Usable Security and Phishing

Dr Kami Vaniea
School of Informatics
University of Edinburgh
kvaniea@inf.ed.ac.uk
@kaniea

THE UNIVERSITY *of* EDINBURGH
informatics

From the news

Jeff Bezos hack: Amazon boss's phone 'hacked by Saudi crown prince'

Exclusive: investigation suggests Washington Post owner was targeted five months before murder of Jamal Khashoggi

- **Revealed: the Saudi heir and the alleged plot to undermine Jeff Bezos**

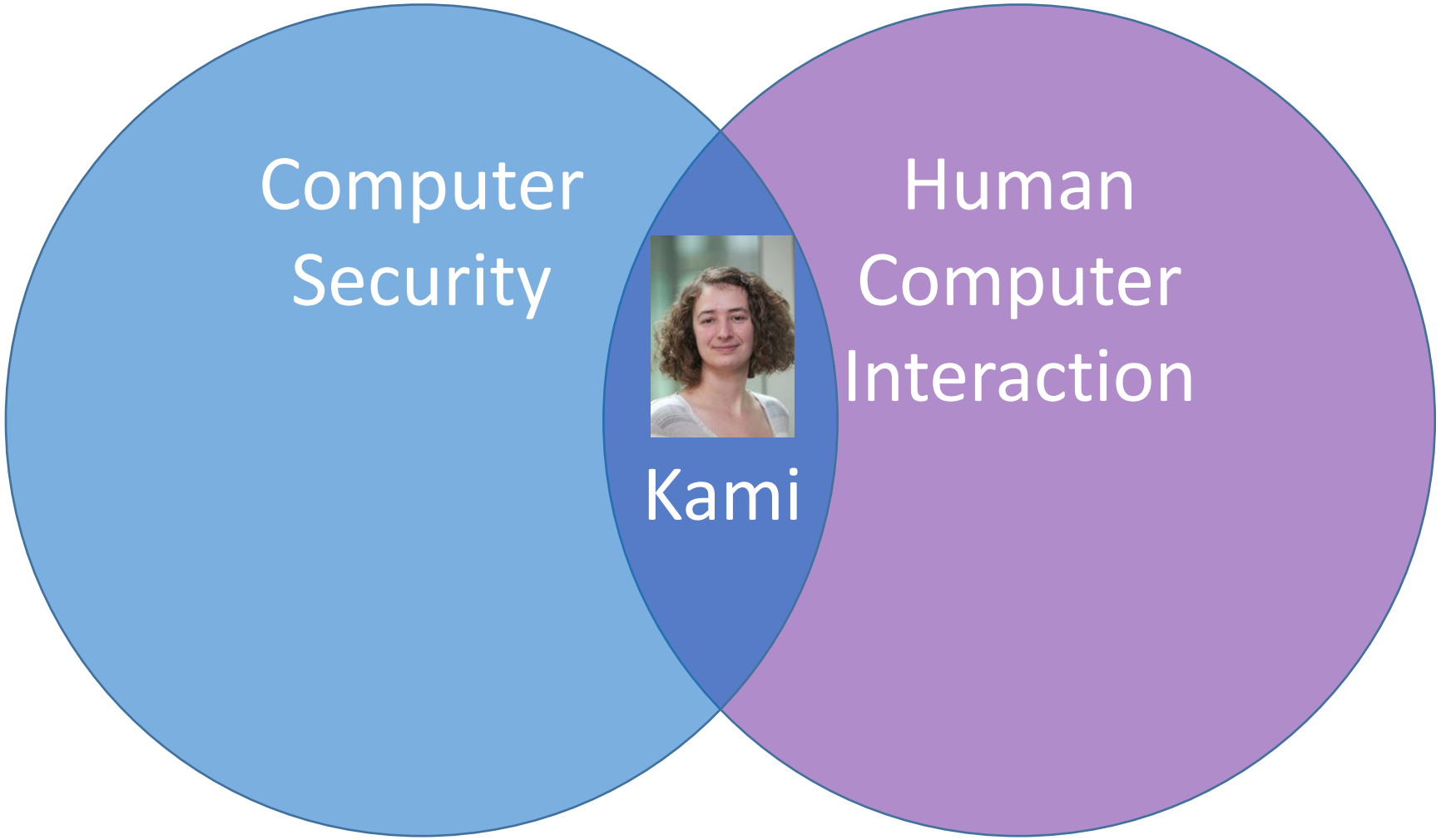
▲ Jeff Bezos, the Saudi crown prince, and the alleged phone-hacking plot – video explainer

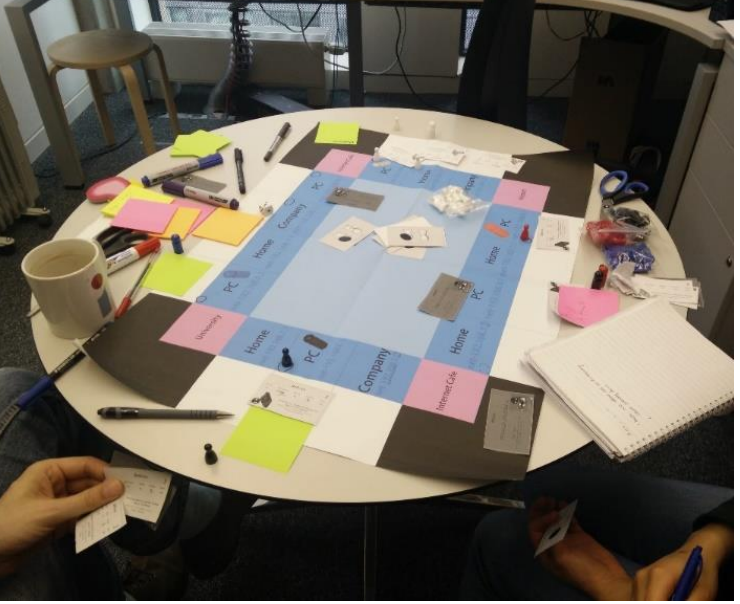
The Amazon billionaire Jeff Bezos had his mobile phone “hacked” in 2018 after receiving a WhatsApp message that had apparently been sent from the personal account of the crown prince of Saudi Arabia, sources have told the Guardian.

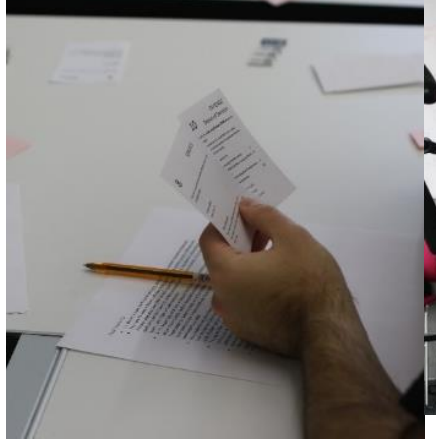
The Amazon billionaire Jeff Bezos had his mobile phone “hacked” in 2018 after receiving a WhatsApp message that had apparently been sent from the personal account of the crown prince of Saudi Arabia, sources have told the Guardian.

The encrypted message from the number used by Mohammed bin Salman is believed to have included a malicious file that infiltrated the phone of the world’s richest man, according to the results of a digital forensic analysis.

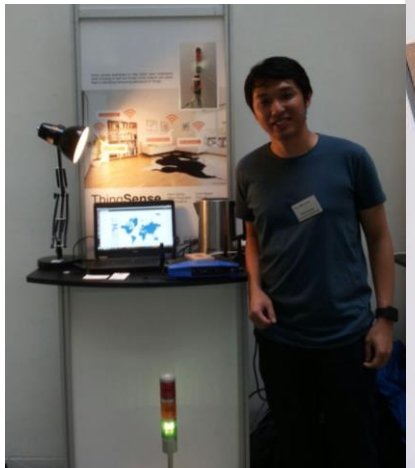
https://www.theguardian.com/technology/2020/jan/21/amazon-boss-jeff-bezoss-phone-hacked-by-saudi-crown-prince

