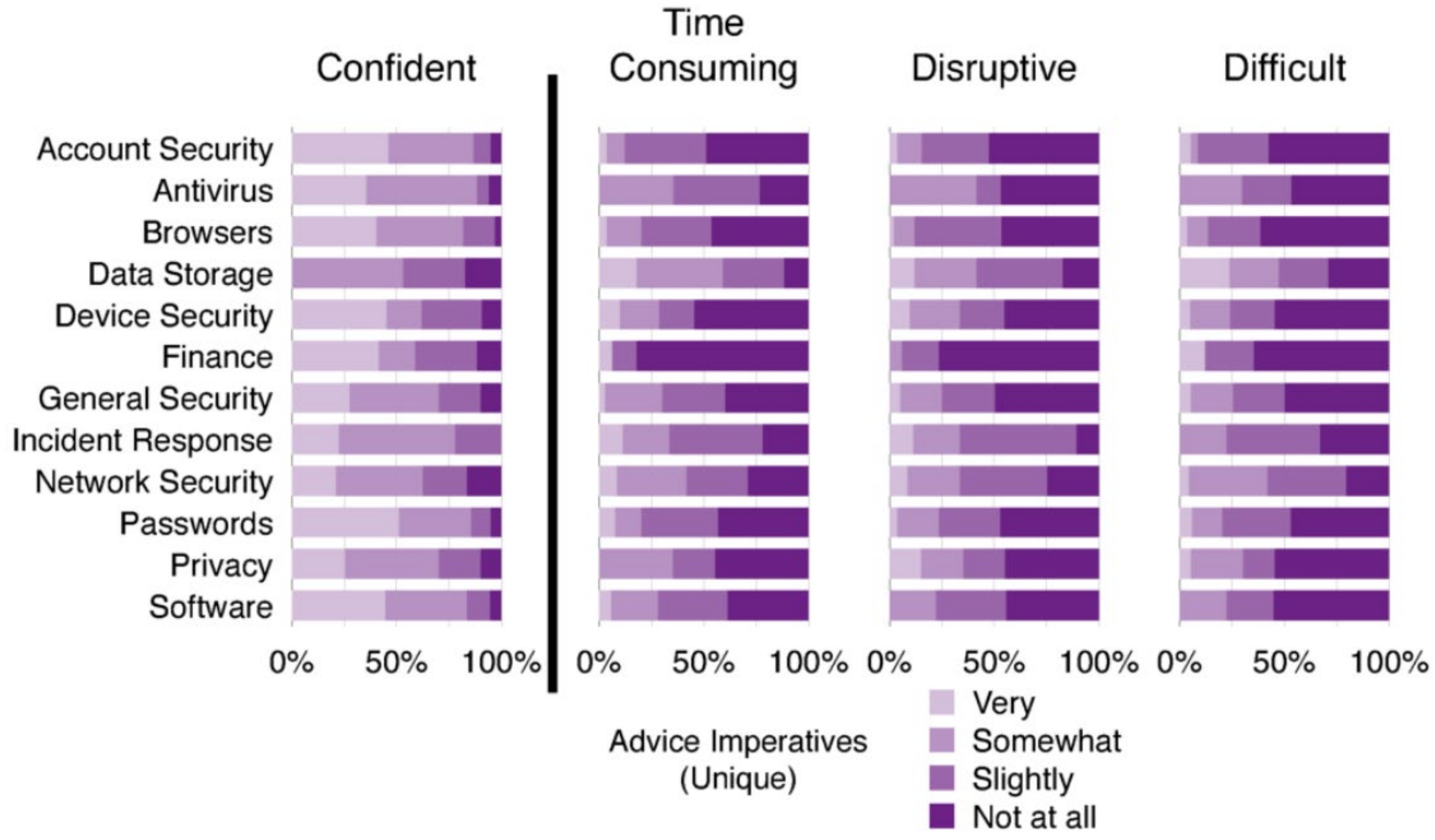
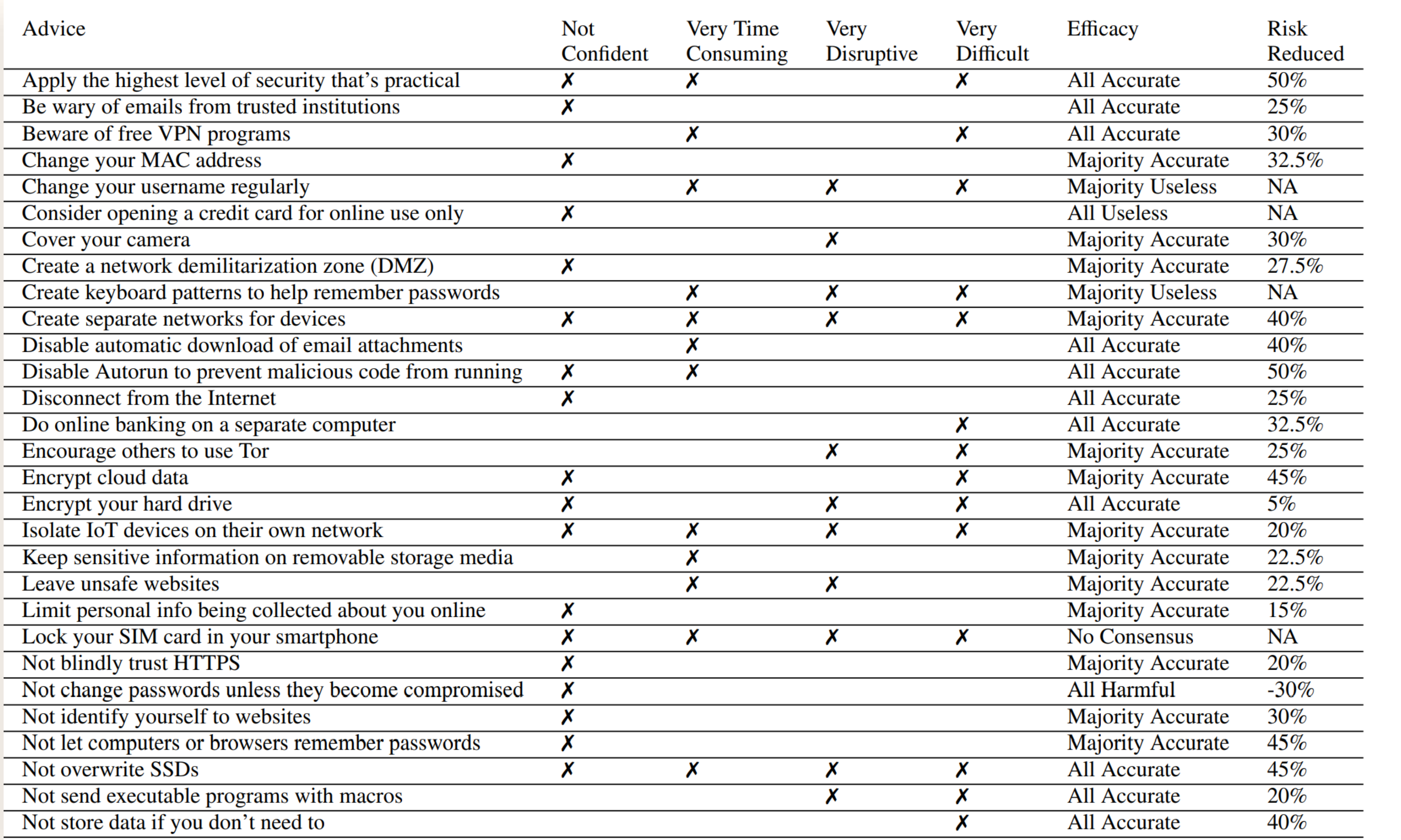


