Security and Privacy Advice and Warning

INFR11158/11230 Usable Security and Privacy

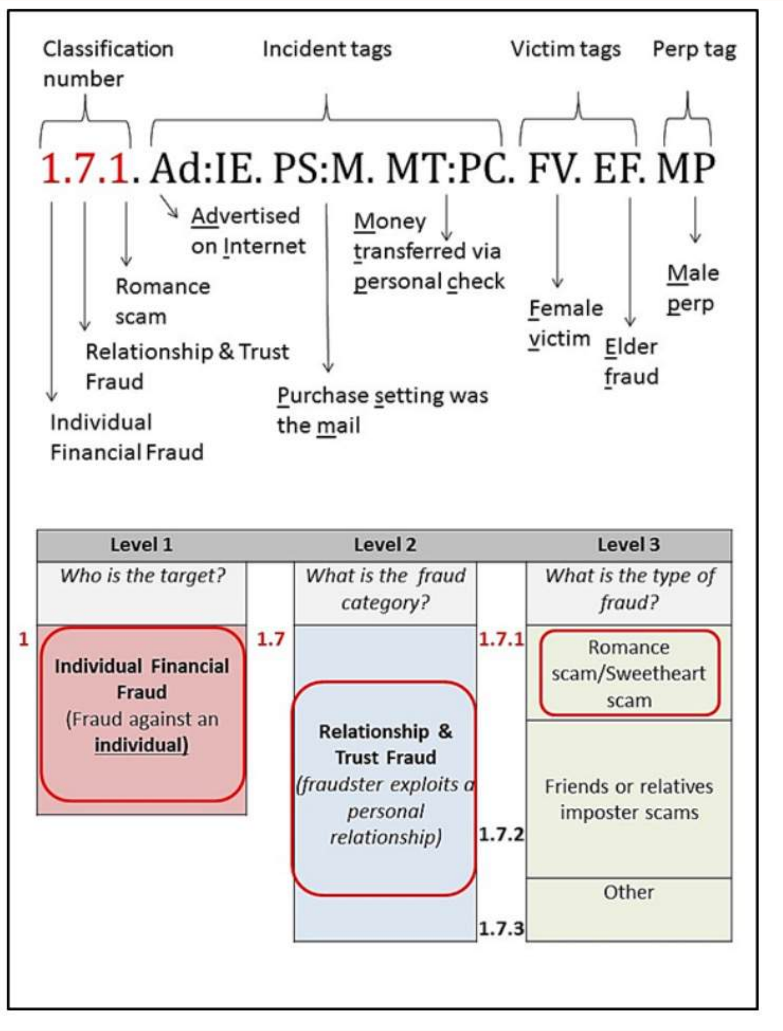
Dr. Jingjie Li

07/03/2025

THE UNIVERSITY of EDINBURGH

Stanford Fraud Taxonomy

Mary, age 67, reports that her online relationship started out as a friendship. Mary found the man on a social networking site. The two “lovers” would tell each other about themselves and later spoke to one another over the phone. He told her he was stuck in Nigeria and needed help to fly home. Mary started mailing checks to help her lover. She blew through her own money and eventually had to start taking out loans to help him.


Classification number
Incident tags
Victim tags
Perp tag
1.7.1. Ad:IE. PS:M. MT:PC. FV. EF. MP
Advertised on Internet
Money transferred via personal check
Romance scam
Relationship & Trust Fraud
Individual Financial Fraud
Purchase setting was the mail
Female victim
Elder fraud
Male perp

Level 1	Level 2	Level 3
Who is the target?	*What is the fraud category?*	*What is the type of fraud?*
1 **Individual Financial Fraud** (Fraud against an **individual)**	1.7 **Relationship & Trust Fraud** *(fraudster exploits a personal relationship)*	1.7.1 Romance scam/Sweetheart scam
		1.7.2 Friends or relatives imposter scams
		1.7.3 Other

https://longevity.stanford.edu/financial-fraud-research-center/wp-content/uploads/2016/03/Full-Taxonomy-report.pdf

Overview of Stanford Fraud Taxonomy

- Consumer Investment Fraud
    - Securities fraud
        - Equity investment fraud
            - Penny stock fraud
            - …
        - …
    - …
- Consumer Products and Services Fraud
    - …
        - *Phishing websites/emails/calls*
- Employment Fraud
- Prize and Grant Fraud
- Phantom Debt Collection Fraud
- Charity Fraud
- Relationship and Trust Fraud

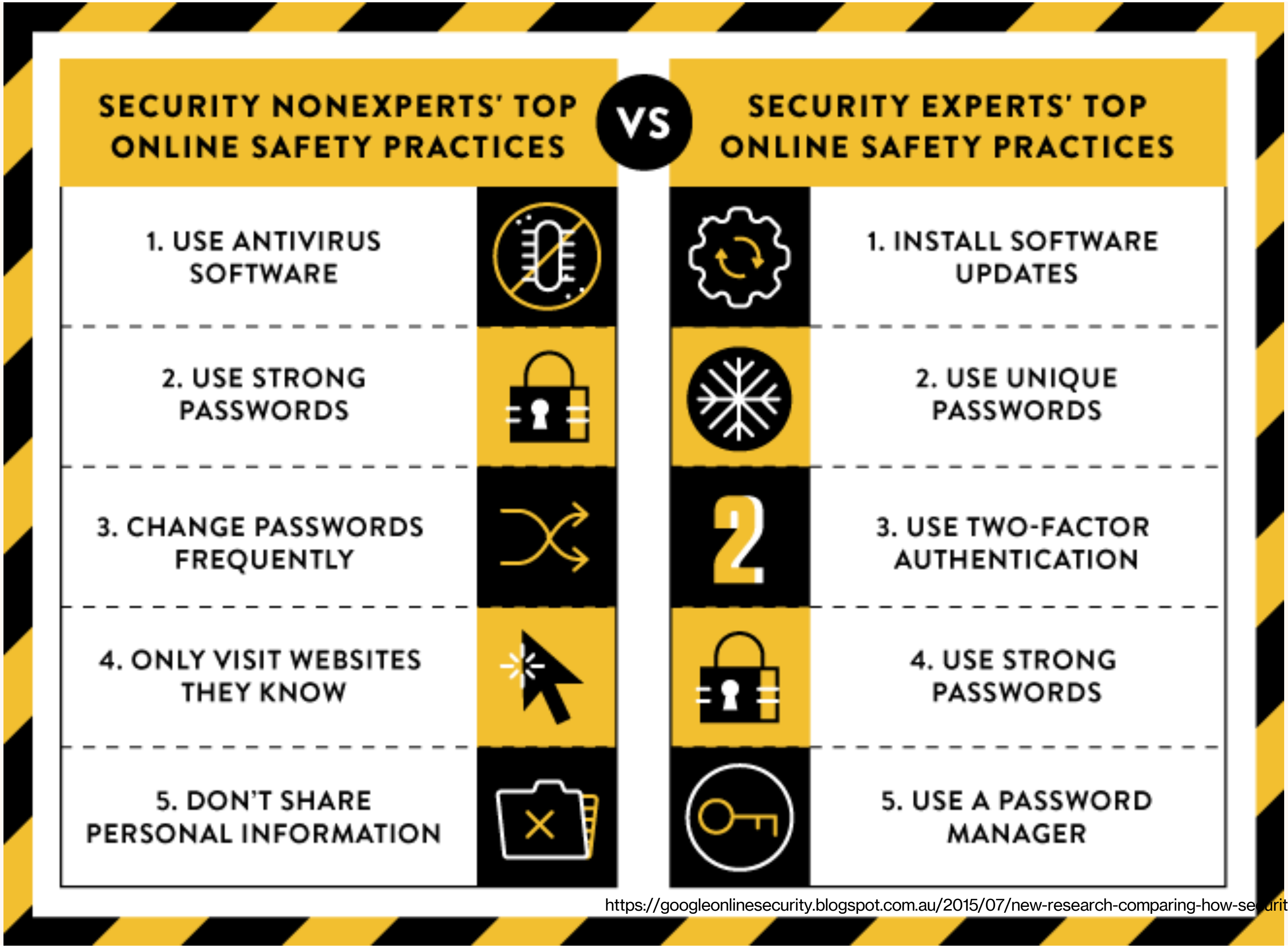
Overview of Stanford Fraud Taxonomy

- Consumer Investment Fraud
    - Investors gain and lose money in financial markets for a variety of legitimate reasons, yet the following definitions refer to investment fraud, where someone knowingly misleads an investor on the basis of false information. While many investment vehicles listed below have legitimate versions, they can also be used in investment scams where the earnings are grossly misrepresented or the investment itself is nonexistent.
- Consumer Products and Services Fraud
    - This broad category covers all fraud related to the purchase of tangible goods and services. It also includes vacations and travel, house/apartment rentals, purchase of pets, concerts/performances, and other events or items the victim paid for but did not receive as promised.
- Employment Fraud
    - In this broad category of fraud schemes, the expected benefit is employment or training to develop a profitable business. Fraudsters advertise work opportunities that require few skills or qualifications, but claim to provide above average financial rewards
- Prize and Grant Fraud
    - The hallmark of this category of fraud is that victims are led to believe they will receive winnings in the form of a prize, lottery, grant, or windfall of money, provided that they first purchase certain products or make advance payments to cover fictitious fees and taxes.