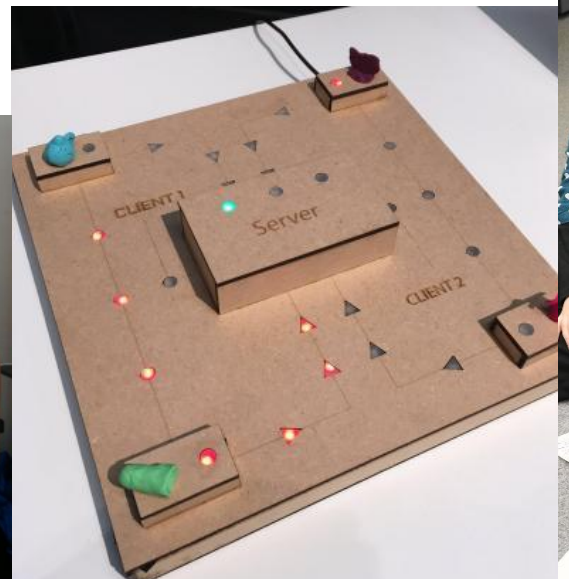

Computer Security
Human Computer Interaction
Kami





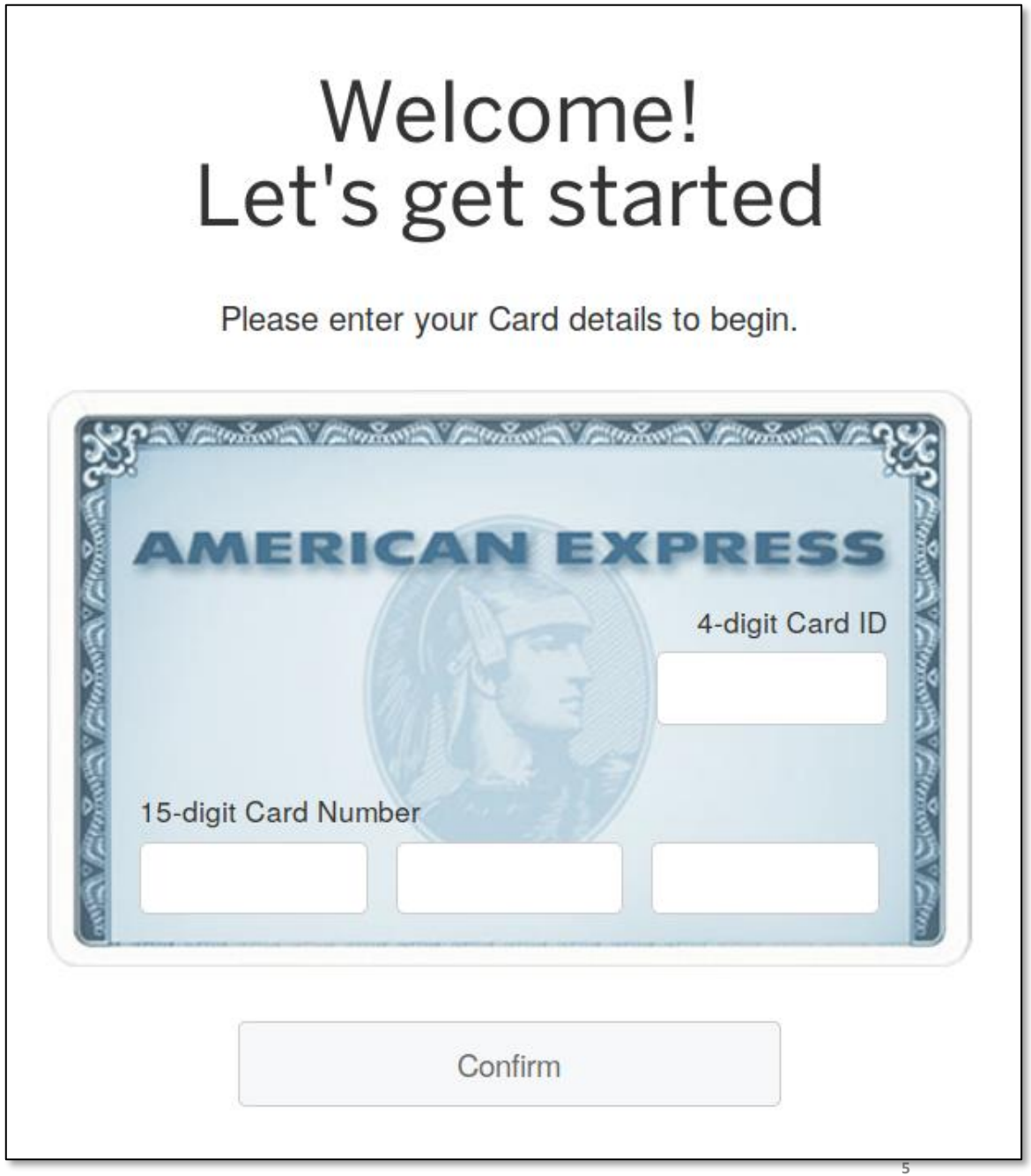
TULiPS
TECHNOLOGY USABILITY LAB
IN PRIVACY AND SECURITY

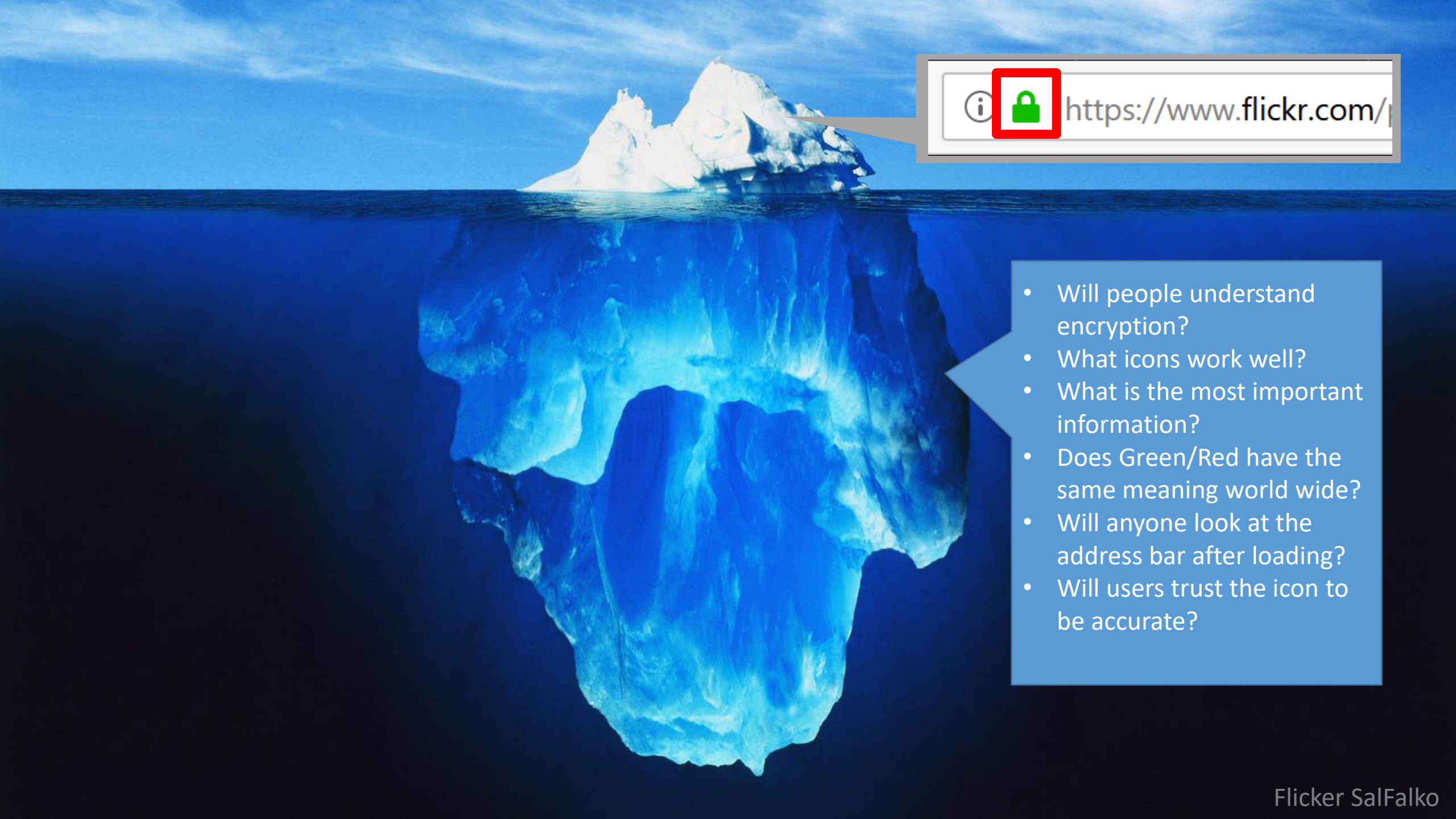




Outline

- What is “usable security”?
- An explanation of phishing
- Authentication in brief
- Passive vs active indicators



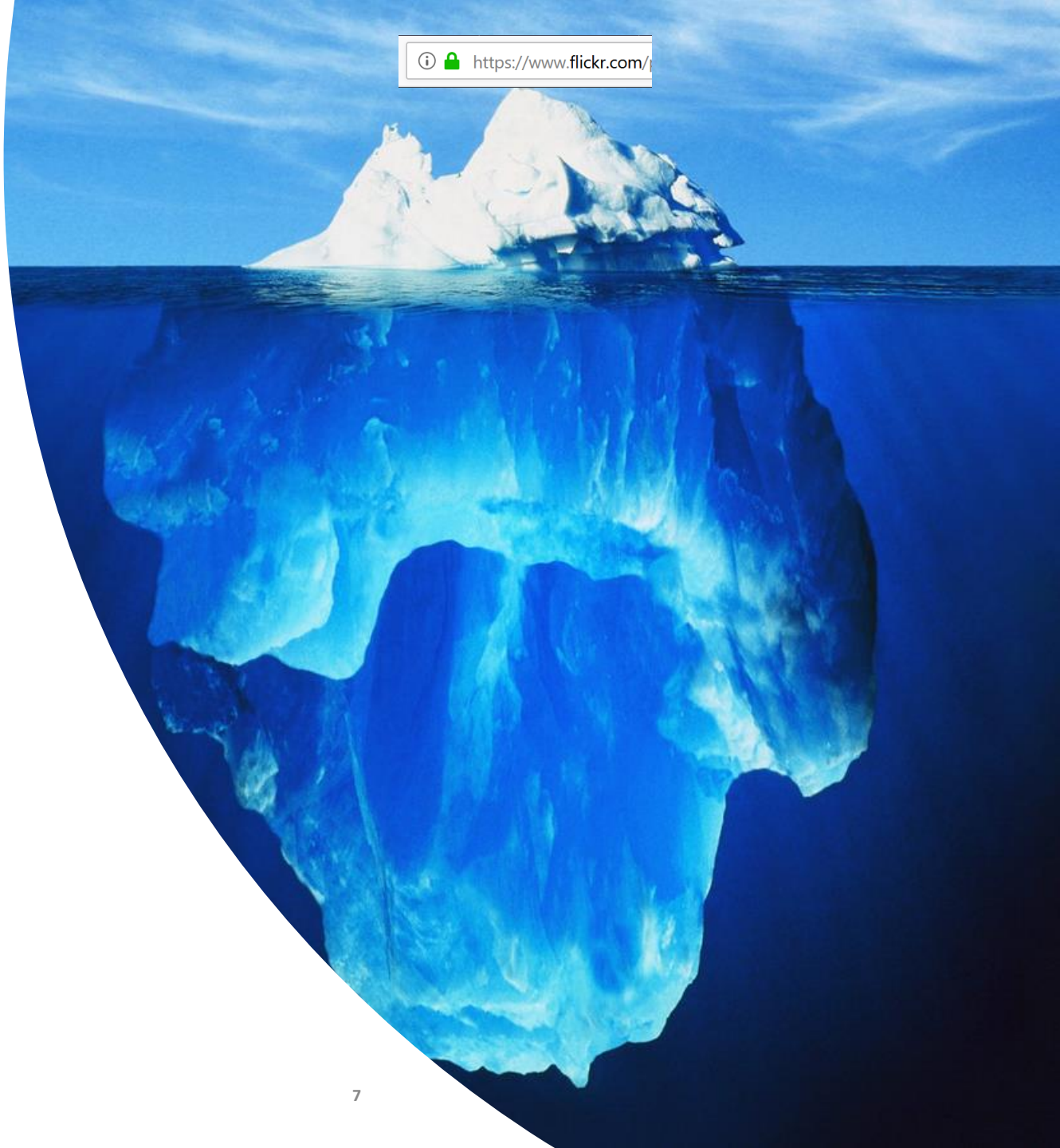


- Will people understand encryption?
- What icons work well?
- What is the most important information?
- Does Green/Red have the same meaning world wide?
- Will anyone look at the address bar after loading?
- Will users trust the icon to be accurate?

Flicker SalFalko

Usable security is challenging because:

- Users are unmotivated to care about security over their current task.
- Complex configurations make sense to computer scientists but not to end users.
- Good feedback/advice is very hard to give to users.
- Barn door – once security or privacy is lost, its gone. There is no undo.

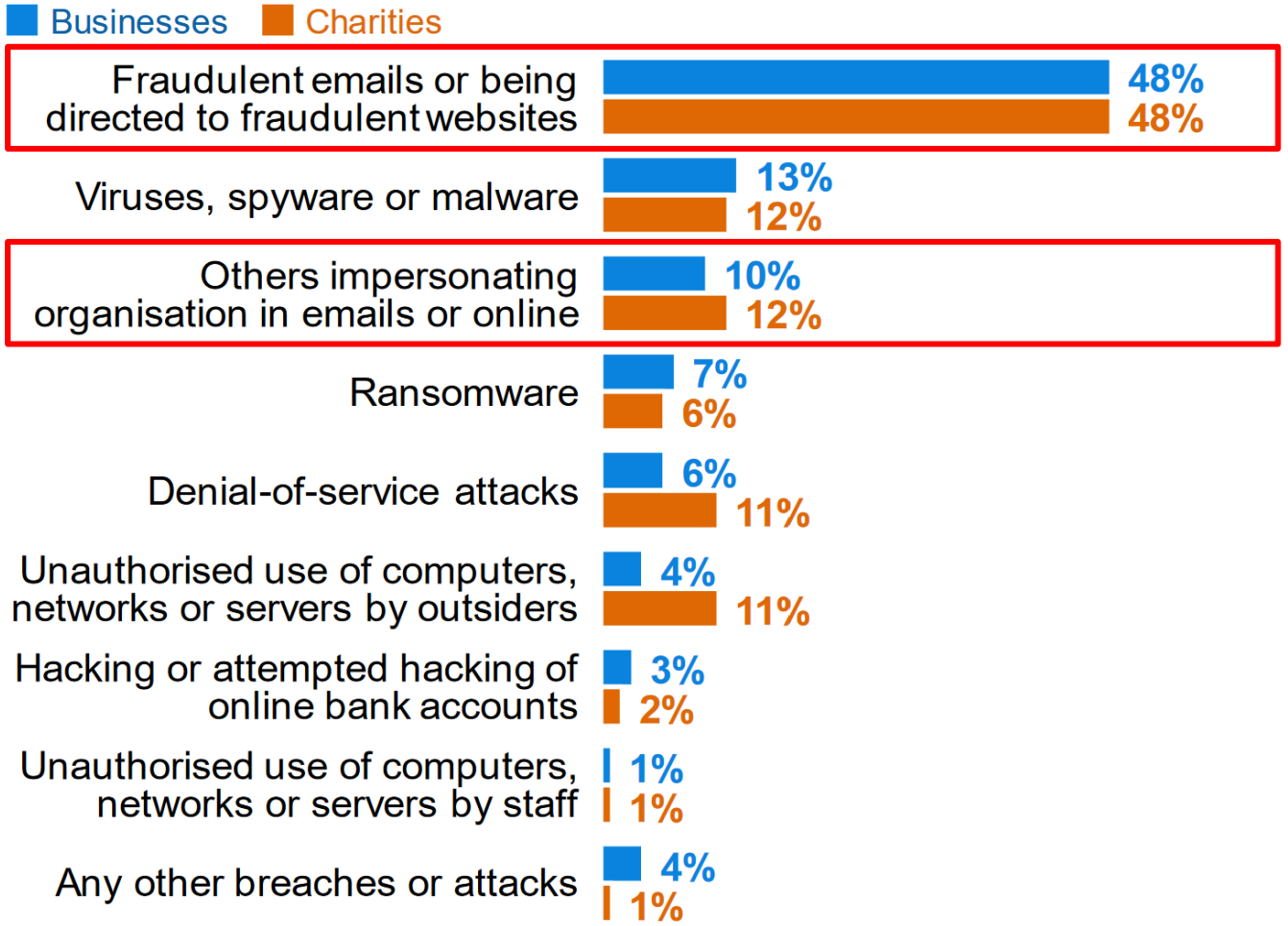


Phishing

Phishing is very common and very disruptive to UK businesses

Also, it really annoys those of us who are just trying to get our work done.

Q. What was the one cyber security breach, or related series of breaches or attacks, that caused the most disruption to your organisation in the last 12 months?



Bases: 778 businesses that identified a breach or attack in the last 12 months; 218 charities

HMG Department for Digital, Culture, Media & Sport. Cyber Security Breaches Survey 2019. July 2019.