Figure 3: Advice actionability by topic across 374 unique advice imperatives.

Results



Advice	Not Confident	Very Time Consuming	Very Disruptive	Very Difficult	Efficacy	Risk Reduced
Apply the highest level of security that's practical	✗	✗		✗	All Accurate	50%
Be wary of emails from trusted institutions	✗				All Accurate	25%
Beware of free VPN programs		✗		✗	All Accurate	30%
Change your MAC address	✗				Majority Accurate	32.5%
Change your username regularly		✗	✗	✗	Majority Useless	NA
Consider opening a credit card for online use only	✗				All Useless	NA
Cover your camera			✗		Majority Accurate	30%
Create a network demilitarization zone (DMZ)	✗				Majority Accurate	27.5%
Create keyboard patterns to help remember passwords		✗	✗	✗	Majority Useless	NA
Create separate networks for devices	✗	✗	✗	✗	Majority Accurate	40%
Disable automatic download of email attachments		✗			All Accurate	40%
Disable Autorun to prevent malicious code from running	✗	✗			All Accurate	50%
Disconnect from the Internet	✗				All Accurate	25%
Do online banking on a separate computer				✗	All Accurate	32.5%
Encourage others to use Tor			✗	✗	Majority Accurate	25%
Encrypt cloud data	✗			✗	Majority Accurate	45%
Encrypt your hard drive	✗		✗	✗	All Accurate	5%
Isolate IoT devices on their own network	✗	✗	✗	✗	Majority Accurate	20%
Keep sensitive information on removable storage media		✗			Majority Accurate	22.5%
Leave unsafe websites		✗	✗		Majority Accurate	22.5%
Limit personal info being collected about you online	✗				Majority Accurate	15%
Lock your SIM card in your smartphone	✗	✗	✗	✗	No Consensus	NA
Not blindly trust HTTPS	✗				Majority Accurate	20%
Not change passwords unless they become compromised	✗				All Harmful	-30%
Not identify yourself to websites	✗				Majority Accurate	30%
Not let computers or browsers remember passwords	✗				Majority Accurate	45%
Not overwrite SSDs	✗	✗	✗	✗	All Accurate	45%
Not send executable programs with macros			✗	✗	All Accurate	20%
Not store data if you don't need to				✗	All Accurate	40%