Overview of Stanford Fraud Taxonomy

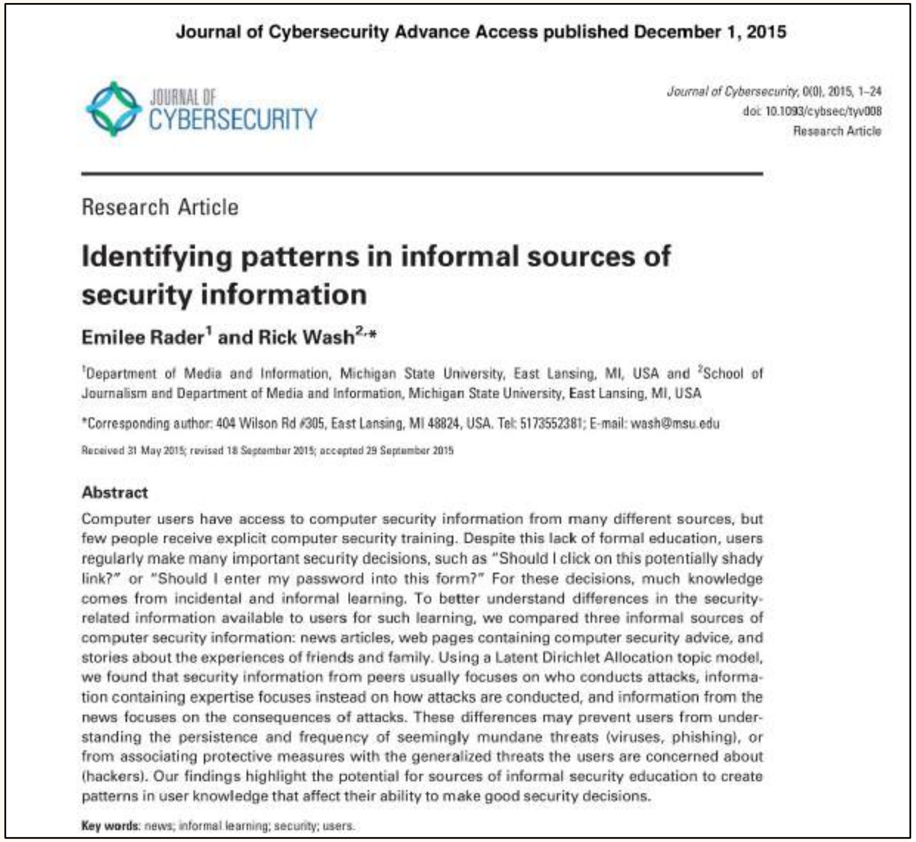
- Phantom Debt Collection Fraud
  - This category of fraud refers to fake debt collectors who deceive and possibly threaten individuals to convince them to pay debts they don't owe.
- Charity Fraud
  - This category of fraud involves scam artists collecting money by posing as a genuine charity. There is no expected benefit or product/service resulting from the transaction. Instead, the expected outcome from the perspective of the victim is organized charitable giving.
- Relationship and Trust Fraud
  - In these schemes, the fraudster exploits a personal relationship with the victim and there is no expectation of a product or service from the interaction. Instead, the expected outcome from the perspective of the victim is the fostering of a personal relationship.

How to prevent online fraud?



SECURITY NONEXPERTS' TOP ONLINE SAFETY PRACTICES	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.

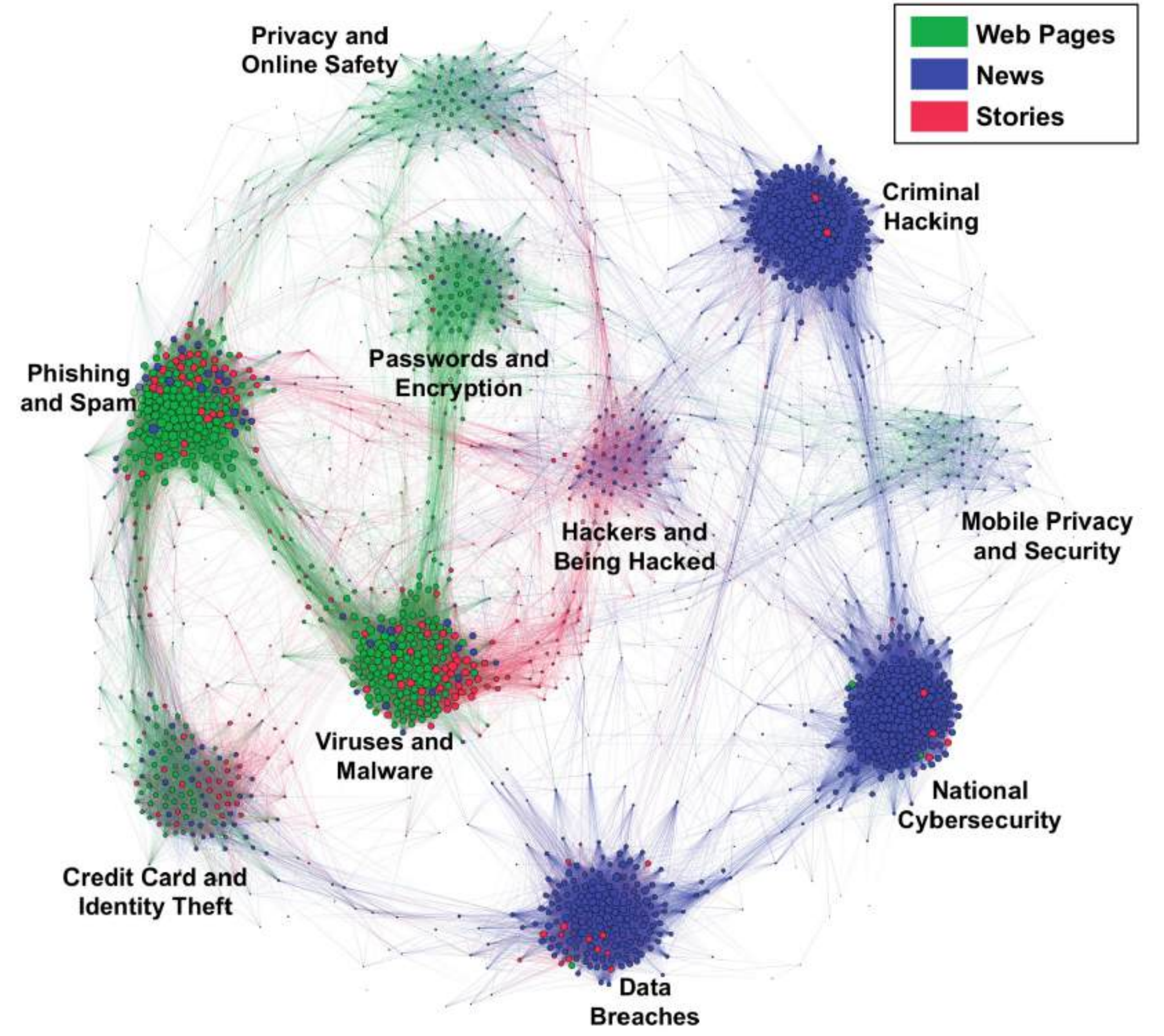
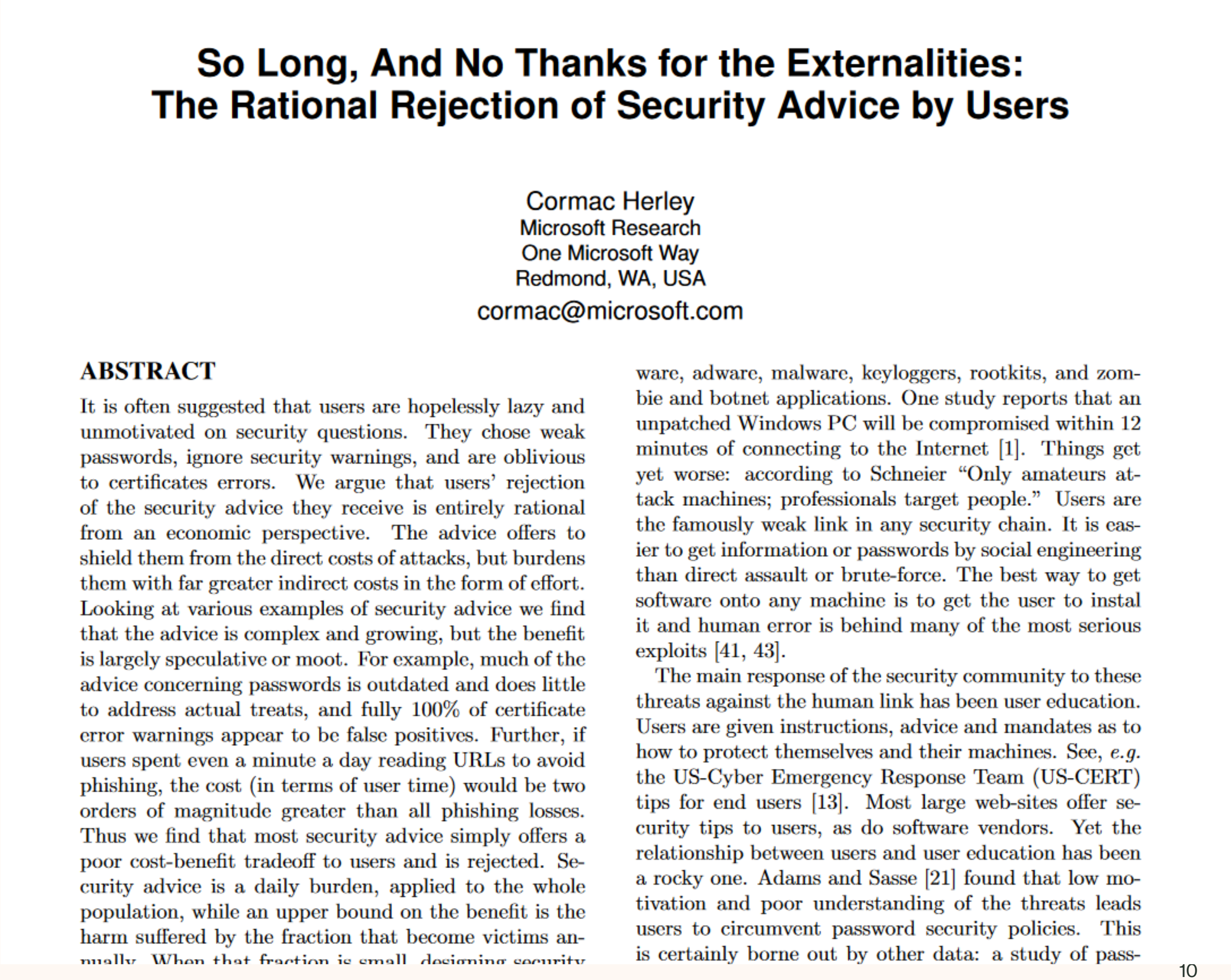


Figure 8. The document similarity graph, with clusters for each topic. There is one node for each document in the dataset. The red nodes are stories, green are web pages, and blue are news articles. Larger nodes are connected to more other documents. Edges represent the Pearson correlation between the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

(How) do people take advice?

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 effect other groups or people.