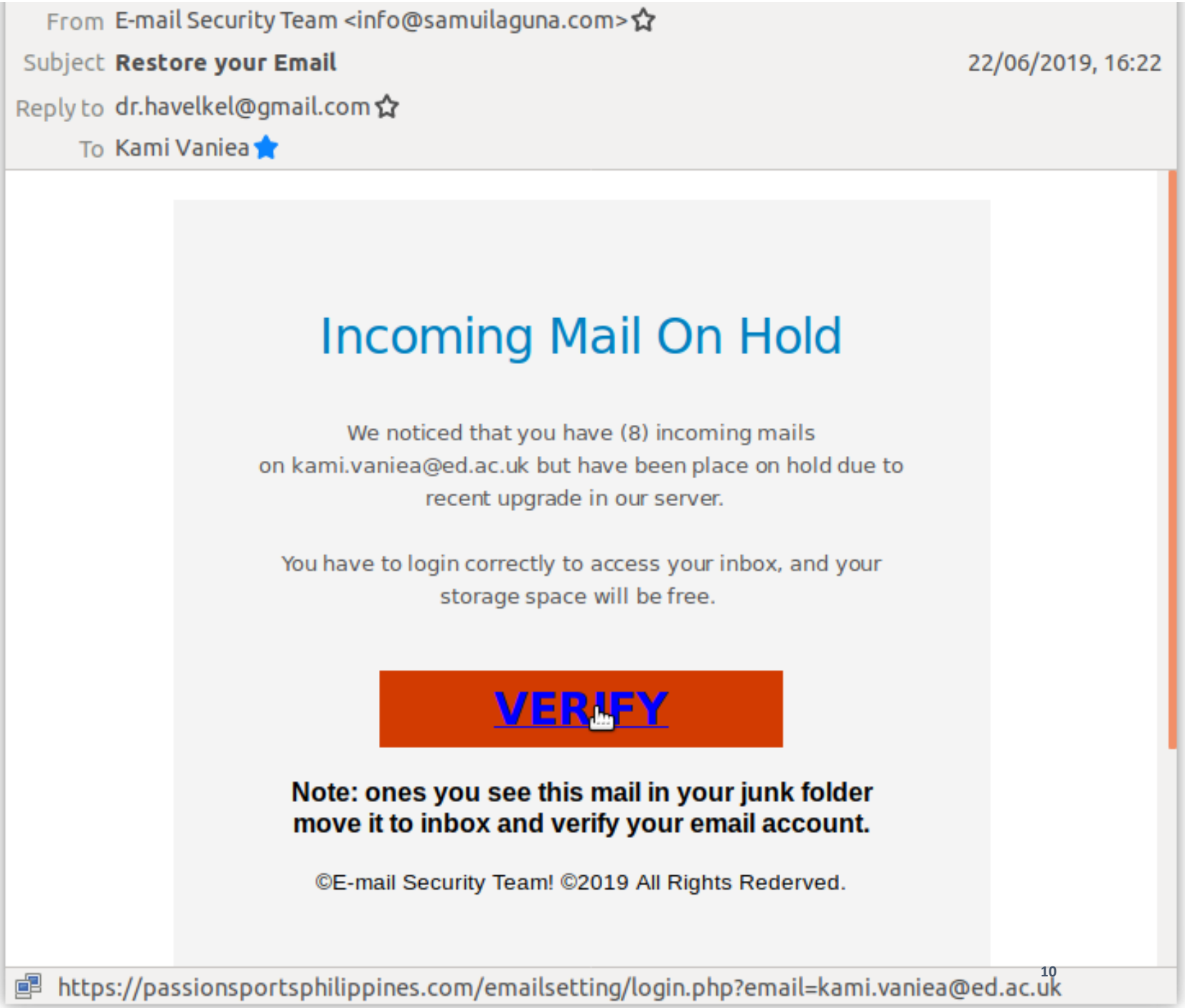
This is a phishing email

Look real

- Fear appeal – blocked email ☹
- Realistic event
- (Mostly) well formatted

But

- Wrong URL
- Wrong From



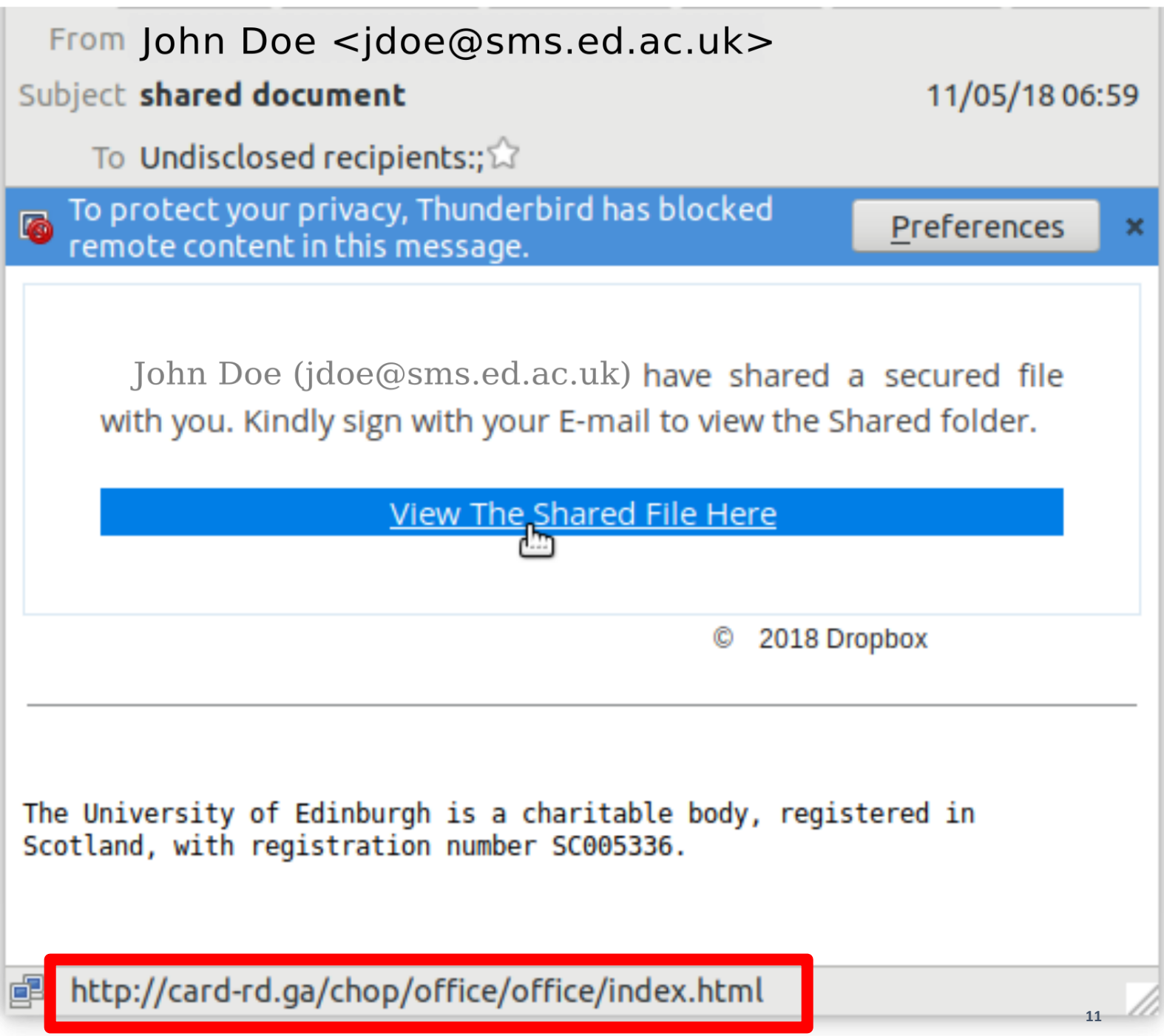
This is a phishing email

Look real

- Realistic event
- Real student
- Visually identical to real email

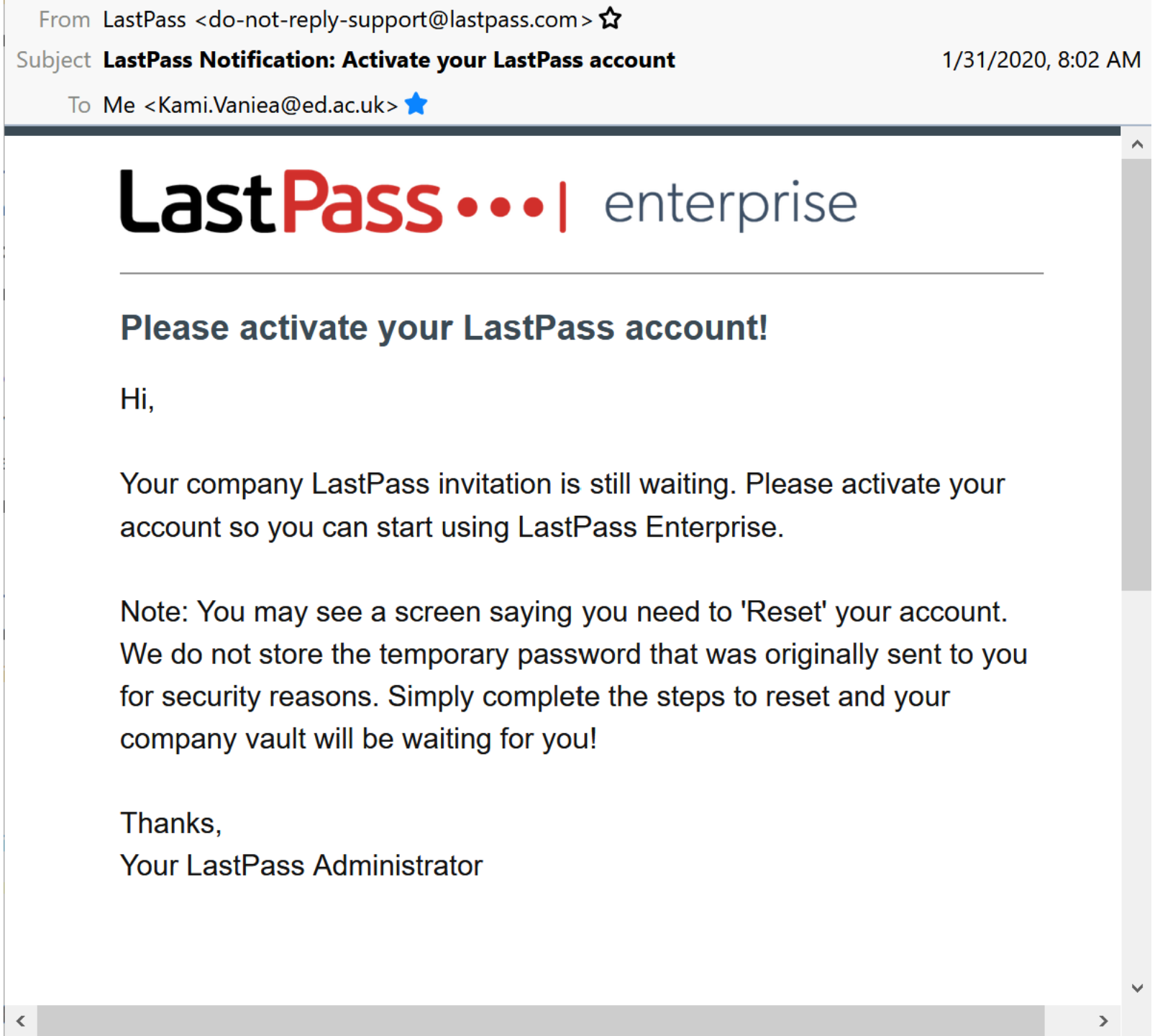
But

- Wrong URL



This is not a phishing email

- Asking user to “reset” a password for company account
- Appeal to authority branding
- No use of my first name



From LastPass <do-not-reply-support@lastpass.com>

Subject **LastPass Notification: Activate your LastPass account** 1/31/2020, 8:02 AM

To Me <Kami.Vaniea@ed.ac.uk>

LastPass ••• | enterprise

Please activate your LastPass account!

Hi,

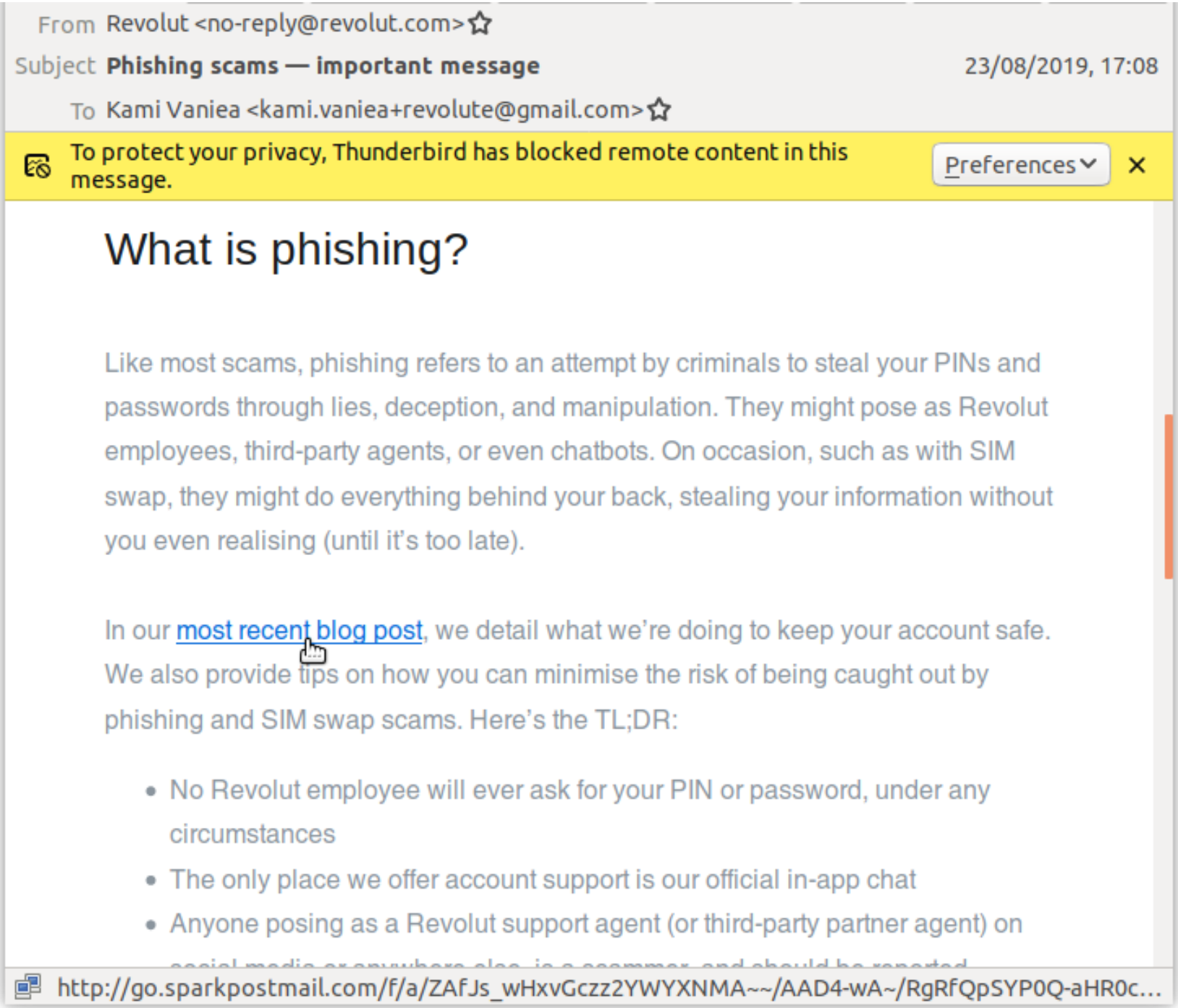
Your company LastPass invitation is still waiting. Please activate your account so you can start using LastPass Enterprise.

Note: You may see a screen saying you need to 'Reset' your account. We do not store the temporary password that was originally sent to you for security reasons. Simply complete the steps to reset and your company vault will be waiting for you!

Thanks,
Your LastPass Administrator

This is not a phishing email

- Wrong URL (sparkpostmail.com)
- Asks user to click links
- Contains a GUID (privacy issue)
- Gets flagged for remote content by Thunderbird



WHAT ARE THE MOST 'SUCCESSFUL' PHISHING CAMPAIGNS?