Results

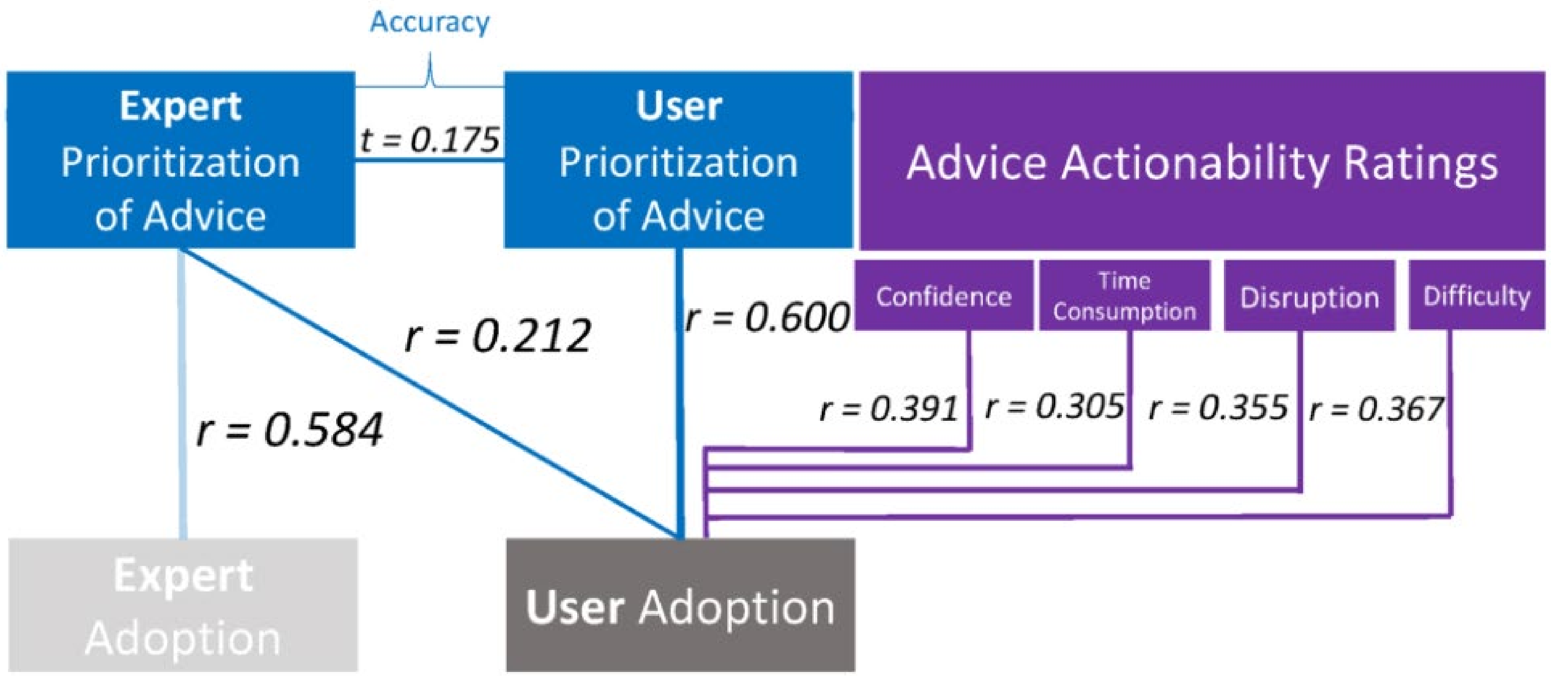


Figure 6: Correlation between security advice adoption, actionability, and priority rankings.

Questions

Take-home

- **(Blog)** Geeng, C., Harris, M., Redmiles, E. and Roesner, F., 2022. "Like Lesbians Walking the Perimeter": Experiences of US LGBTQ+ Folks With Online Security, Safety, and Privacy Advice. In *31st USENIX Security Symposium (USENIX Security 22)* (pp. 305-322).
- **(Blog)** NCSC - Social Media: how to use it safely