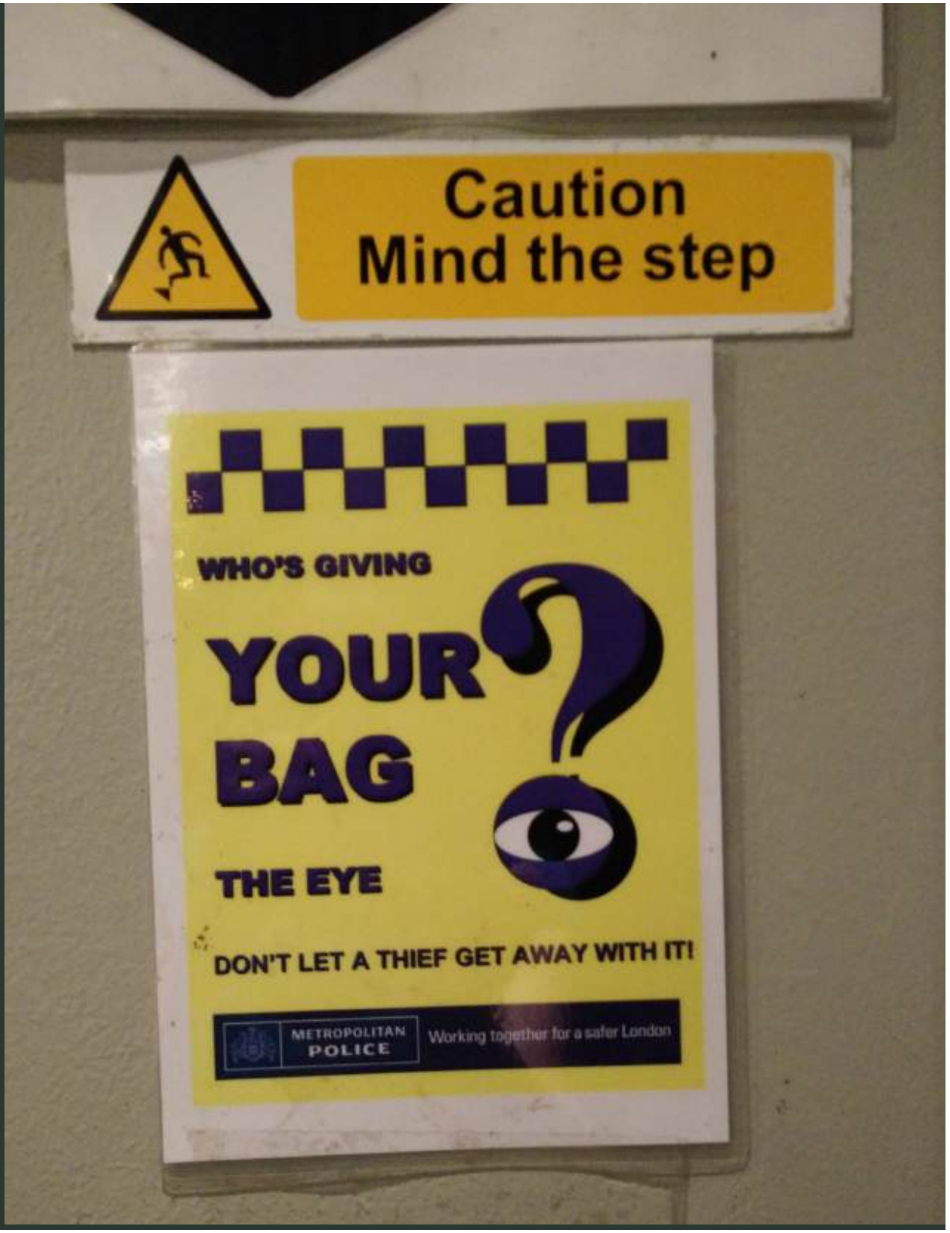
Internality – The costs or benefits of an activity effect the user themselves.

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

Previously we talked about phishing and we talked about advice.

Start thinking about what advice we give people, how we give it, and how to deliver it effectively.


Caution
Mind the step
WHO'S GIVING
YOUR
BAG
THE EYE
DON'T LET A THIEF GET AWAY WITH IT!
METROPOLITAN POLICE
Working together for a safer London

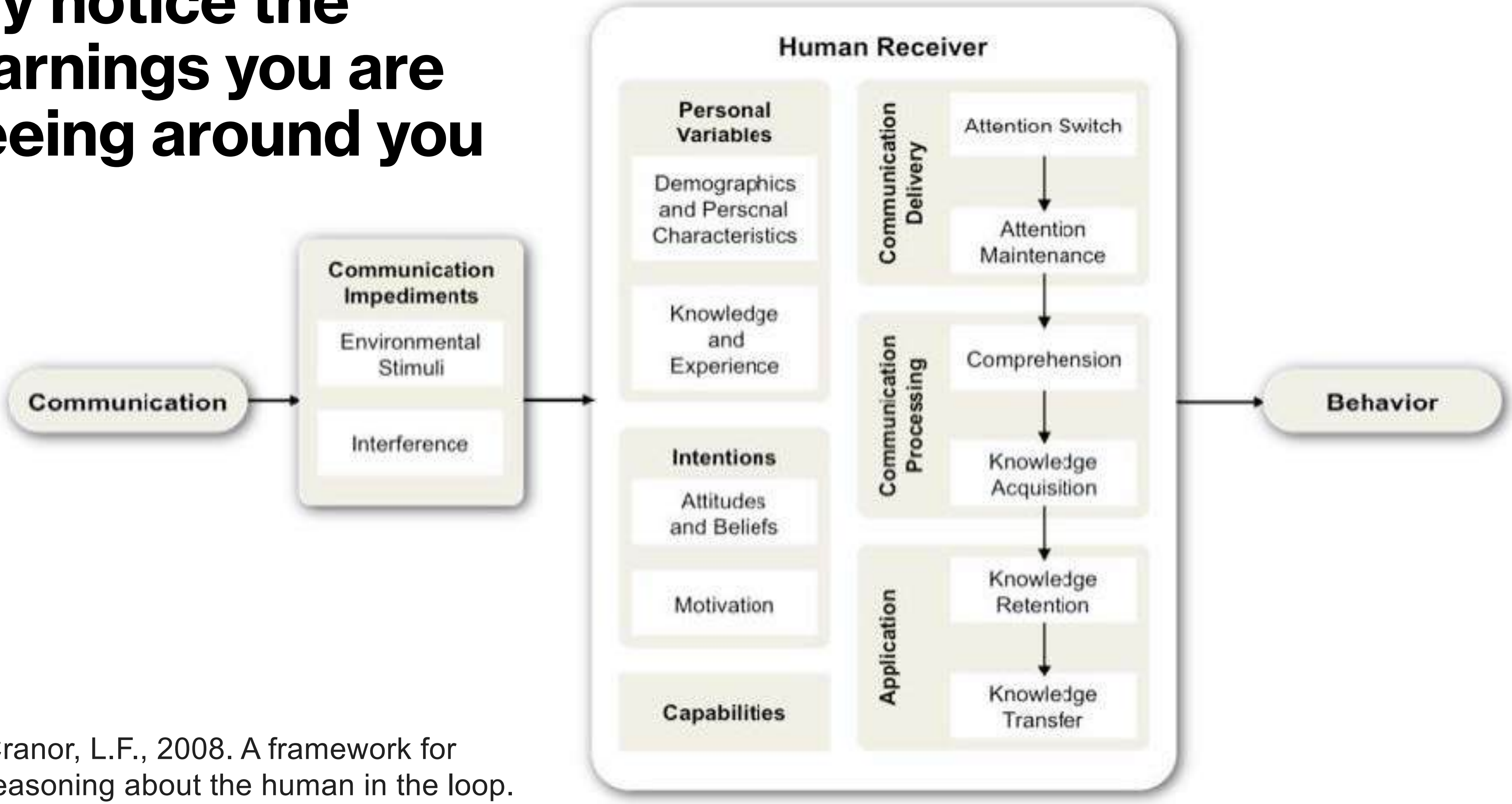
In the next few slides I want to make three points:

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

Try notice the warnings you are seeing around you

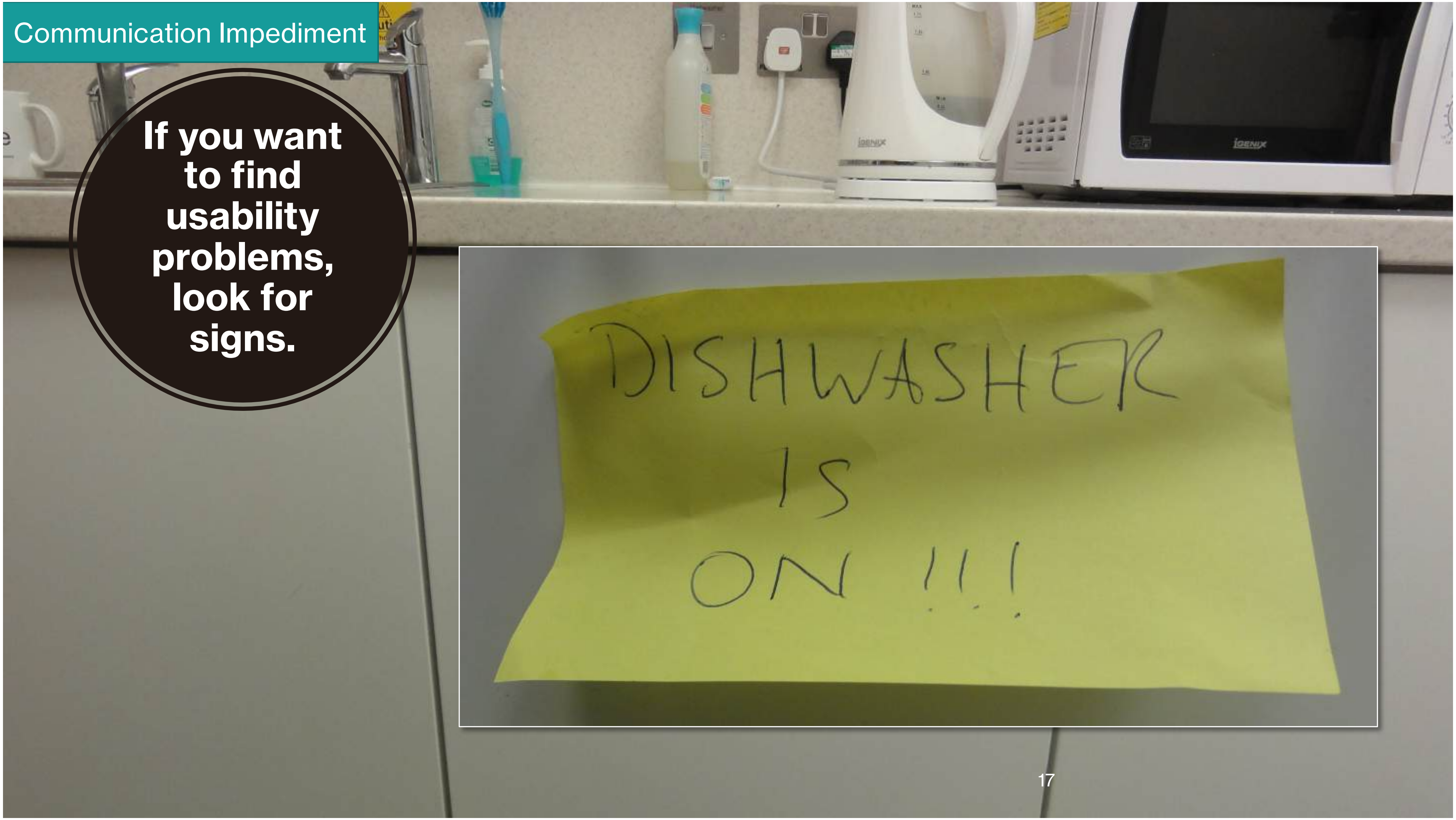


Cranor, L.F., 2008. A framework for reasoning about the human in the loop.