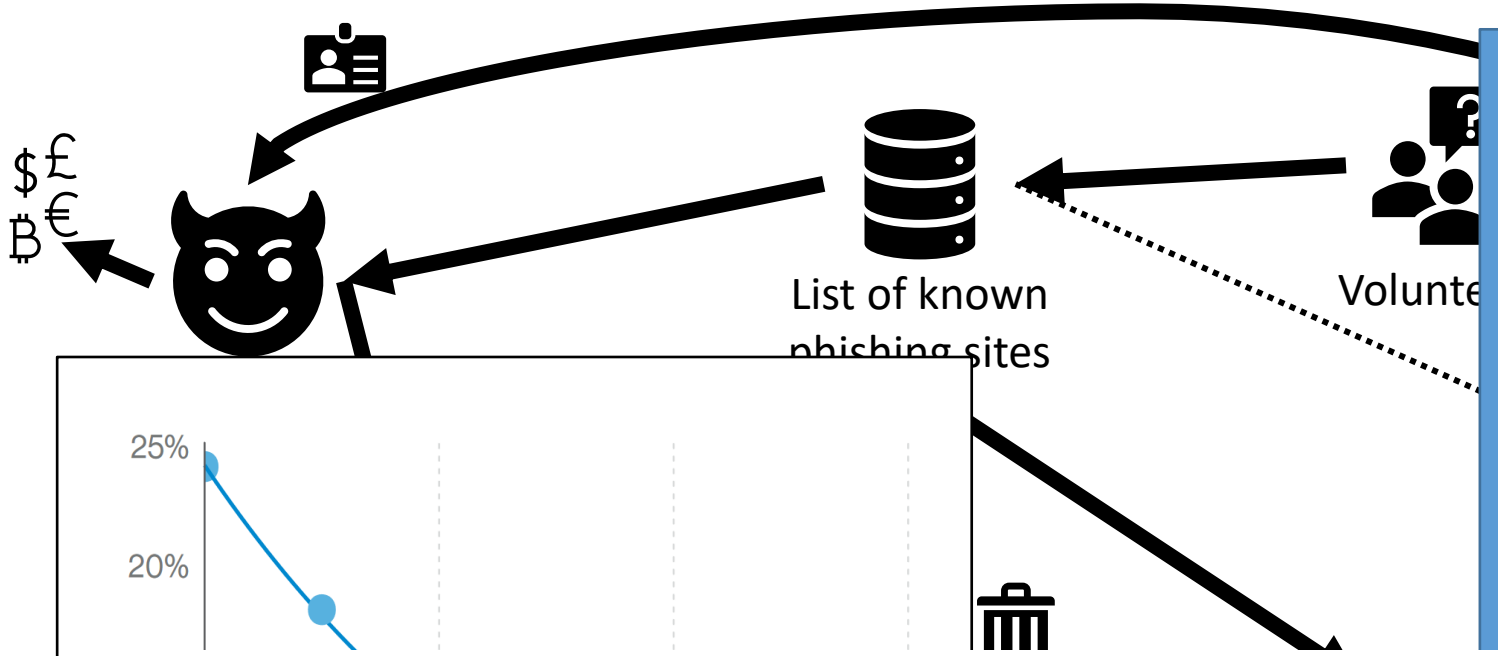
As we all know, some phishing tests are trickier than others. Here are some of the subject lines that **garnered the highest failure rates** among end users for campaigns that were sent to a minimum of 1,500 recipients:

- Toll Violation Notification
- [EXTERNAL]: Your Unclaimed Property
- Updated Building Evacuation Plan (also among the highest failure rates in 2017)
- Invoice Payment Required
- February 2018 – Updated Org Chart
- Urgent Attention (a notification requesting an email password change)

Proofpoint. State of the Phish 2019 Report. http://proofpoint.com/security-awareness

IT professionals can be very bad at writing high-quality communications….

Phishing ecosystem



17%

Of phishing campaigns are reported at all.

Verizon. 2018 Data Breach Investigation Report. P13.

	April	May	June
Number of unique phishing Web sites detected	59,756	61,820	60,889
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	37,054	40,177	34,932
Number of brands targeted by phishing campaigns	341	308	289

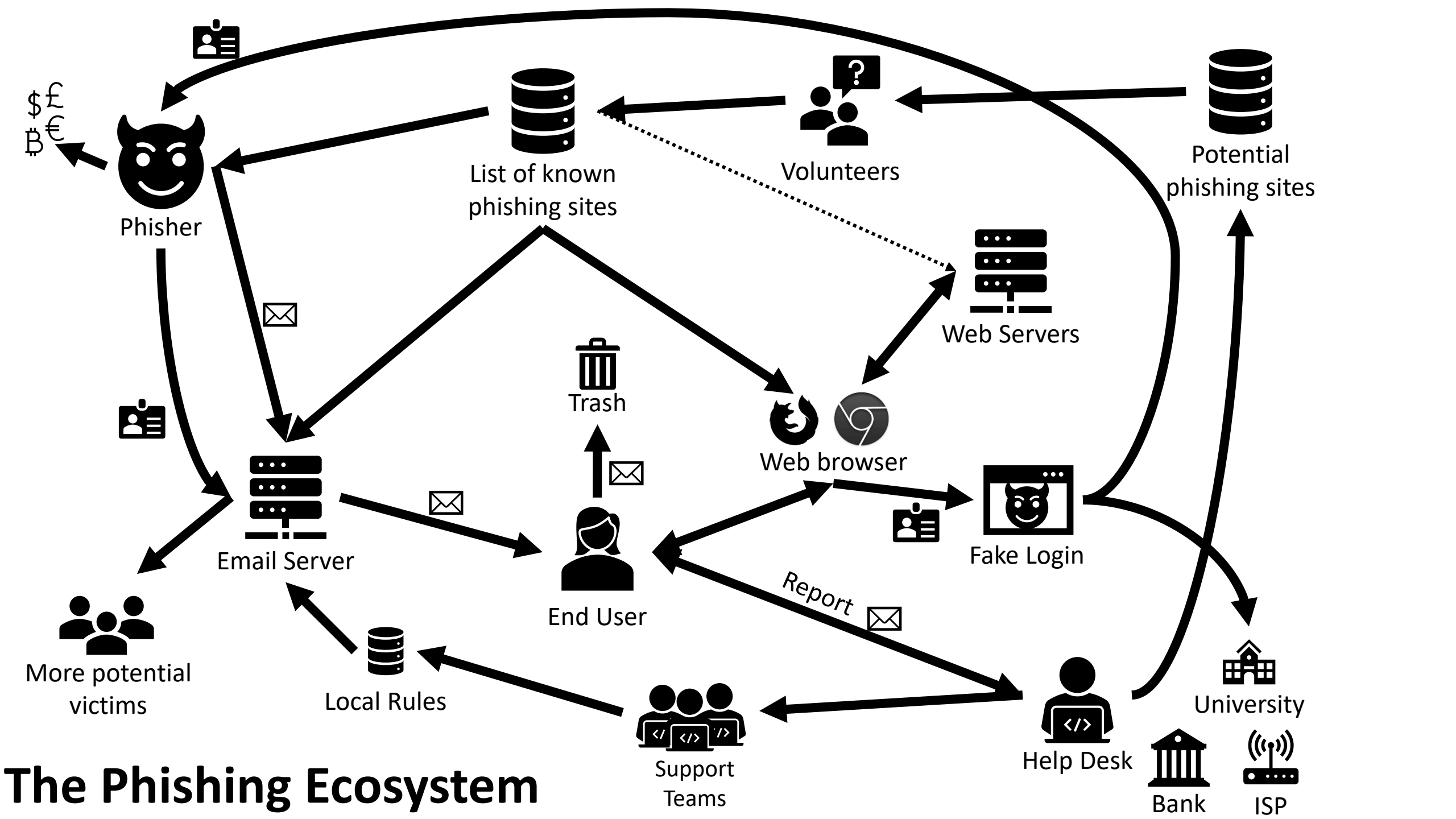
APWG. Phishing Activity Trends Report, 2nd Quarter 2019.

Report. p16

Verizon. 2019 Data Breach Investigation Report. P32.

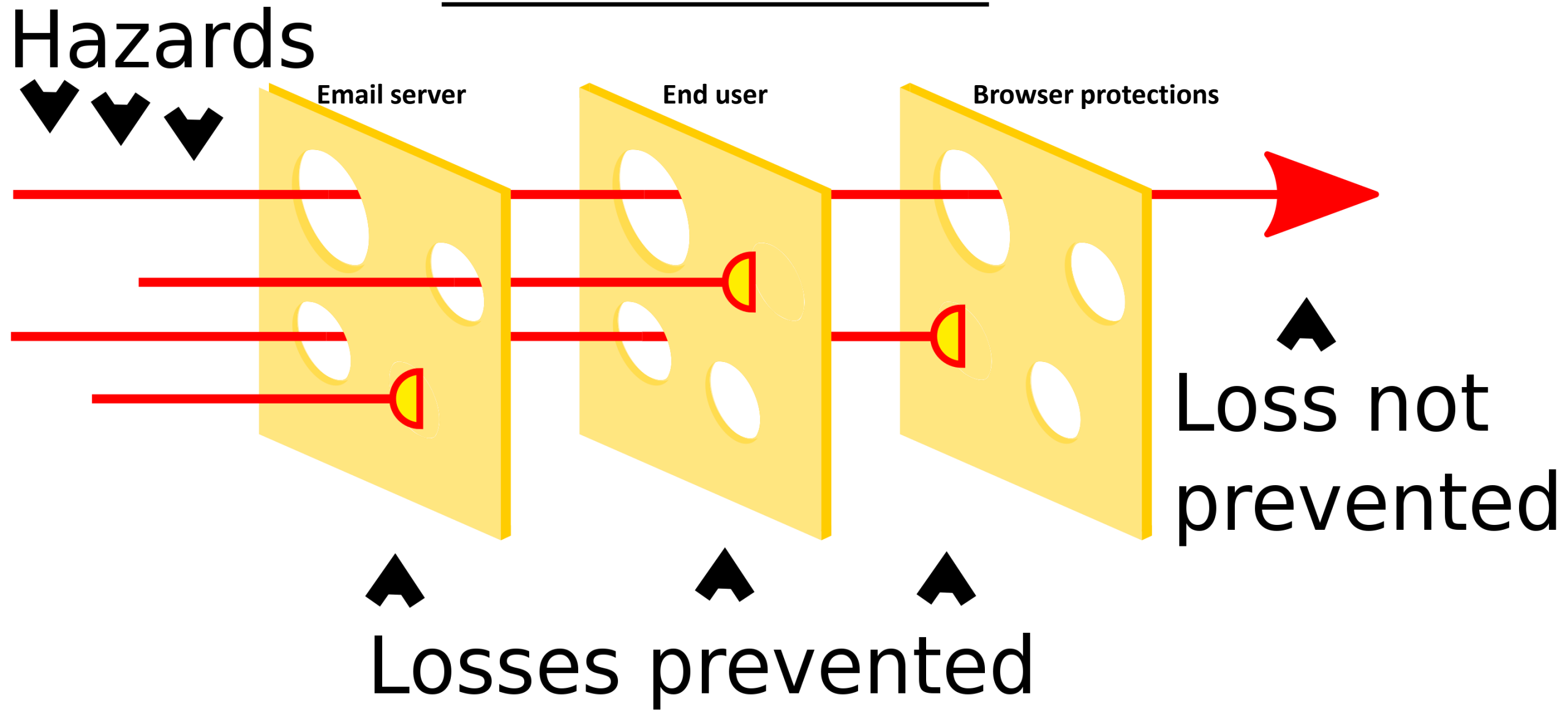
Bank ISP

The Phishing Ecosystem



The Phishing Ecosystem

Swiss Cheese Model



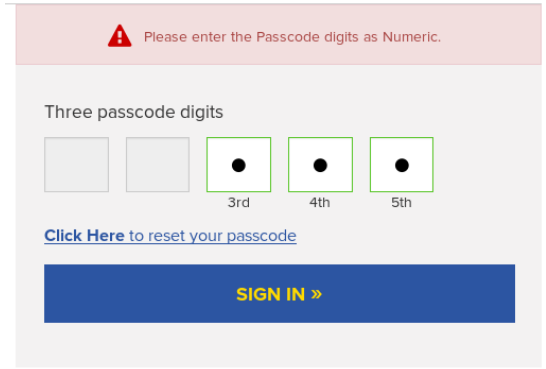
By BenAveling - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=91881875

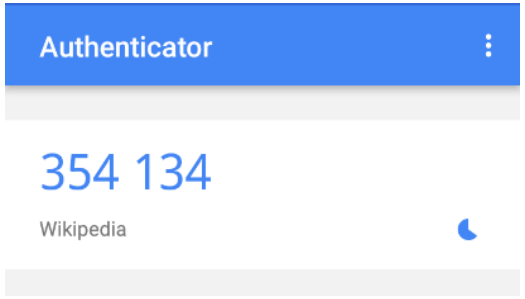
Main “solutions”

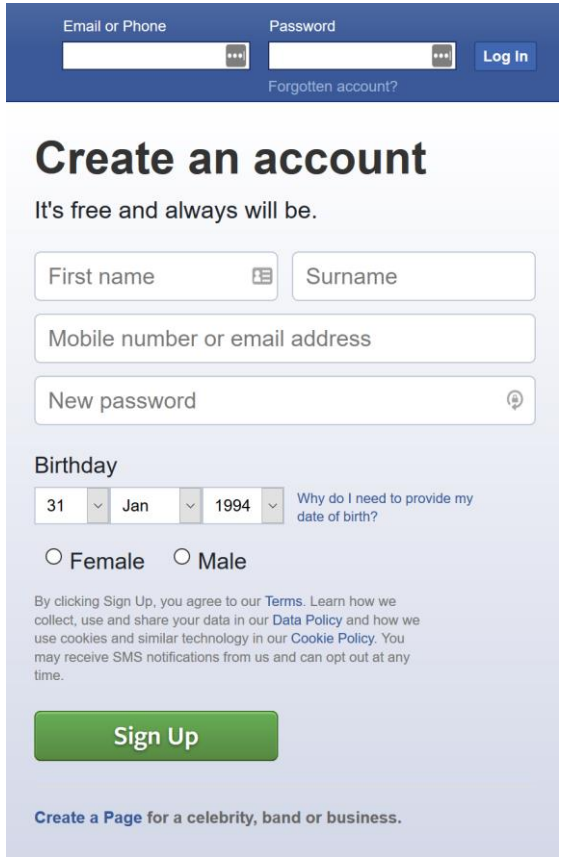
- Automatically block attacks using filters
  - Stop email from even arriving in inboxes
  - Block people from visiting known bad websites
- Train users
  - Provide users with training on how to identify phishing attacks
- Support users
  - Show UI indicators to help users tell the difference between real and fake sites
    - Also known as “passive indicators”, like the lock icon
  - Provide feedback when phishing is reported or blocked
- Improve protection of authentication credentials
  - Make it harder to impossible for a user to give away credentials
  - Limit the damage of credential sharing to one transaction
  - Let users authenticate websites

Why does phishing work?
Authentication is very broken

Authentication is how Entity A proves their identity to Entity B.





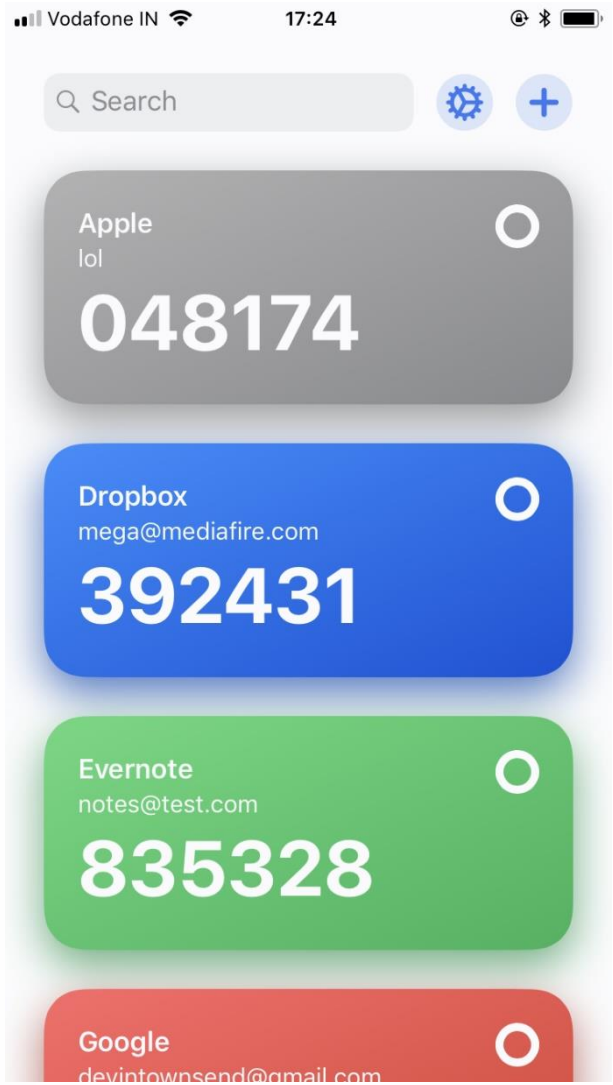


Authentication

Other features than identity can be authenticated

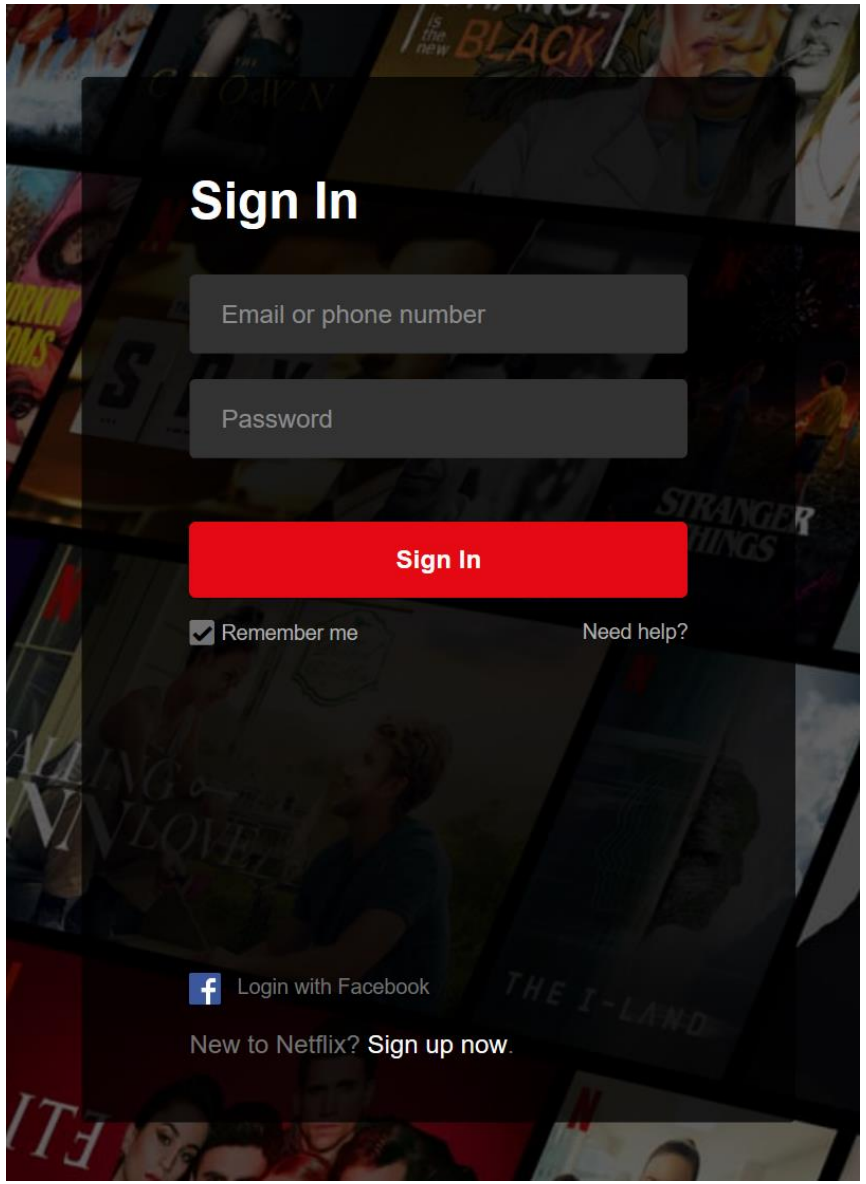
Have paid for a ticket to the show.

Age, binary of over or under 18 years old.

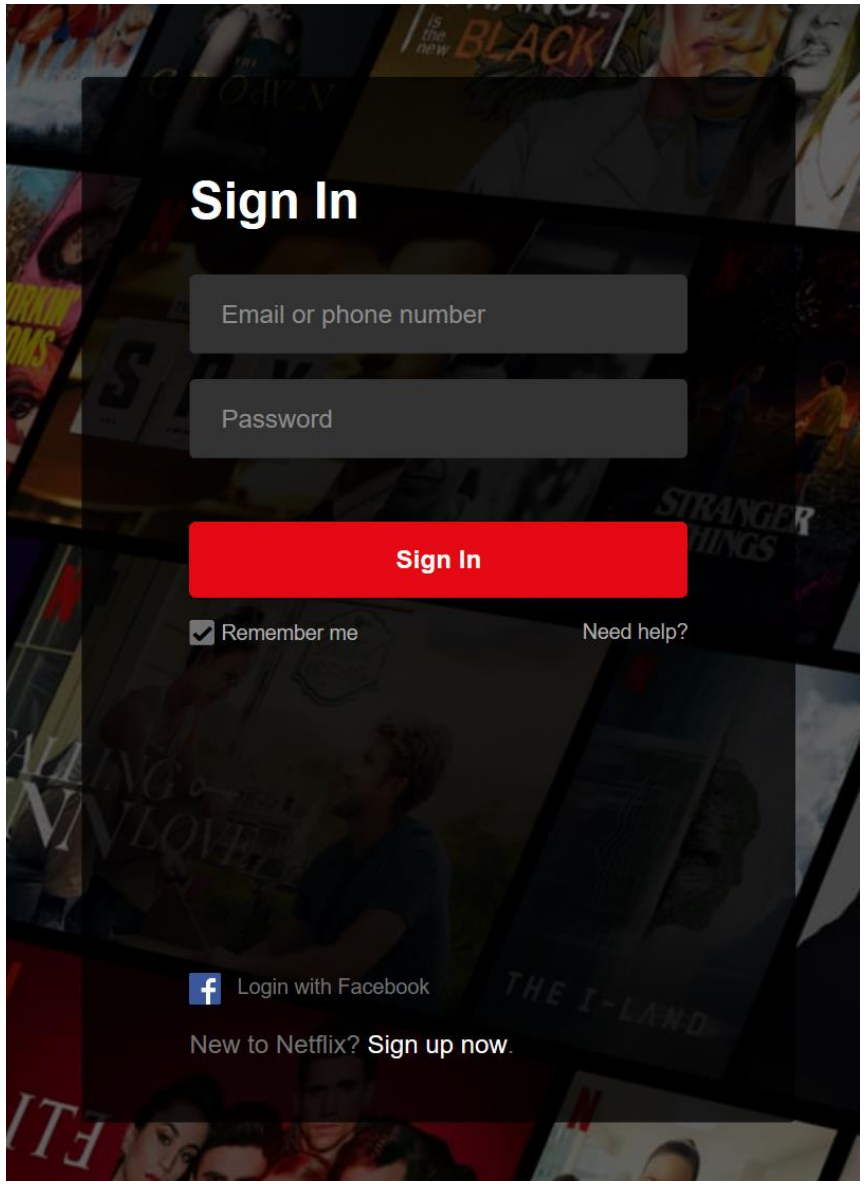


Can get text messages sent to a specific phone number.

We normally think of authentication as one directional

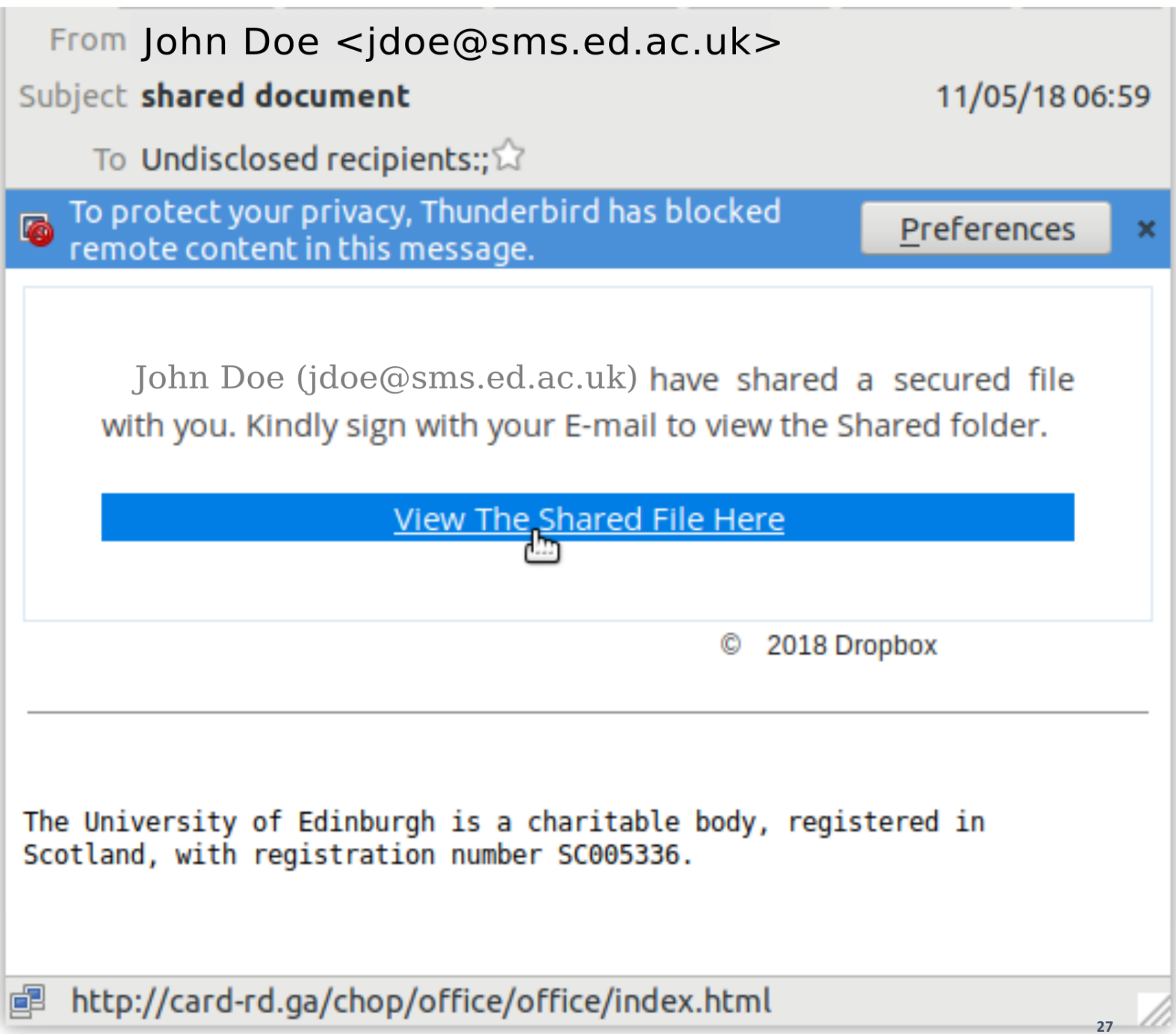


But it is actually two directional



The user must first make sure they are interacting with the “correct” website. Then the website must make sure that they are interacting with the “correct” user.

Emails like this one attempt to look like they are from a real company so the user will skip the user-side authentication check.



Phishing Support (a history lesson)

AOHell

Possibly the first case of phishing.

America Online (AOL) users were "mail bombed" where lots of mail was sent to their AOL inboxes unsolicited.

Illegal program troubles America Online

By Simson Garfinkel
SPECIAL TO THE GLOBE

An illegal computer program making the rounds on some electronic bulletin board systems is creating havoc for America Online Inc. and its customers.

Called AOHell, the program has a number of devilish features seemingly designed to turn on-line lives into living nightmares.

Armed with AOHell, a user can send hundreds of electronic mail messages to unwitting victims in just a few seconds. The technique, known as "mail bombing," can also be used to clog someone's fax machine and even someone's US mailbox.

Exploiting an apparent bug in the authorized AOL software, AOHell can also abruptly log off legitimate subscribers simply by striking the "punt" command. Another command will send a graphically obscene gesture to customers in AOL's chat forums. A button called "Ghost" will clear everyone's comments but the AOHell user's.

The author of the insidious program, who identifies himself in the program's electronic manual as Da Chronic, says he wrote AOHell because: "I hate the staff on AOL for one, I hate most of the people on AOL for another, and I wanted to cause a lot of chaos."

Indeed, AOHell's worst punches seem to be aimed directly at America Online itself.

AOHell has a nefarious system built into it for generating fictitious credit-card numbers. According to users, the program can make free accounts that last up to 10 hours of on-line time or one week, whichever comes first.

"Any member using AOHell will have their account immediately terminated," said Margaret Ryan, an AOL spokeswoman.

Ryan wouldn't say whether AOL has any technical fixes in the works that would prevent the program from functioning properly.

Although AOHell's author has chosen to remain anonymous, a built-in feature allows AOHell users to send bug reports to the author. Those reports get sent to a computer in Finland called an anonymous remailer, which allows people on the Internet to exchange electronic mail without knowing each other's identities.

"If you think AOHell 2.0 is marvelous, wait until you see 3.0," wrote the program's author, in response to an electronic mail message. "I'm almost finished with it and it will make version 2 look like a Commodore 64 program."

better, and most providers now sell service at the higher speed.