Human in the Loop: Communication Impediments

- **Environmental stimuli** (either related or unrelated) may divert users' attention away
- **Interference** prevents communication from being received as intended (can be malicious)

Communication Impediment



If you want to find usability problems, look for signs.

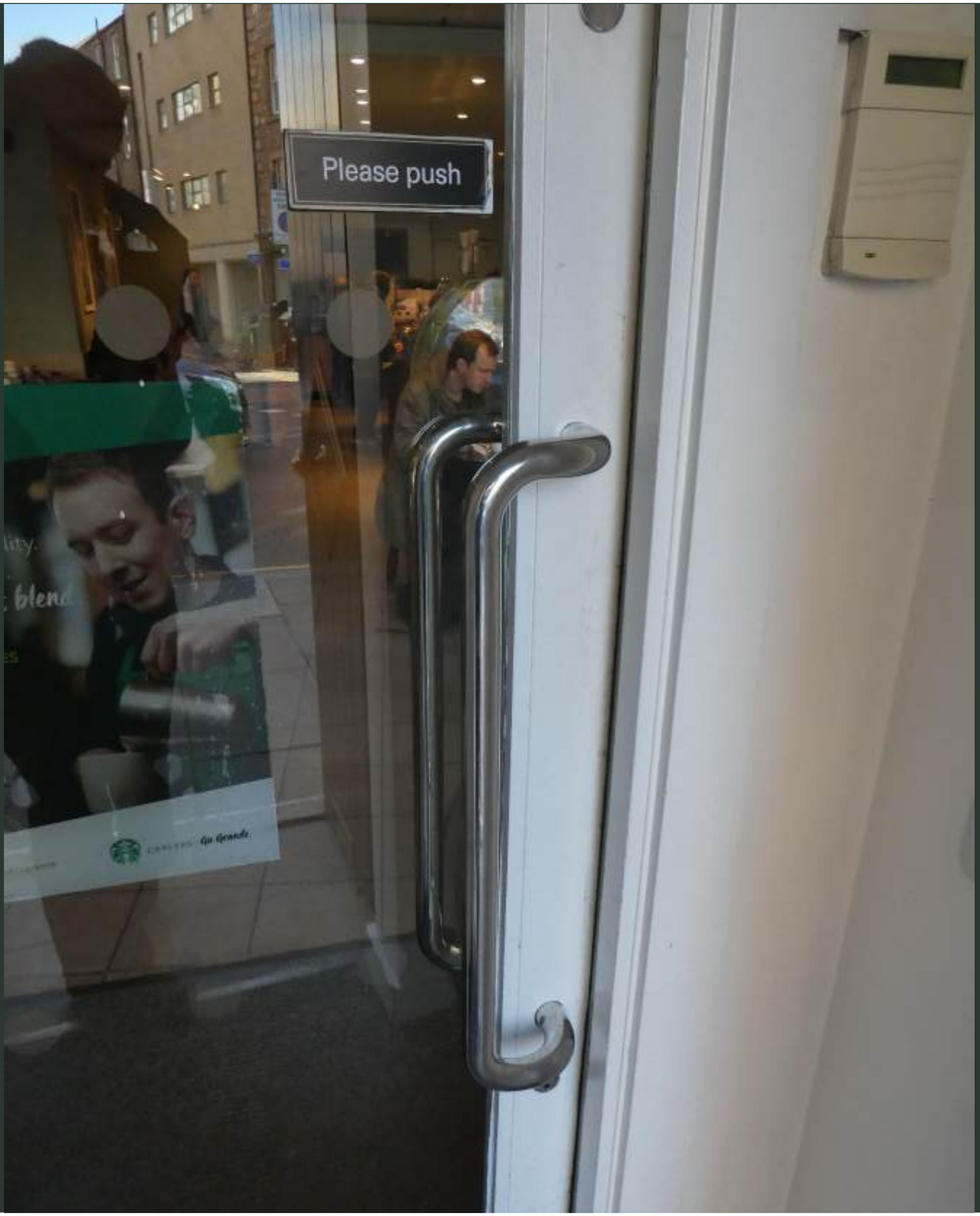
Human in the Loop: Human Receiver

- **Communication delivery:** should pay attention long enough to process it
- **Communication processing:** comprehend and acquire knowledge
- **Application:** retent the knowledge and knows when it’s applicable and to apply it

Communication Delivery

First reaction: Pull

Sign says: Push

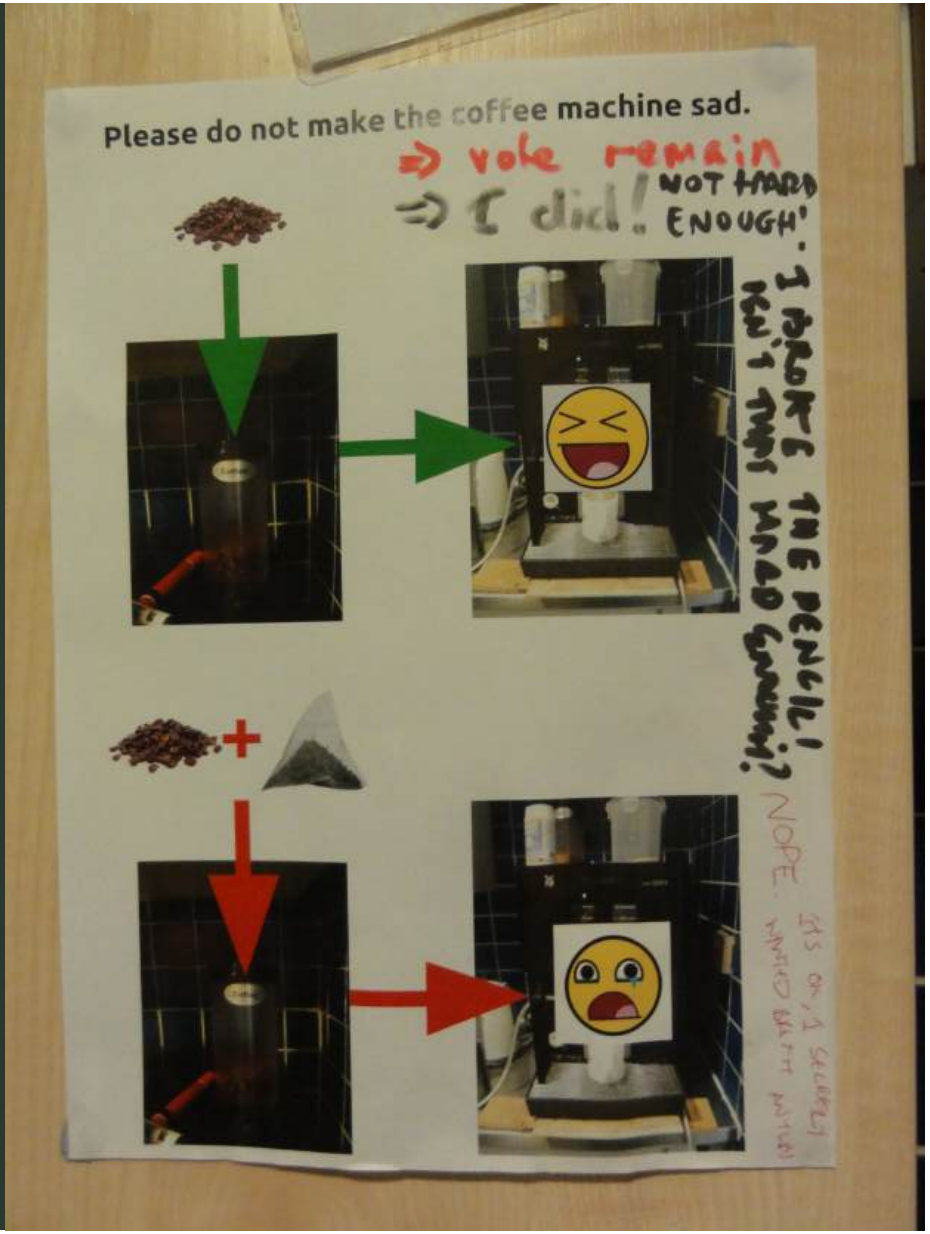


Human in the Loop: Human Receiver

- **Personal variables,** e.g., demographics, personal characteristics, knowledge , etc. – ability to comprehend and apply communications
- **Intentions** like attitudes, impacting the decision of whether to pay attention on a communication
- **Capabilities** to take proper actions

Knowledge and Experience

Maybe something is not obvious



Please do not make the coffee machine sad.

⇒ vote remain

⇒ I did! NOT HARD ENOUGH'.

I BROKE THE PENCIL! ISN'T THIS HARD ENOUGH?

NOPE. ITS OK, I SECRETLY WANTED BREXIT ANYWAY

Knowledge Acquisition & Retention

Maybe the tool is too confusing to use without explanation

Attitudes and Beliefs

Maybe people have an attitude that certain warnings don’t apply to them or are not actually relevant

Intentions

Signs highlight common problems people in a space are experiencing.

Intention – tradeoff happens here, but not always in a very rational way

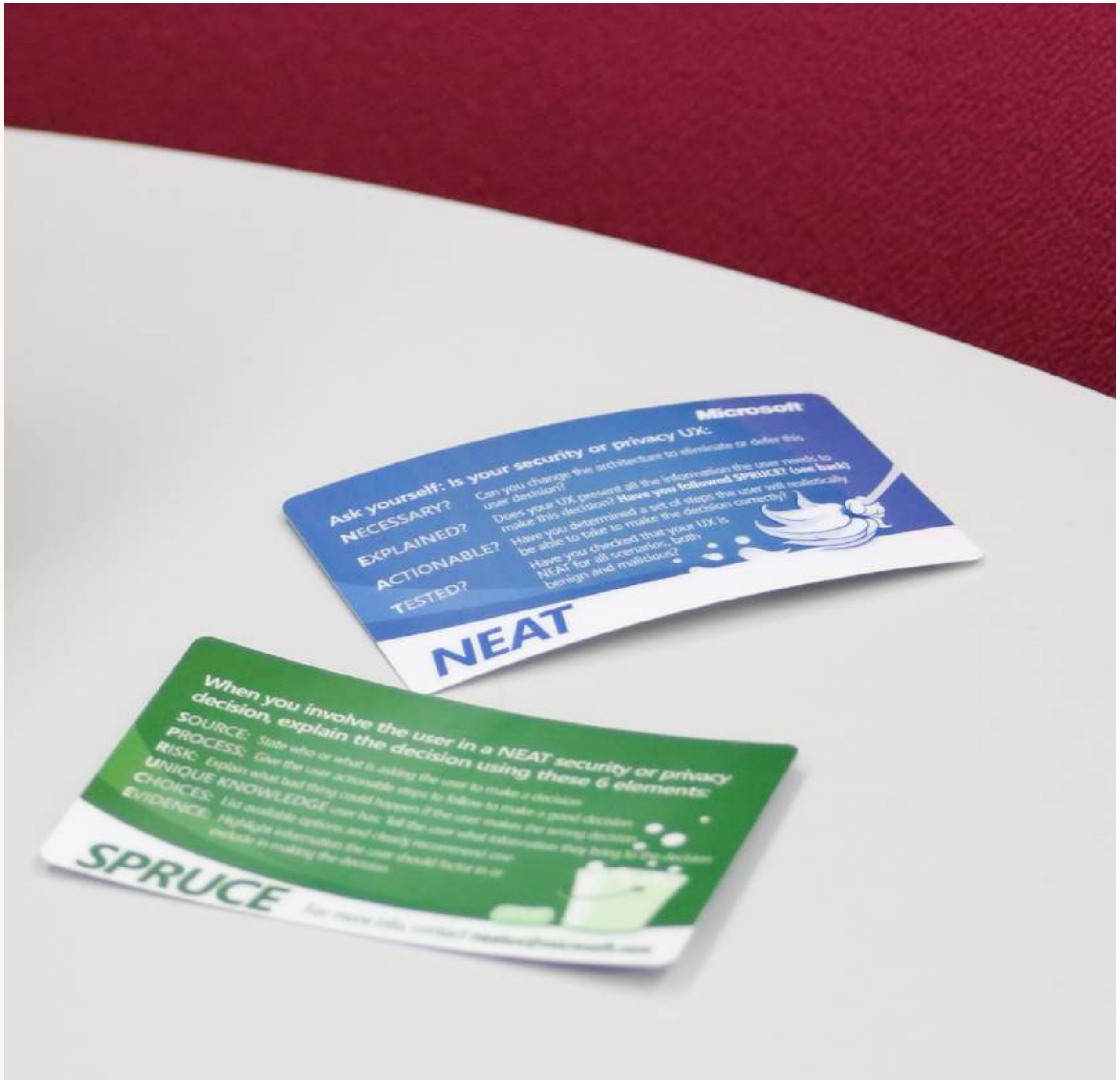
Think-pair-share

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

Further evaluating advice and warning

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*

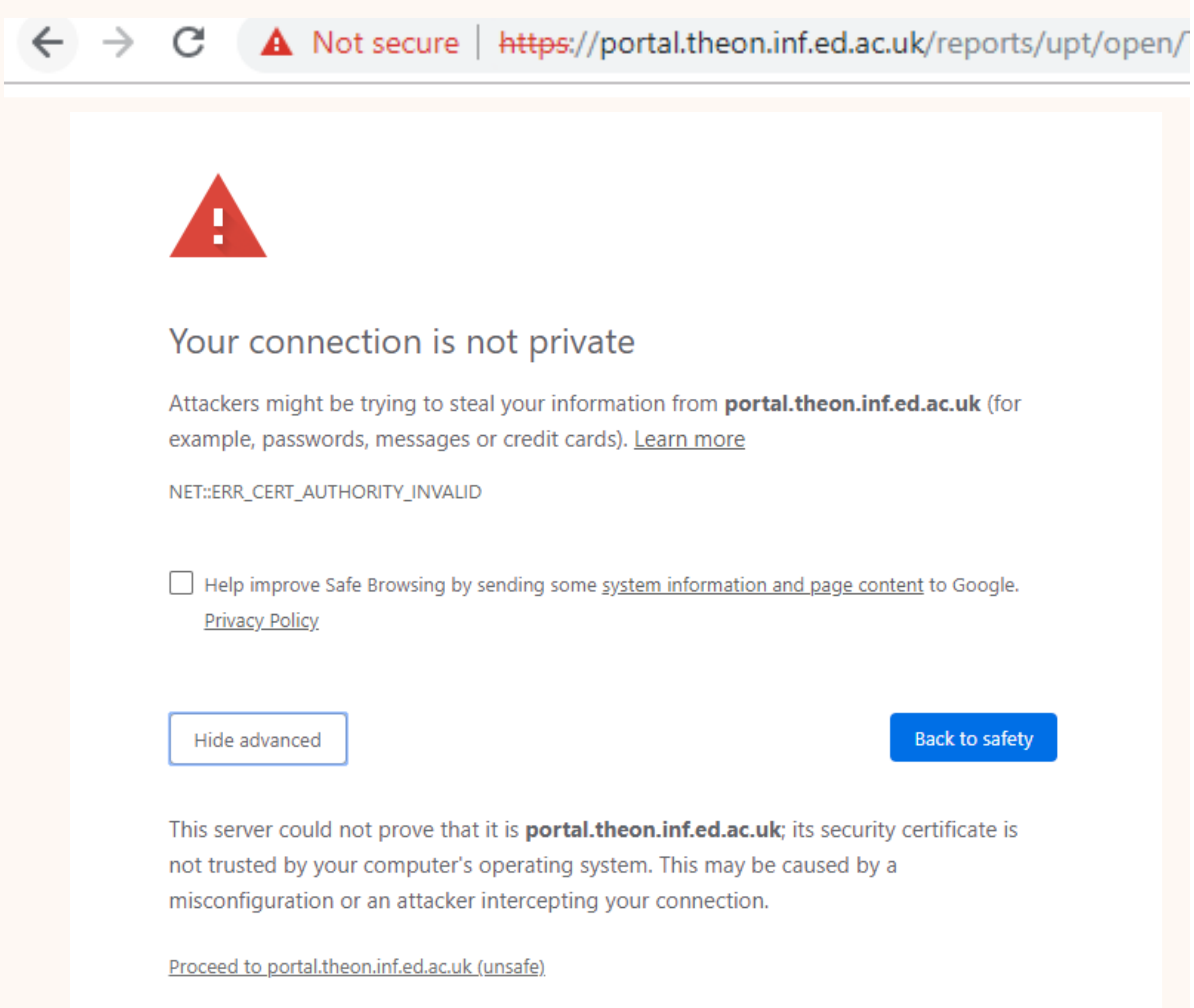
CHOICES: *List available options and clearly recommend one*

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

SPRUCE For more info, contact [illegible]

I'd like to use this example.

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



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

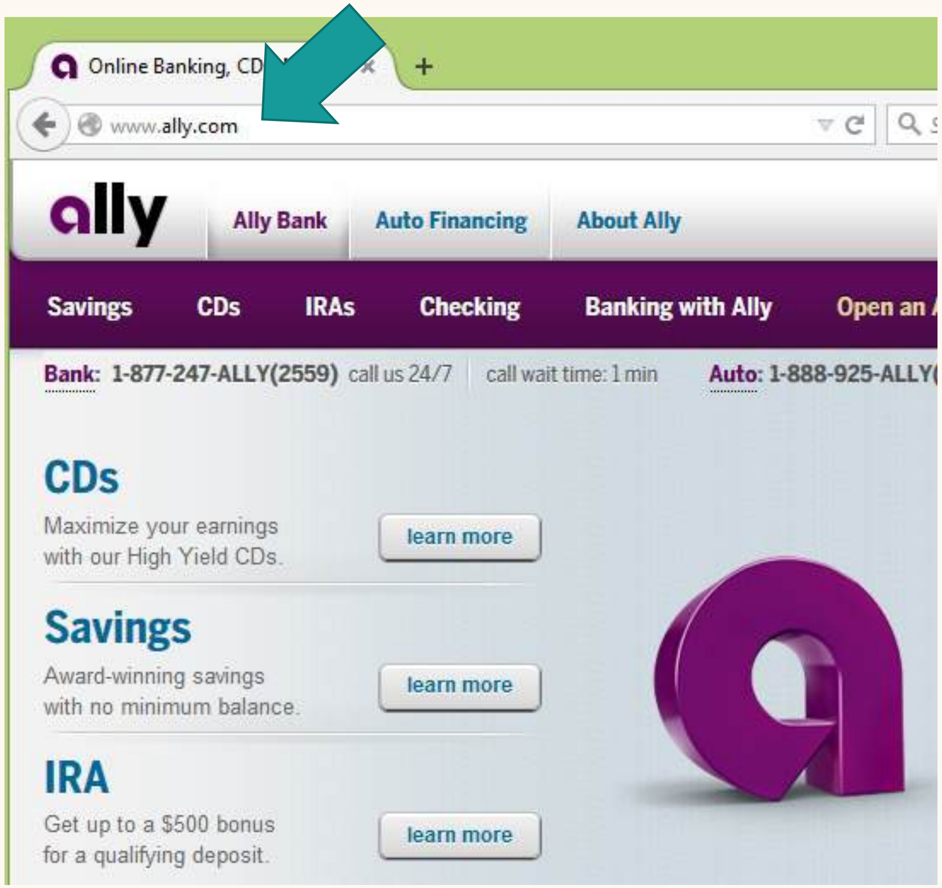
NET::ERR_CERT_AUTHORITY_INVALID

□ 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)