Prices vary widely, but the entry level – offered by Xensei of Quincy and prob-

Local companies frequently put together software bundles they know will work with their systems and offer them to customers to ease the once-daunting task

the easy-to-use software that made it the darling of computer novices, Prodigy sprinted another length ahead this week.

Modem speeds, which doubled and re-

https://simson.net/clips/1995/95.Globe.AOHell.pdf

AOHell

First, AOL tried to "fix" by banning accounts using AOHell. So attackers started compromising other people's accounts and getting them banned.

Illegal program troubles America Online

By Simson Garfinkel
SPECIAL TO THE GLOBE

An illegal computer program making the rounds on some electronic bulletin board systems is creating havoc for America Online Inc. and its customers.

Called AOHell, the program has a number of devilish features seemingly designed to turn on-line lives into living nightmares.

Armed with AOHell, a user can send hundreds of electronic mail messages to unwitting victims in just a few seconds. The technique, known as "mail bombing," can also be used to clog someone's fax machine and even someone's US mailbox.

Exploiting an apparent bug in the authorized AOL software, AOHell can also abruptly log off legitimate subscribers simply by striking the "punt" command. Another command will send a graphically obscene gesture to customers in AOL's chat forums. A button called "Ghost" will clear everyone's comments but the AOHell user's.

The author of the insidious program, who identifies himself in the program's electronic manual as Da Chronic, says he wrote AOHell because: "I hate the staff on AOL for one, I hate most of the people on AOL for another, and I wanted to cause a lot of chaos."

Indeed, AOHell's worst punches seem to be aimed directly at America Online itself.

AOHell has a nefarious system built into it for generating fictitious credit-card numbers. According to users, the program can make free accounts that last up to 10 hours of on-line time or one week, whichever comes first.

"Any member using AOHell will have their account immediately terminated," said Margaret Ryan, an AOL spokeswoman.

Ryan wouldn't say whether AOL has any technical fixes in the works that would prevent the program from functioning properly.

Although AOHell's author has chosen to remain anonymous, a built-in feature allows AOHell users to send bug reports to the author. Those reports get sent to a computer in Finland called an anonymous remailer, which allows people on the Internet to exchange electronic mail without knowing each other's identities.

"If you think AOHell 2.0 is marvelous, wait until you see 3.0," wrote the program's author, in response to an electronic mail message. "I'm almost finished with it and it will make version 2 look like a Commodore 64 program."

better, and most providers now sell service at the higher speed.

Prices vary widely, but the entry level – offered by Xensei of Quincy and prob-

Local companies frequently put together software bundles they know will work with their systems and offer them to customers to ease the once-daunting task

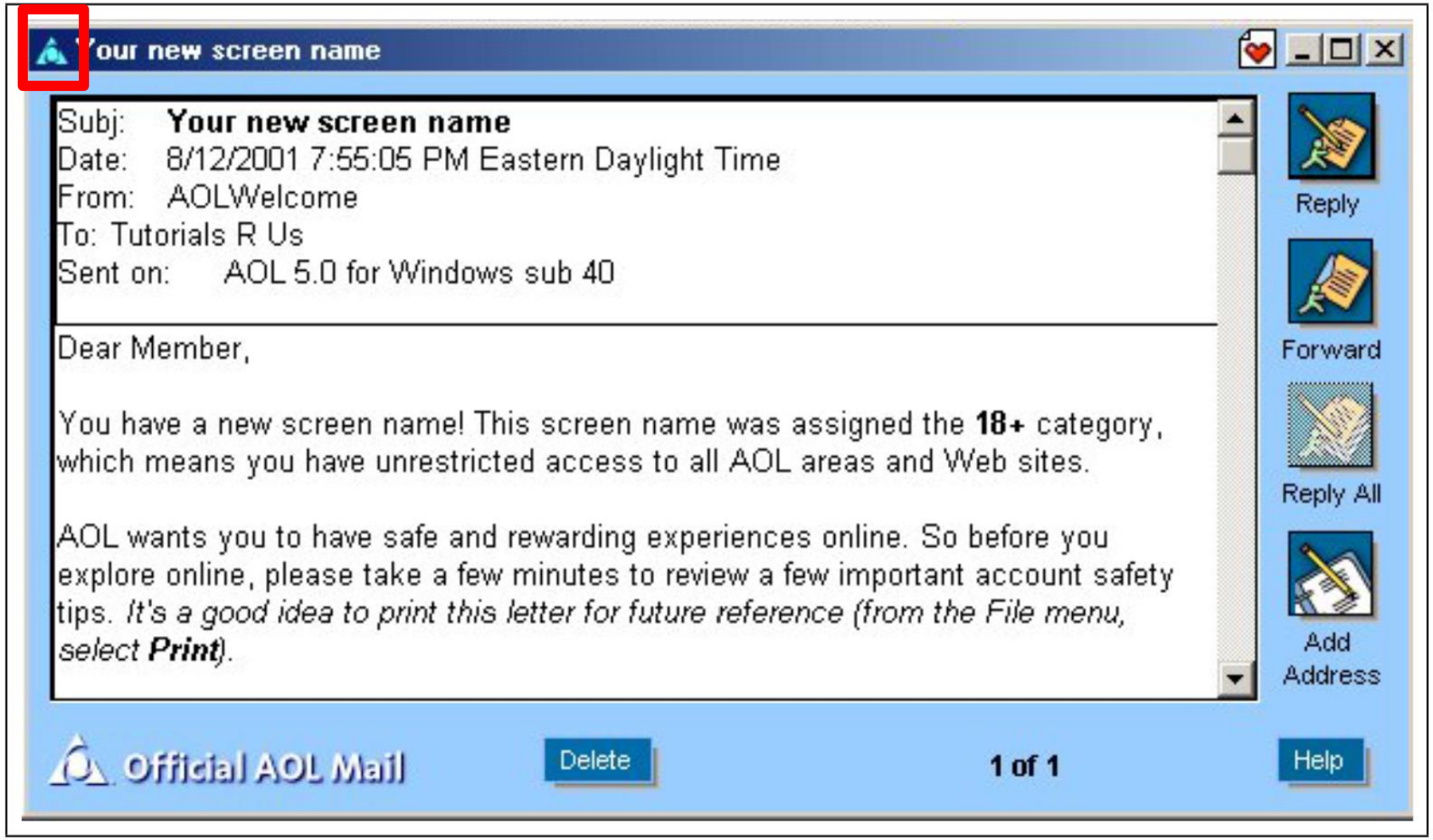
the easy-to-use software that made it the darling of computer novices, Prodigy sprinted another length ahead this week.

Modem speeds, which doubled and re-

https://simson.net/clips/1995/95.Globe.AOHell.pdf

AOHell

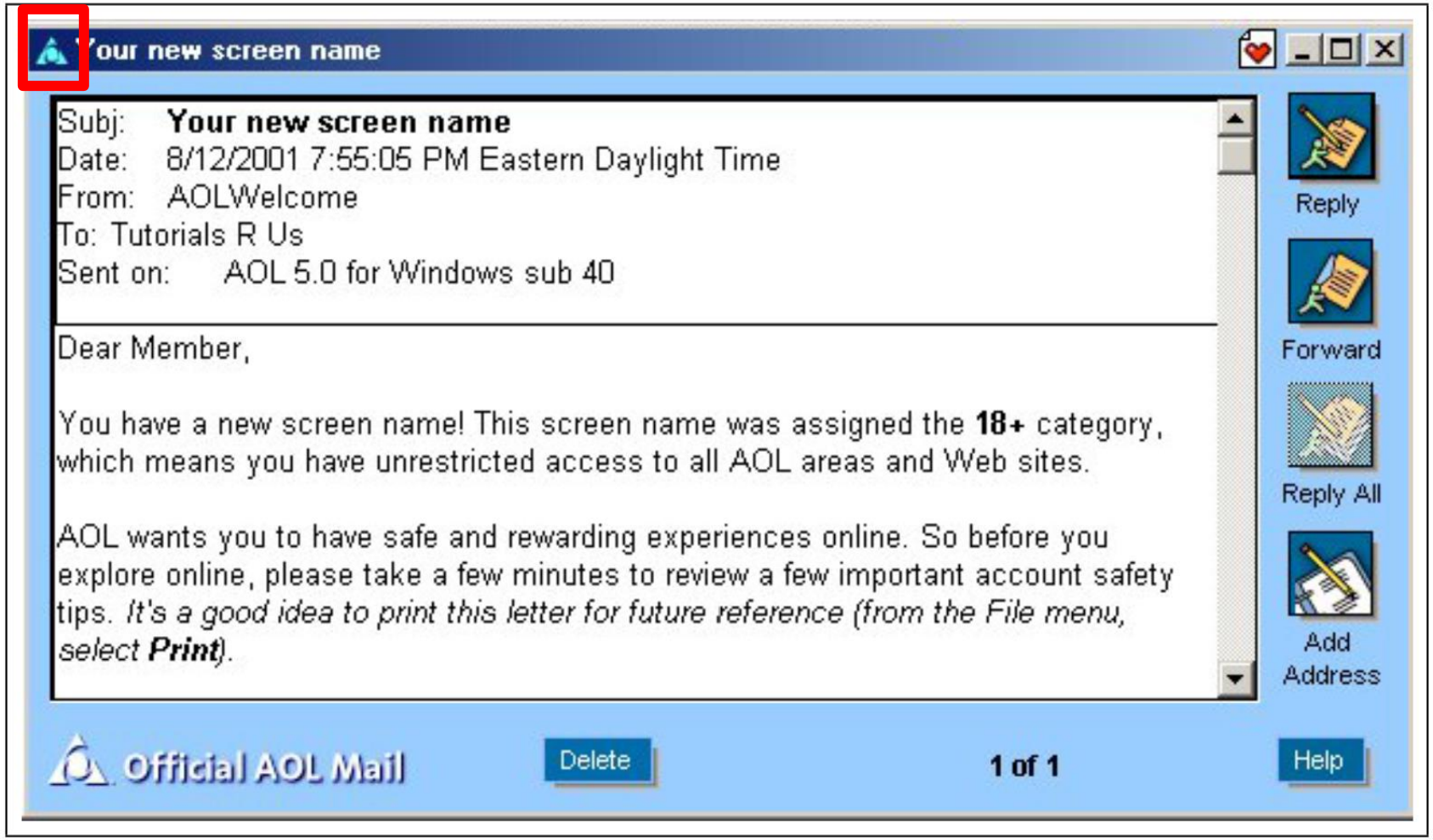
Then, AOL started using a blue icon to distinguish official AOL messages from other users' messages.



Garfinkel, Simson. Design principles and patterns for computer systems that are simultaneously secure and usable. 2005.

Passive Indicator

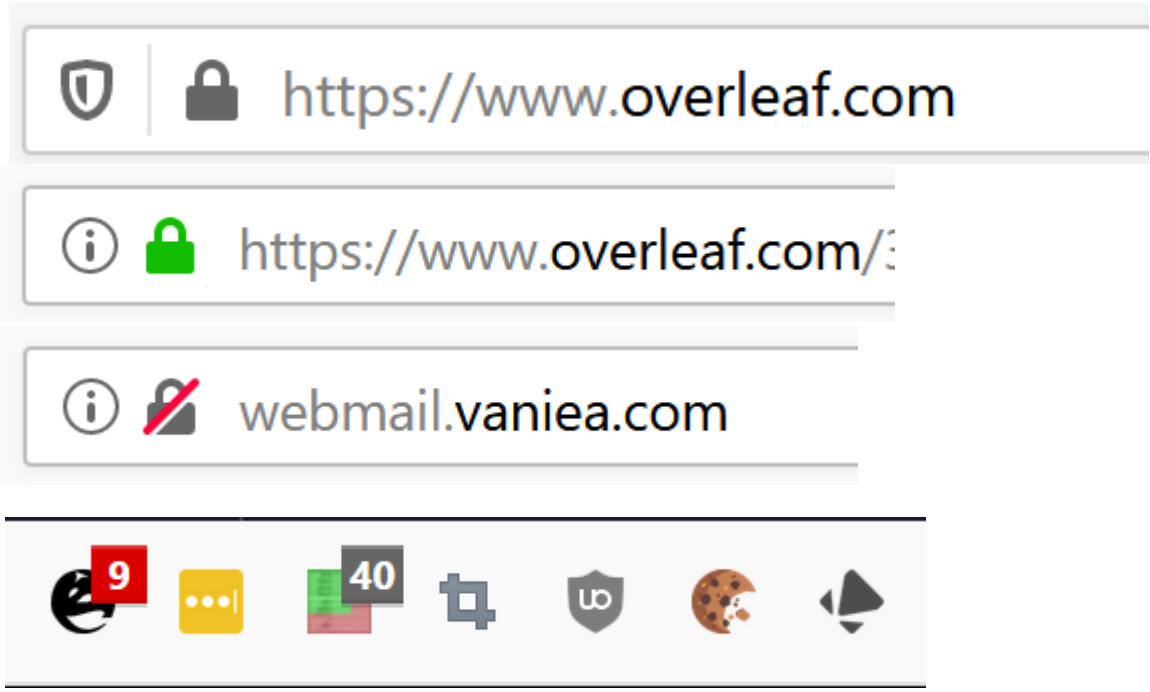
A UI element that provides information, but the user is not forced to look at or interact with.



Garfinkel, Simson. Design principles and patterns for computer systems that are simultaneously secure and usable. 2005.

Passive Indicator

A UI element that provides information, but the user is not forced to look at or interact with.



Phishing moves to email

Phishing moved off AOL and onto the less secure email. Directing people to fake sites, particularly fake financial sites.

Online Fraud Gets Sophisticated

By Laurianne McLaughlin

Online criminals are learning new tricks. Using craftier techniques, more Web scam artists are grabbing consumers' personal and financial data this year than ever before. One popular new scheme, called "phishing" or "spoofing," targets unsuspecting consumers with emails and bogus Web sites purported to be from established companies such as electronics store Best Buy, which experienced a spoof scam in June.

Here's how it worked: Consumers received emails informing them of suspicious online transactions and advising them to visit a Best Buy "fraud department" Web page. The mation are the most troubling new scam on the Internet," says Jana Monroe, Assistant Director of the FBI's Cyber Division.

At the same time, older scams, such as identity theft and auction fraud, keep on humming. Despite an associated jump in consumer complaints, however, confidence in Web shopping remains strong as businesses, state governments, and law enforcement groups work to find new ways to fight back.