http versus https



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

CDs

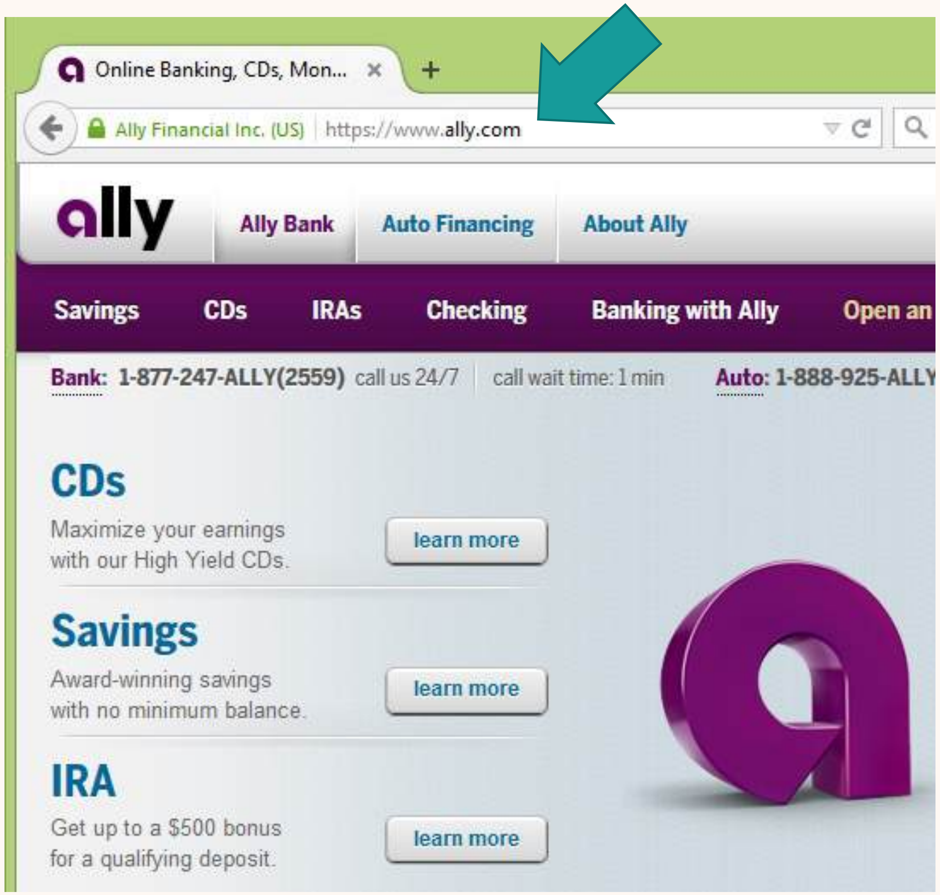
Maximize your earnings with our High Yield CDs.

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:

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

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?

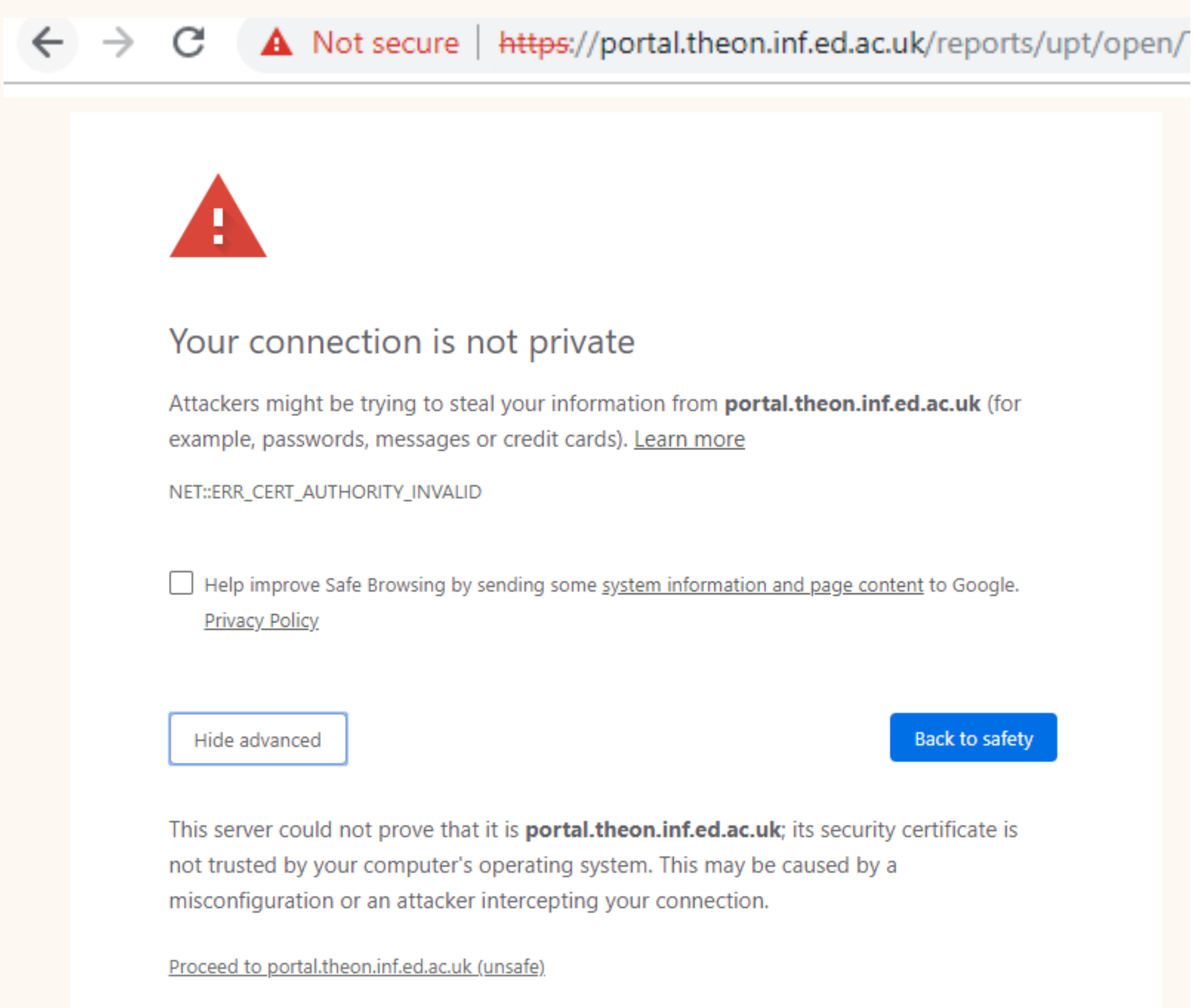
Tested – Have you checked that your user experience is NEAT for all scenarios, both benign and malicious? Have you tested it on a human who is not a member of your team?