Rise in Identity Thefts

The Internet Fraud Complaint Center (www.ifccfbi.gov), a clearinghouse group that aids US consumers who've suffered from online crimes, referred

gartner.com/Init) study found that seven million adults experienced identity theft in the preceding 12 months. That's a 79 percent increase from Gartner's February 2002 survey.

Another survey released in July by the nonprofit Privacy & American Business group (www.pandab.org) found similar results, with seven million Americans reporting identity theft in 2002, an 81 percent hike compared to 2001. This research group also reported that 38 percent of those hit by identity theft since 2001 suffered out-of-pocket expenses, for an average of US$740 apiece.

The Gartner study concludes that financial institutions must do more to

Phishing moves to email

- Massive rise in identity theft
- Financial loss skyrocketing
- Low conviction rate with “1-in-700 chance of escaping capture”
- Burdon falling on consumers

Online Fraud Gets Sophisticated

By Laurianne McLaughlin

Online criminals are learning new tricks. Using craftier techniques, more Web scam artists are grabbing consumers’ personal and financial data this year than ever before. One popular new scheme, called “phishing” or “spoofing,” targets unsuspecting consumers with emails and bogus Web sites purported to be from established companies such as electronics store Best Buy, which experienced a spoof scam in June.

Here’s how it worked: Consumers received emails informing them of suspicious online transactions and advising them to visit a Best Buy “fraud department” Web page. The mation are the most troubling new scam on the Internet,” says Jana Monroe, Assistant Director of the FBI’s Cyber Division.

At the same time, older scams, such as identity theft and auction fraud, keep on humming. Despite an associated jump in consumer complaints, however, confidence in Web shopping remains strong as businesses, state governments, and law enforcement groups work to find new ways to fight back.

Rise in Identity Thefts

The Internet Fraud Complaint Center (www.ifccfbi.gov), a clearinghouse group that aids US consumers who’ve suffered from online crimes, referred

gartner.com/Init) study found that seven million adults experienced identity theft in the preceding 12 months. That’s a 79 percent increase from Gartner’s February 2002 survey.

Another survey released in July by the nonprofit Privacy & American Business group (www.pandab.org) found similar results, with seven million Americans reporting identity theft in 2002, an 81 percent hike compared to 2001. This research group also reported that 38 percent of those hit by identity theft since 2001 suffered out-of-pocket expenses, for an average of US$740 apiece.

The Gartner study concludes that financial institutions must do more to

Recommend:

- Businesses should take security seriously
- Financial organizations should auto identify fraudulent applications
- Reduce impact on consumers

Web Shoppers Undaunted

Despite the escalating online fraud rates, users are not running from the conveniences of online shopping. Online retail sales hit US$76 billion in 2002 – a 48 percent surge over the previous year, according to a Shop.org annual study conducted by Forrester Research, which further predicts that online sales will rise to US$96 billion for 2003.

According to the study, a growing number of product categories now sell more than 10 percent of their total retail sales through the Internet. These include computer hardware and software (32 percent), event tickets (17 percent), and books (12 percent).

"I'd question whether people are feeling savvier or more secure," says Gartner Group's Hunter. "Consumers are exhibiting confidence in certain institutions that have taken action to ensure confidence. That does not translate to confidence across the board."

Groups started adopting custom passive indicators.

Unsurprisingly, passive indicators are not very effective.

Do Security Toolbars Actually Prevent Phishing Attacks?

Min Wu, Robert C. Miller, Simson L. Garfinkel
MIT Computer Science and Artificial Intelligence Lab
32 Vassar Street, Cambridge, MA 02139
{minwu, rcm, simsong}@csail.mit.edu

ABSTRACT
Security toolbars in a web browser show security-related information about a website to help users detect phishing attacks. Because the toolbars are designed for humans to use, they should be evaluated for usability – that is, whether these toolbars really prevent users from being tricked into providing personal information. We conducted two user studies of three security toolbars and other browser security indicators and found them all ineffective at preventing phishing attacks. Even though subjects were asked to pay attention to the toolbar, many failed to look at it; others disregarded or explained away the toolbars' warnings if the content of web pages looked legitimate. We found that many subjects do not understand phishing attacks or realize how sophisticated such attacks can be.

Author Keywords
World Wide Web and Hypermedia, E-Commerce, User Study, User Interface Design.

ACM Classification Keywords
H.5.2 User Interfaces, H.1.2 User/Machine Systems, D.4.6 Security and Protection.

INTRODUCTION
Phishing has become a significant threat to Internet users. Phishing attacks typically use legitimate-looking but fake emails and websites to deceive users into disclosing personal or financial information to the attacker. Users can also be tricked into downloading and installing hostile

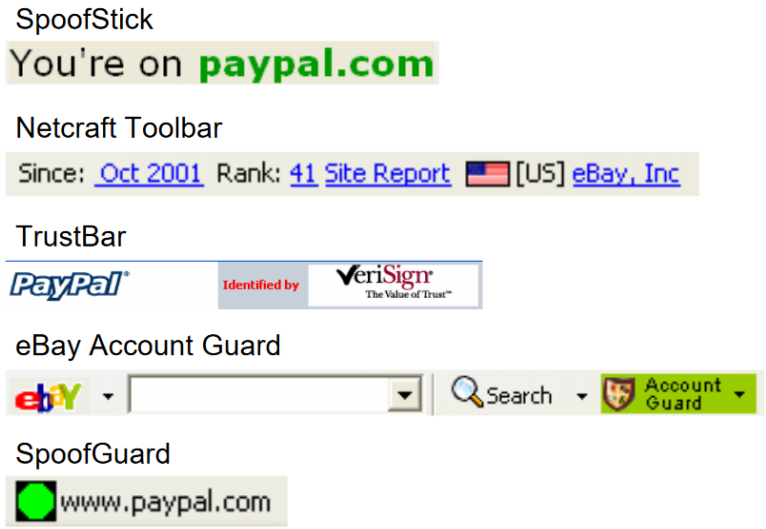


Figure 1. Existing security toolbars

admitted to having provided personal data to a phishing site; and US consumers have lost an estimated $500 million as a result of these attacks. [15]

APWG has collected and archived many phishing attacks. A typical example is an attack against eBay customers, first reported in March 2004. [1] The attack starts with an email claiming that the recipient's account information is invalid and needs to be updated by visiting the provided link. The message appears to come from `S-Harbor@eBay.com`, and the link apparently points to `cgi1.ebay.com`, but actually leads to `210.93.131.250`, a server in South Korea with no relationship to eBay. Following the link produces a web

Groups started adopting custom passive indicators.

Unsurprisingly, passive indicators are not very effective.

Do Security Toolbars Actually Prevent Phishing Attacks?

Min Wu, Robert C. Miller, Simson L. Garfinkel
MIT Computer Science and Artificial Intelligence Lab

Figure 1. Existing security toolbars

emails and websites to deceive users into disclosing personal or financial information to the attacker. Users can also be tricked into downloading and installing hostile

the link apparently points to `cgi1.ebay.com`, but actually leads to `210.93.131.250`, a server in South Korea with no relationship to eBay. Following the link produces a web

Groups started adopting custom passive indicators.

Unsurprisingly, passive indicators are not very effective.

People also tend to rationalize decisions after making them.

Do Se… Attacks?

Among the 30 subjects, 20 were spoofed by at least one wish-list attack (7 used the Neutral-Information toolbar, 6 used the SSL-Verification toolbar, and 7 used the System-Decision toolbar). We interviewed these subjects to find out why they did not recognize the attacks:

- 17 subjects (85%) mentioned in the interview that the web content looked professional or similar to what they had seen before. They were correct because the content *was* the real web site, but a high-quality phishing attack or man-in-the-middle can look exactly like the targeted

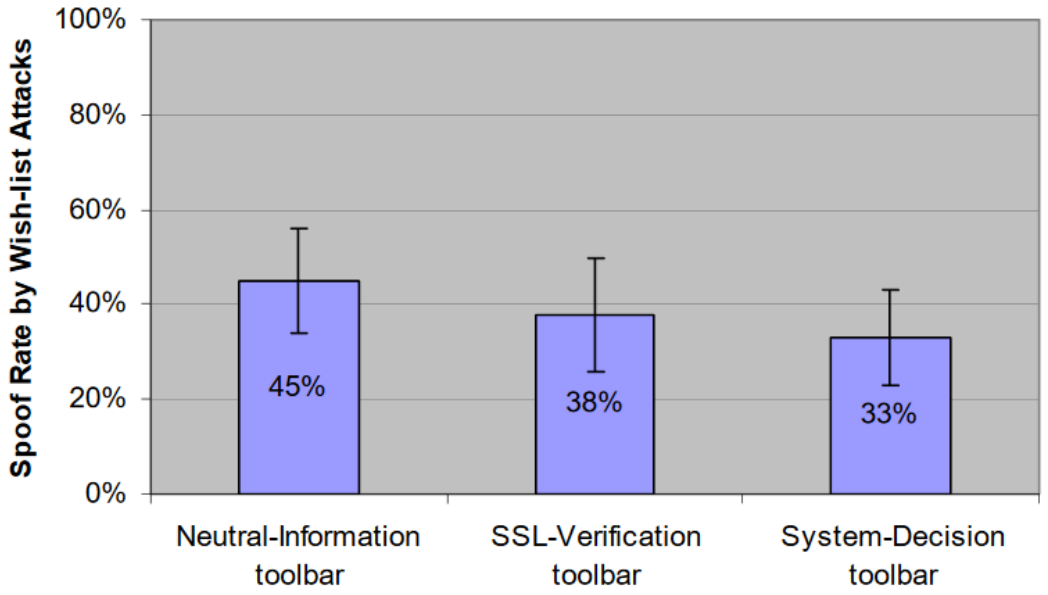


Figure 5. Spoof rates with different toolbars

ABSTRACT
Security tool… information a… attacks. Beca… use, they shou… these toolbars… providing pe… studies of thre… indicators an… phishing attac… attention to t… disregarded o… content of w… many subject… how sophistic…

Author Keyw…
World Wide… Study, User I…

ACM Classifi…
H.5.2 User I… Security and …

INTRODUCTI…
Phishing has… Phishing atta… emails and … personal or fi… also be trick…

[US] eBay, Inc

arch … Account Guard

toolbars

… data to a phishing … timated $500 million

…ny phishing attacks. …eBay customers, first …t starts with an email …nformation is invalid …e provided link. The …bor@eBay.com, and …ay.com, but actually …in South Korea with … link produces a web

Groups started adopting custom passive indicators.

Unsurprisingly, passive indicators are not very effective.

People also tend to rationalize decisions after making them.

12 subjects (60%) used rationalizations to justify the indicators of the attacks that they experienced. Nine subjects explained away odd URLs with comments like:

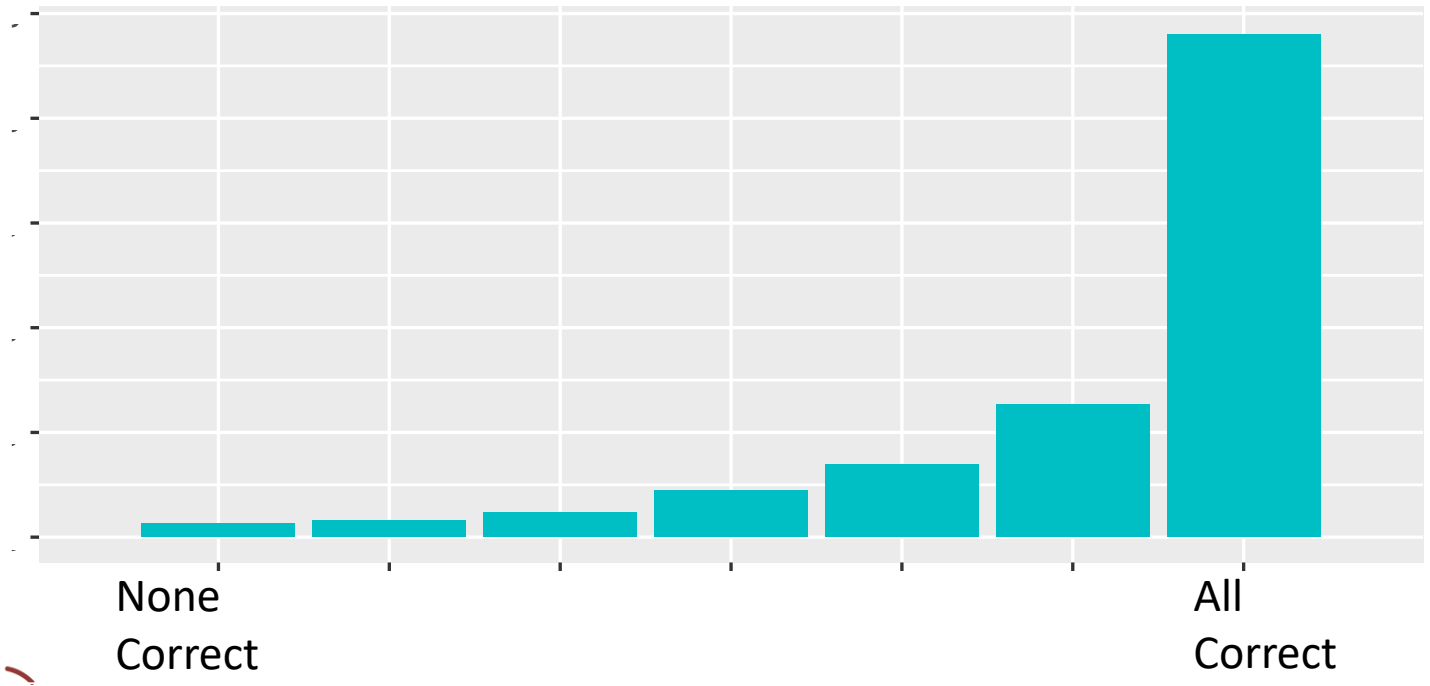
`www.ssl-yahoo.com` is a subdirectory of Yahoo!, like `mail.yahoo.com`.

`sign.travelocity.com.zaga-zaga.us` must be an outsourcing site for `travelocity.com`.

Sometimes the company [Target] has to register a different name [`www.mytargets.com`] from its brand. What if `target.com` has already been taken by another company?

Sometimes I go to a website and the site directs me to another address which is different from the one that I have typed.

I have been to other sites that used IP addresses [instead of domain names].