Necessary

Explained

Actionable

Tested



~~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

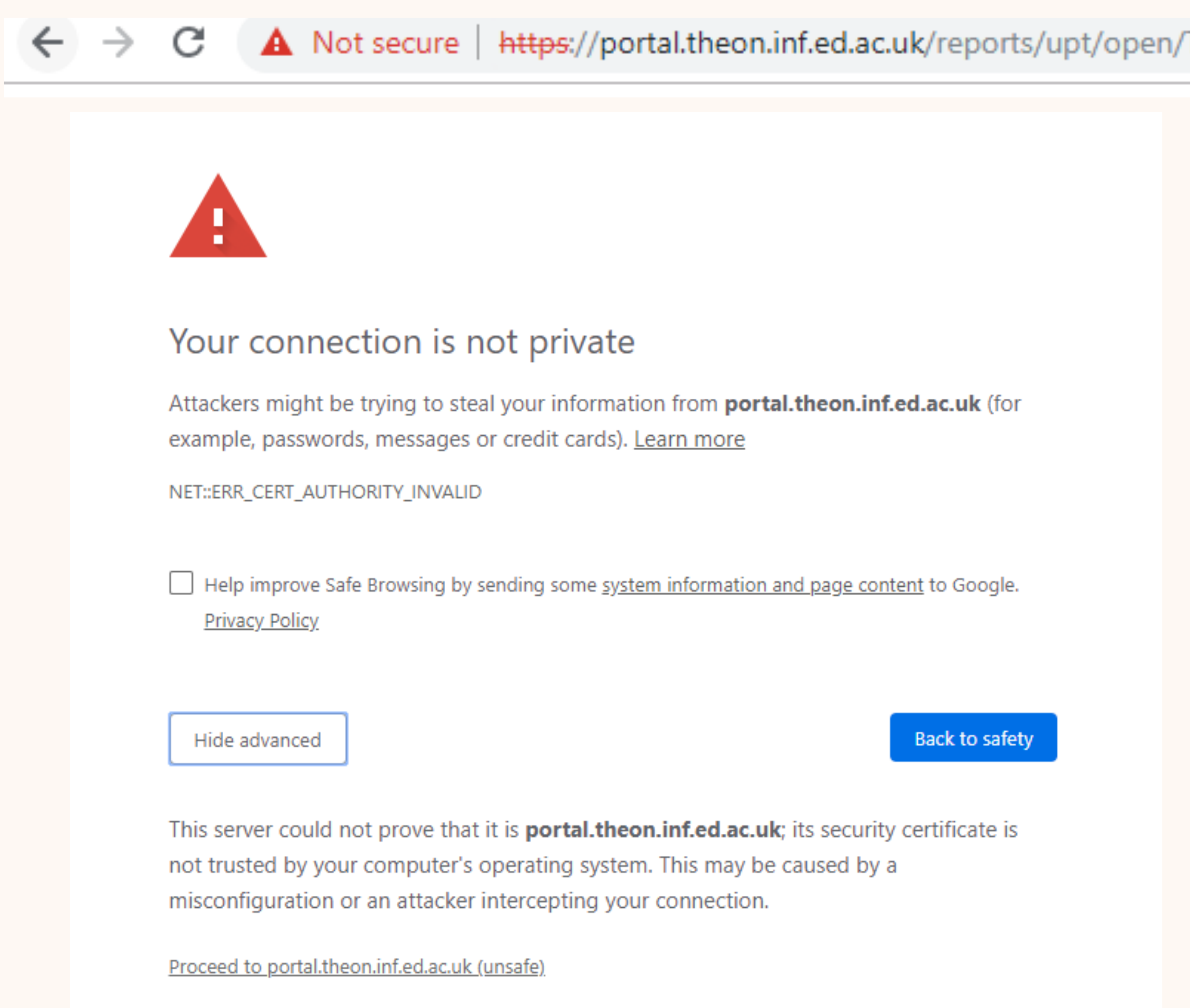
Process

Risk

Unique

Choices

Evidence



~~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

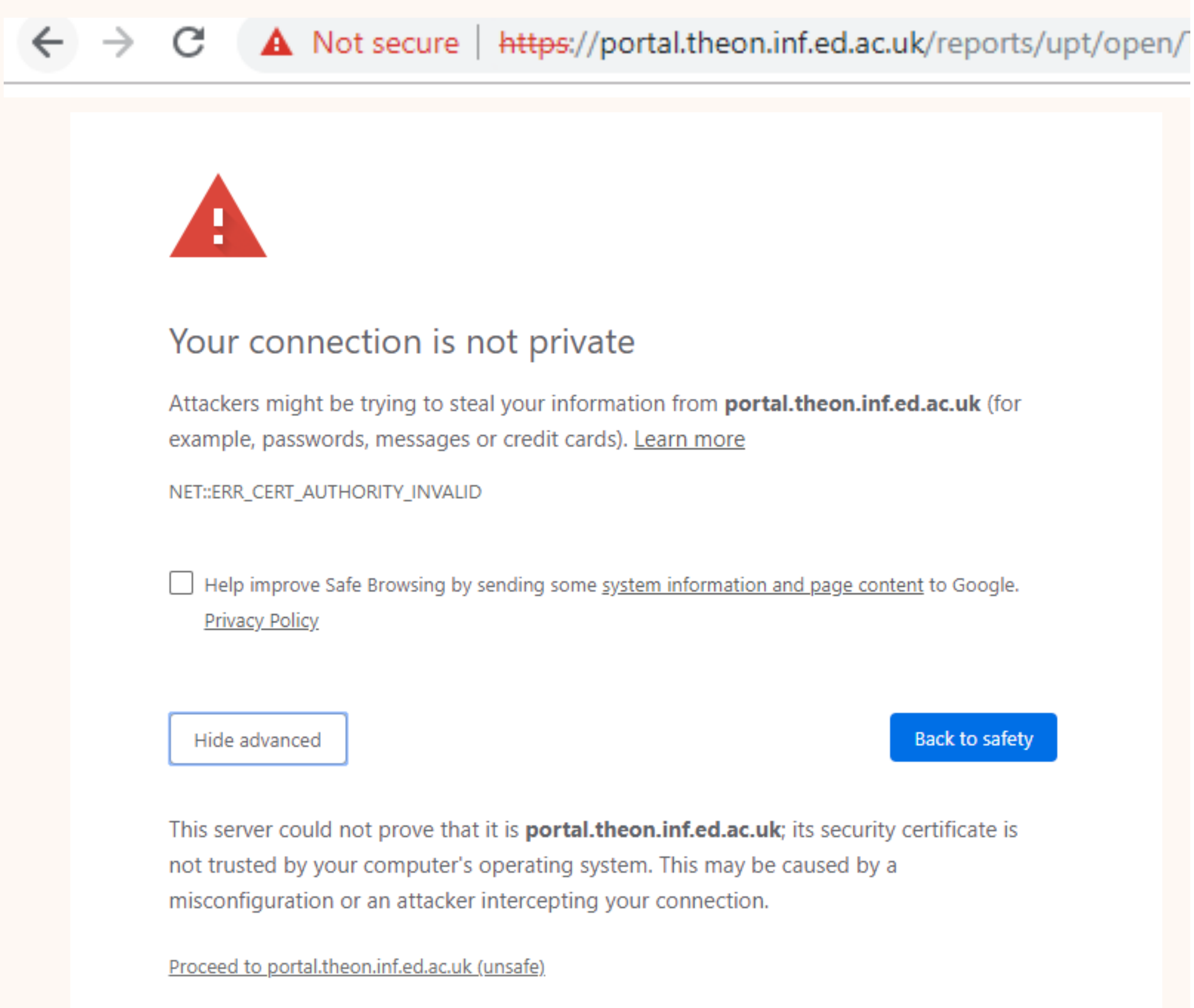
□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy Policy

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)

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.



Your connection is not private

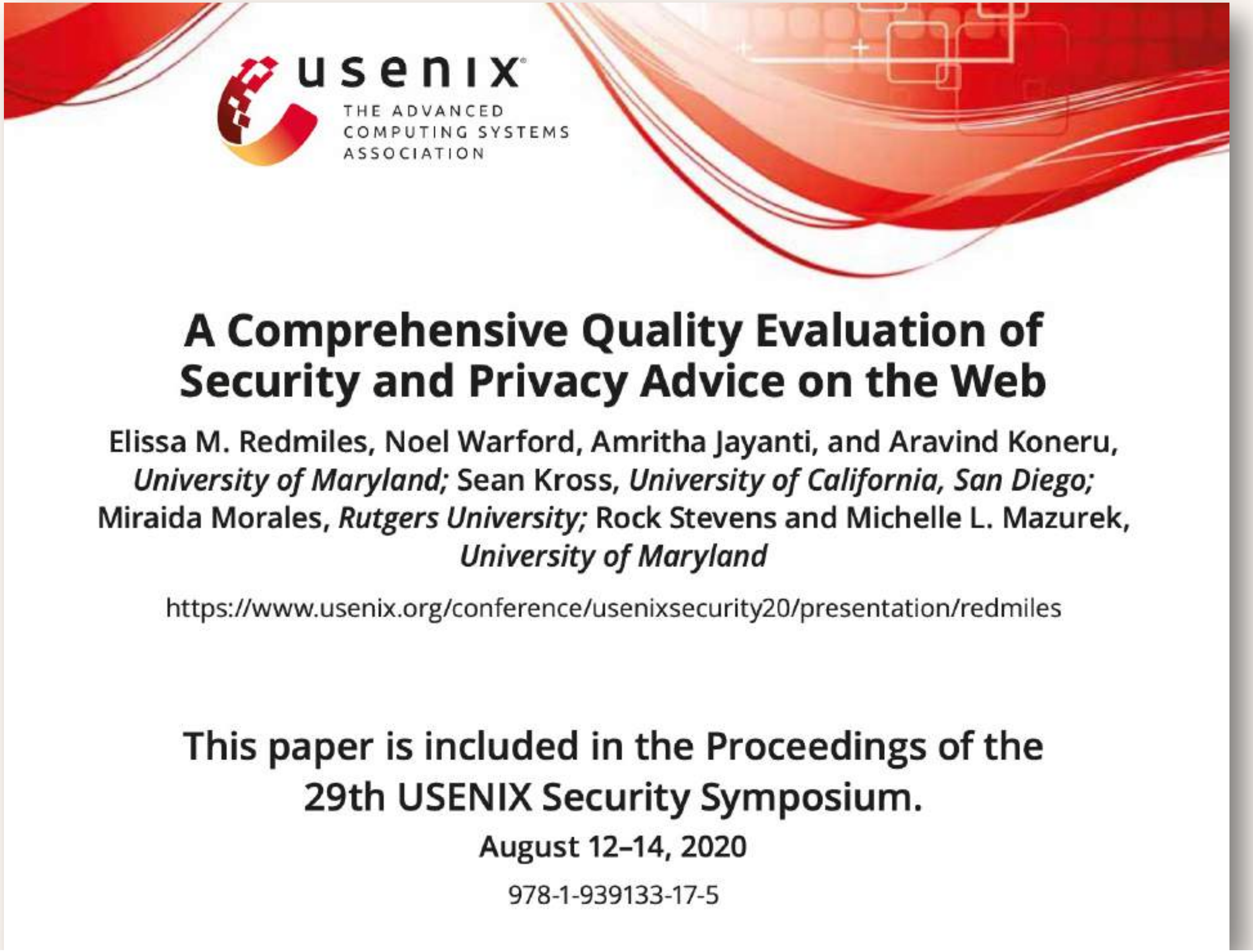
Attackers might be trying to steal your information from **portal.theon.inf.ed.ac.uk** (for example, passwords, messages or credit cards). Learn more

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)



usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

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

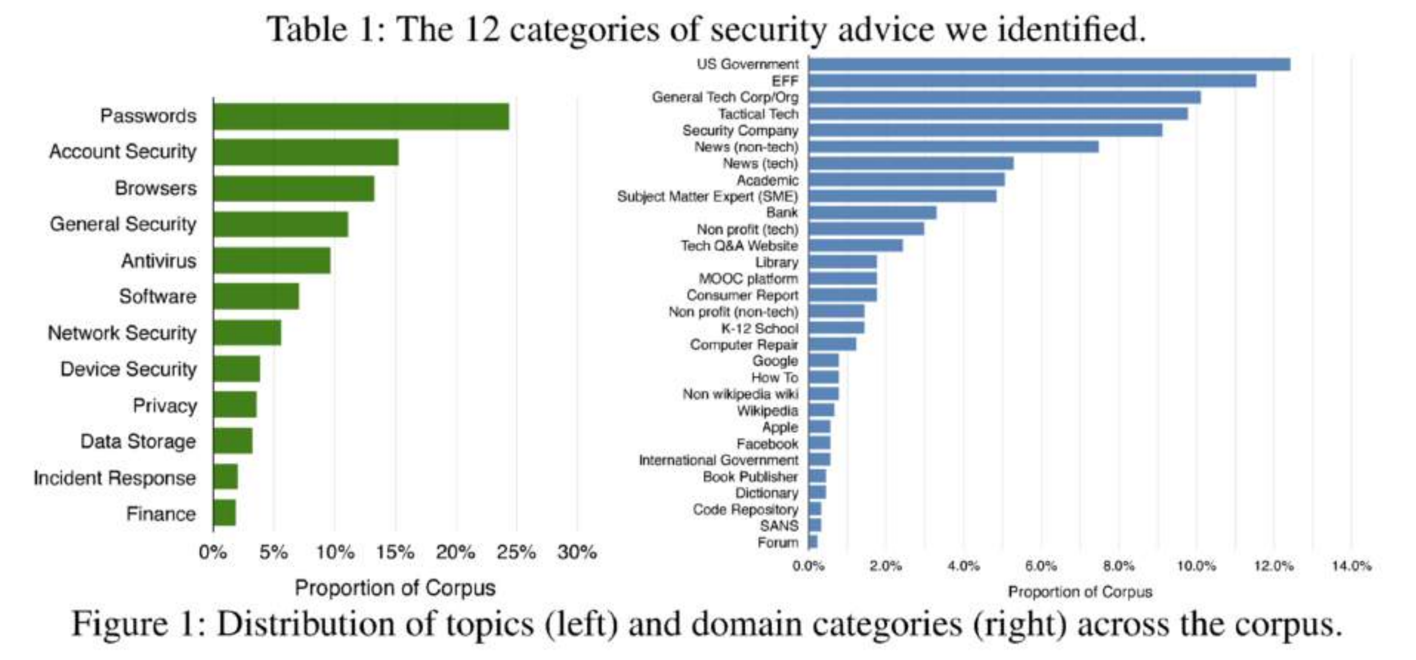


Table 1: The 12 categories of security advice we identified.

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

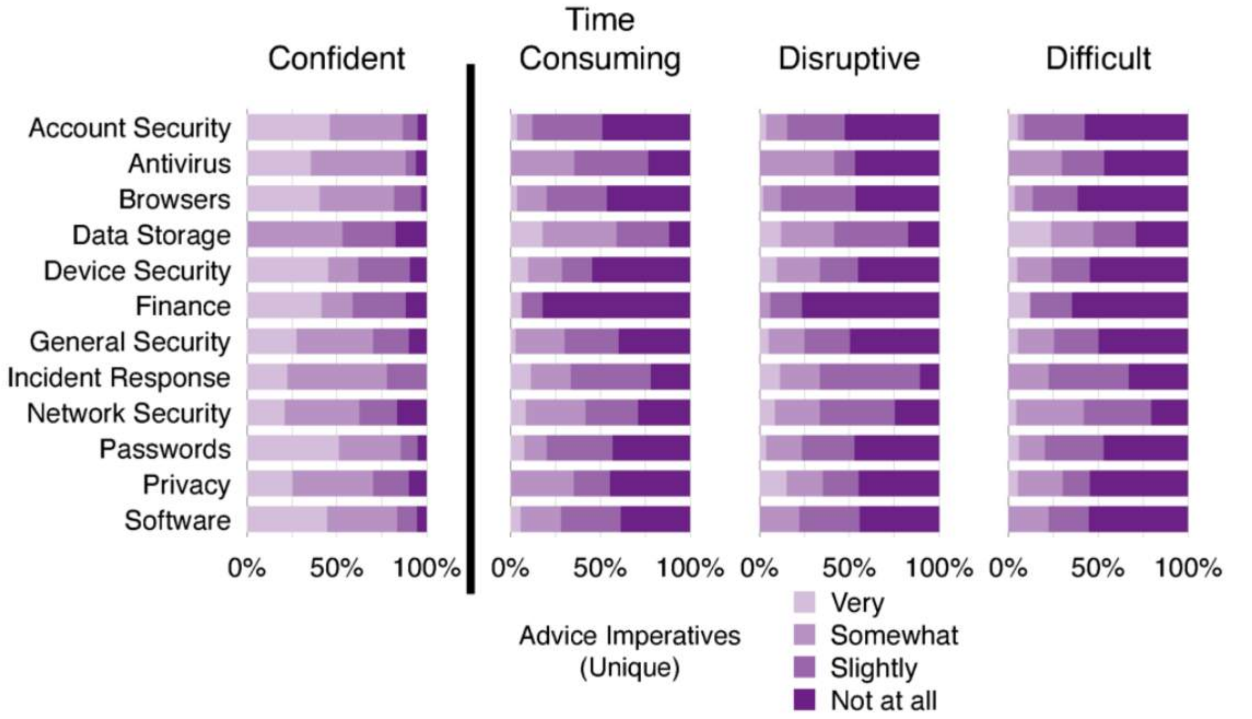
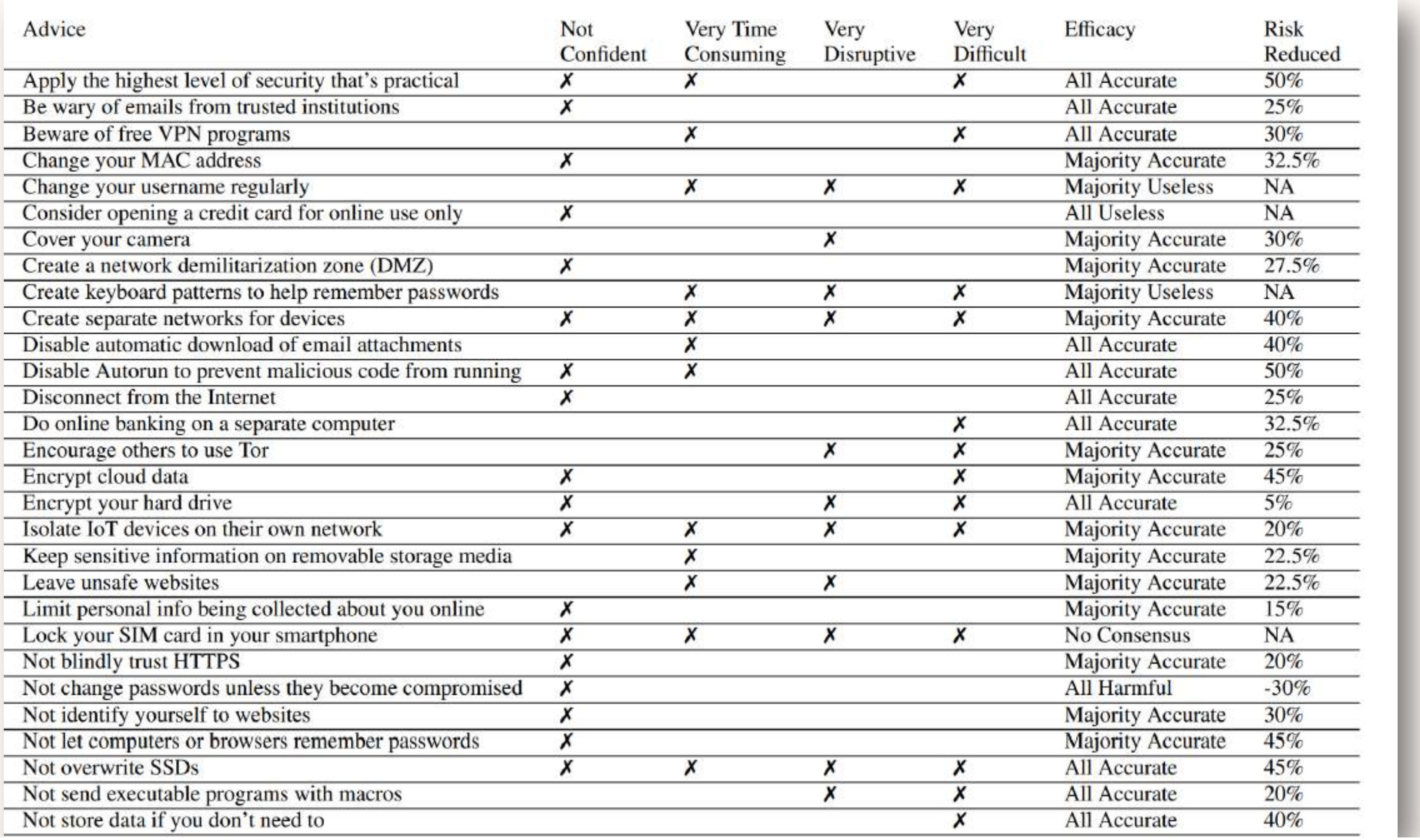


Figure 3: Advice actionability by topic across 374 unique advice imperatives.

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

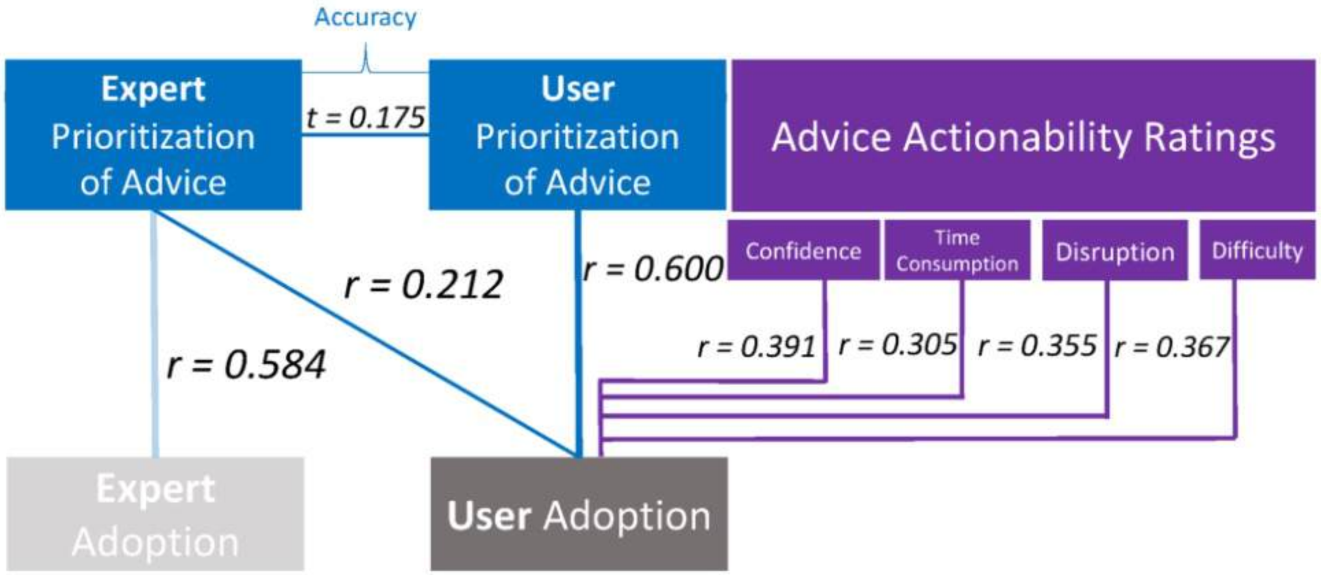


Figure 6: Correlation between security advice adoption, actionability, and priority rankings.

Questions

Take-home

- **(Blog)** Mandal, P., Ami, A.S., Olaiya, V., Razmjo, S.H. and Nadkarni, A., 2024. " Belt and suspenders" or" just red tape"?: Investigating Early Artifacts and User Perceptions of {IoT} App Security Certification. In *33rd USENIX Security Symposium (USENIX Security 24)* (pp. 4927-4944).
- **(Blog)** NCSC - Social Media: how to use it safely