Name in **domain**

i.e. profile.**facebook**.com

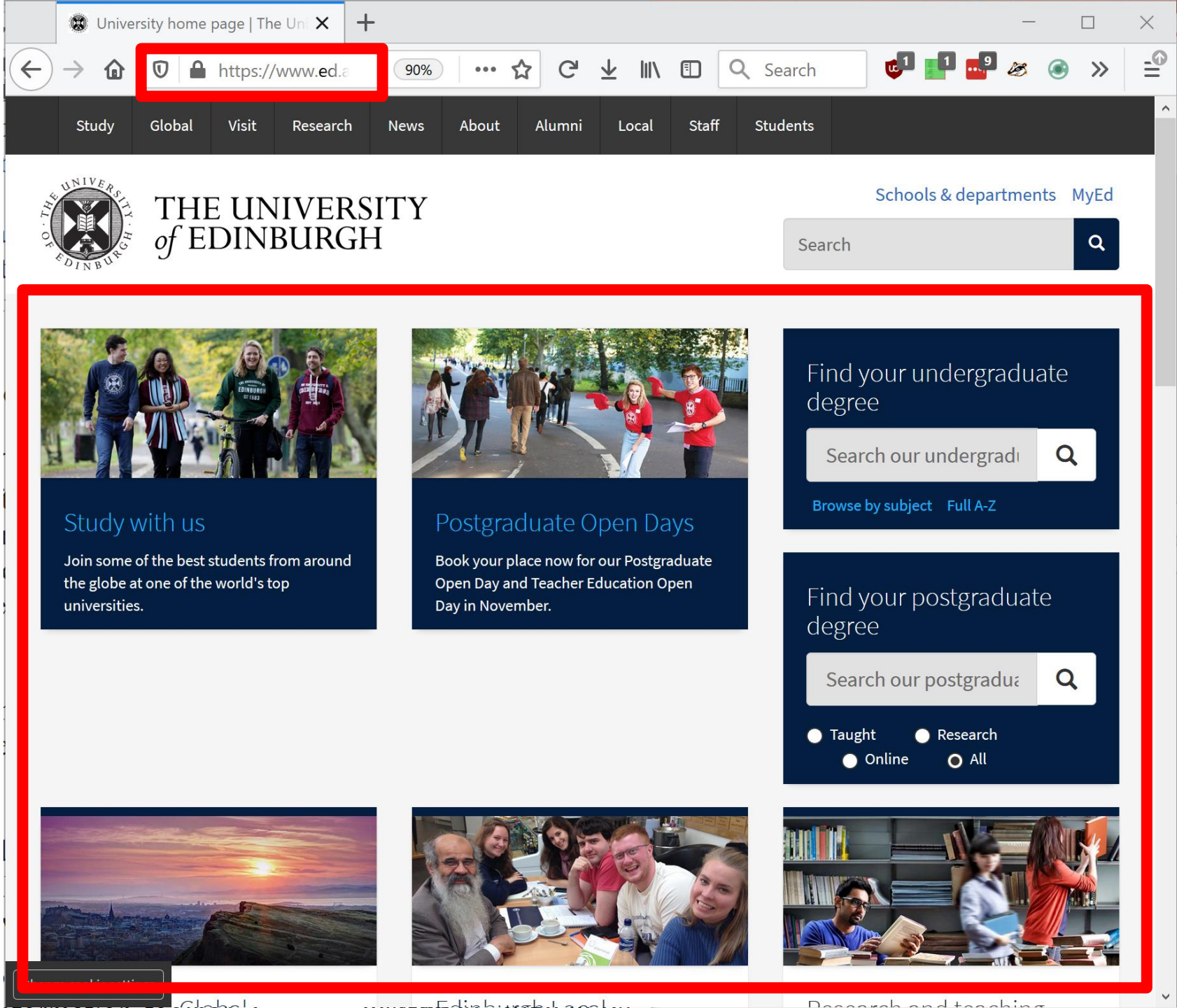
mobile.**paypal**.com

Where are people looking when a page loads?

Answer: page content

Where are the passive security indicators?

Answer: browser chrome



Passive security indicators were not working at the level researchers wanted.

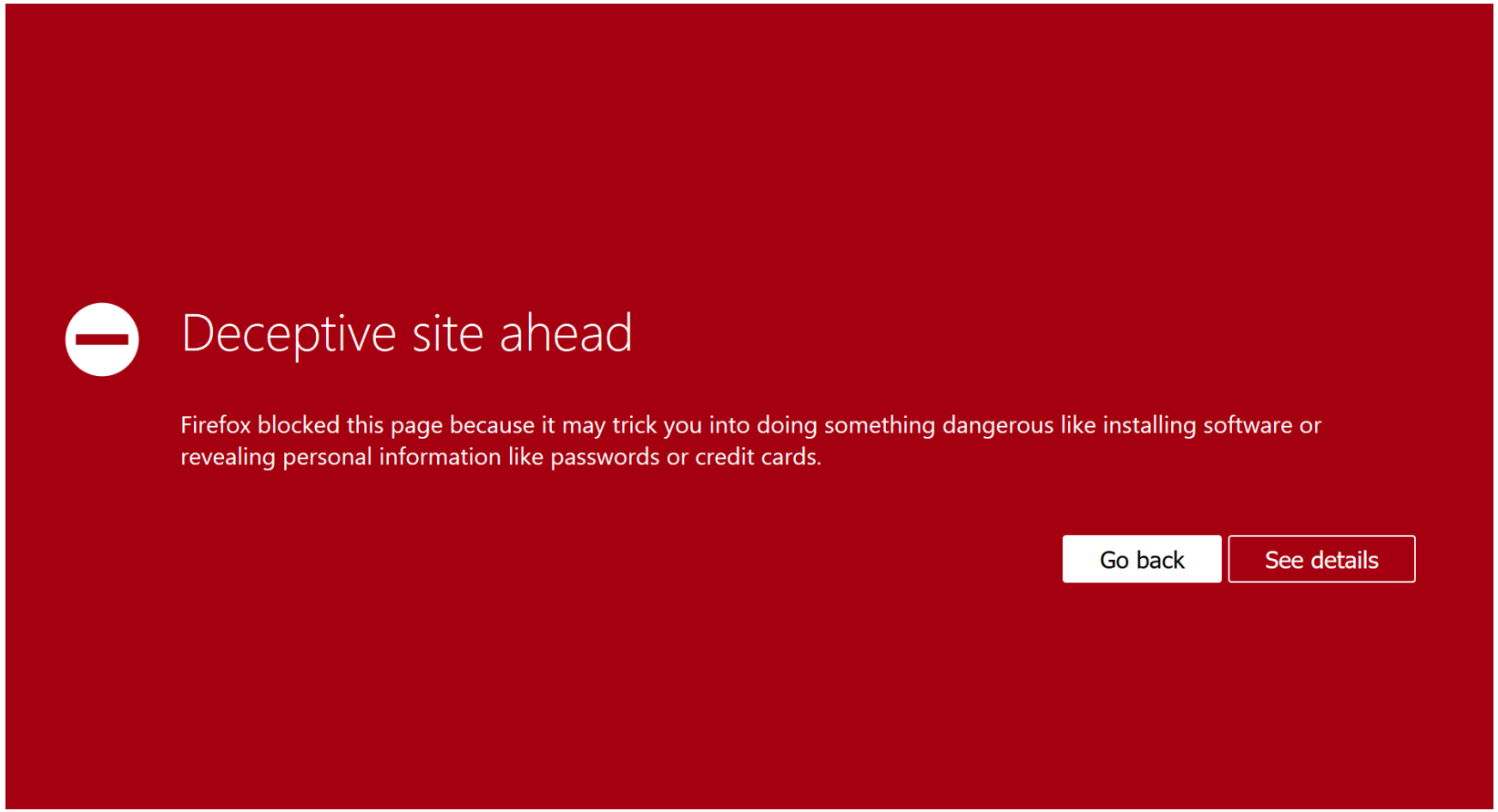
So indicators started getting more obvious and intrusive.

Being passive isn’t working….

So lets be active.

Active Indicator

A UI element that interrupts the user's activity and demands a response.



Active Indicator

Active indicators work better than passive ones in terms of helping people avoid phishing.

Condition Name	Size	Clicked	Phished
Firefox	20	20 (100%)	0 (0%)
Active IE	20	19 (95%)	9 (45%)
Passive IE	10	10 (100%)	9 (90%)
Control	10	9 (90%)	9 (90%)

Table 1. An overview depicting the number of participants in each condition, the number who clicked at least one phishing URL, and the number who entered personal information on at least one phishing website. For instance, nine of the control group participants clicked at least one phishing URL. Of these, all nine participants entered personal information on at least one of the phishing websites.

Egelman, Serge, Lorrie Faith Cranor, and Jason Hong. "You've been warned: an empirical study of the effectiveness of web browser phishing warnings." *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2008.

Click through rates

- "Click through" – when a user sees a warning and chooses to proceed anyway.
- Willingness to use Linux or use nightly builds of browsers indicates users are **more** willing to click through warnings.

Operating System	Malware		Phishing	
	Firefox	Chrome	Firefox	Chrome
Windows	7.1%	23.5%	8.9%	17.9%
MacOS	11.2%	16.6%	12.5%	17.0%
Linux	18.2%	13.9%	34.8%	31.0%

Table 1: User operating system vs. clickthrough rates for malware and phishing warnings. The data comes from stable (i.e., release) versions.

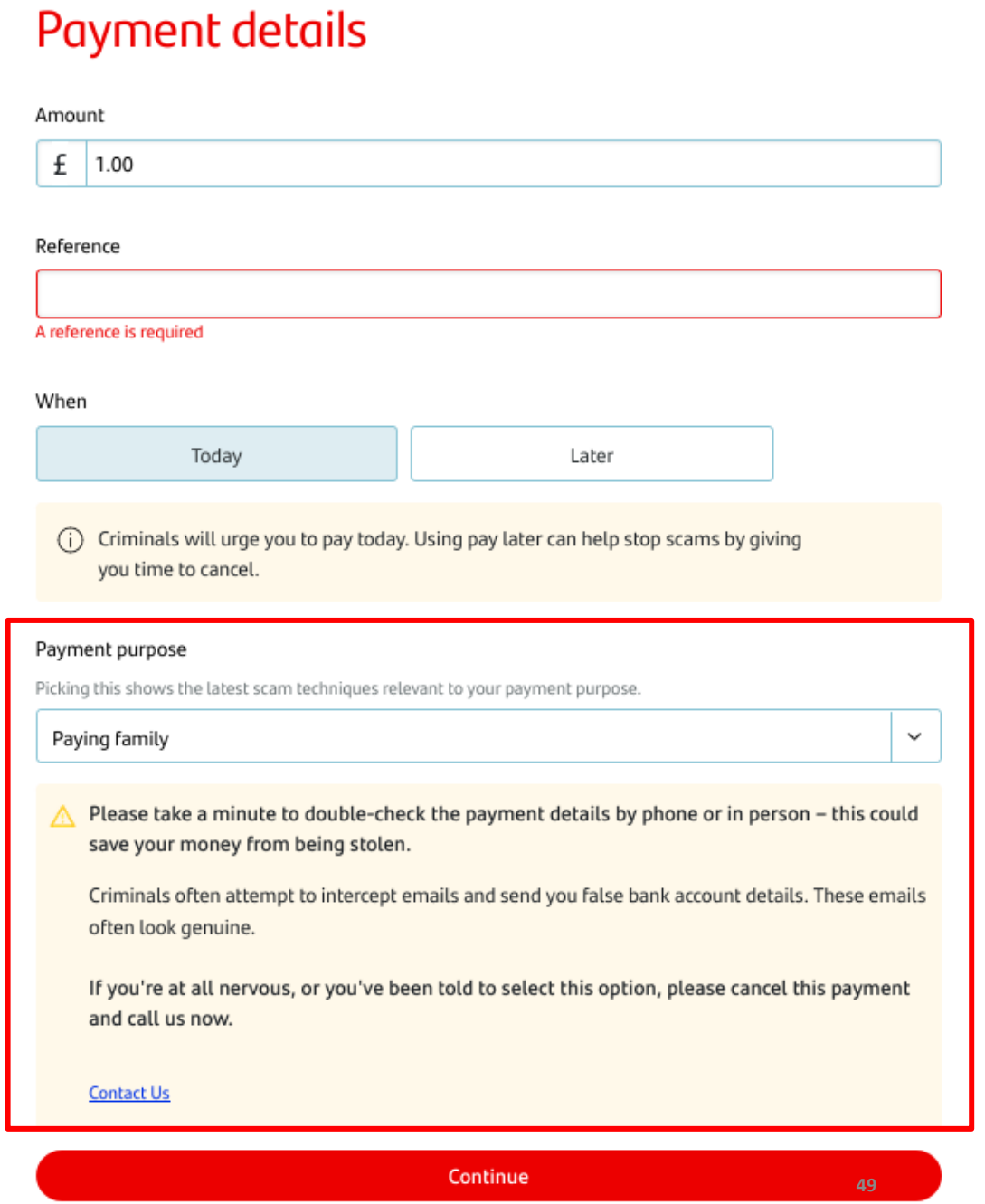
Channel	Malware		Phishing	
	Firefox	Chrome	Firefox	Chrome
Stable	7.2%	23.2%	9.1%	18.0%
Beta	8.7%	22.0%	11.2%	28.1%
Dev	9.4%	28.1%	11.6%	22.0%
Nightly	7.1%	54.8%	25.9%	20.4%

Table 2: Release channel vs. clickthrough rates for malware and phishing warnings, for all operating systems.

Akhawe, Devdatta, and Adrienne Porter Felt. "Alice in warningland: A large-scale field study of browser security warning effectiveness." *Presented as part of the 22nd {USENIX} Security Symposium (USENIX Security 13)*. 2013.

Active indicators are alive and well in 2022

- Screenshot of Santander payment page
- Asks payment purpose, then gives specific advice based on answer
- More customized to user needs, but still likely ignored



Payment purpose

Picking this shows the latest scam techniques relevant to your payment purpose.

Paying family

⚠ Please take a minute to double-check the payment details by phone or in person – this could save your money from being stolen.

Criminals often attempt to intercept emails and send you false bank account details. These emails often look genuine.

If you're at all nervous, or you've been told to select this option, please cancel this payment and call us now.

Contact Us

Where are users learning about security?

- Users follow advice from sources they trust
- Users self-evaluate advice they feel they understand, like password advice
- Marketing material in the advice results in less trust
- High socioeconomic users get phishing training at work and tend to follow it
- Low socioeconomic users tend to get and follow advice from friends and service providers (ISPs)

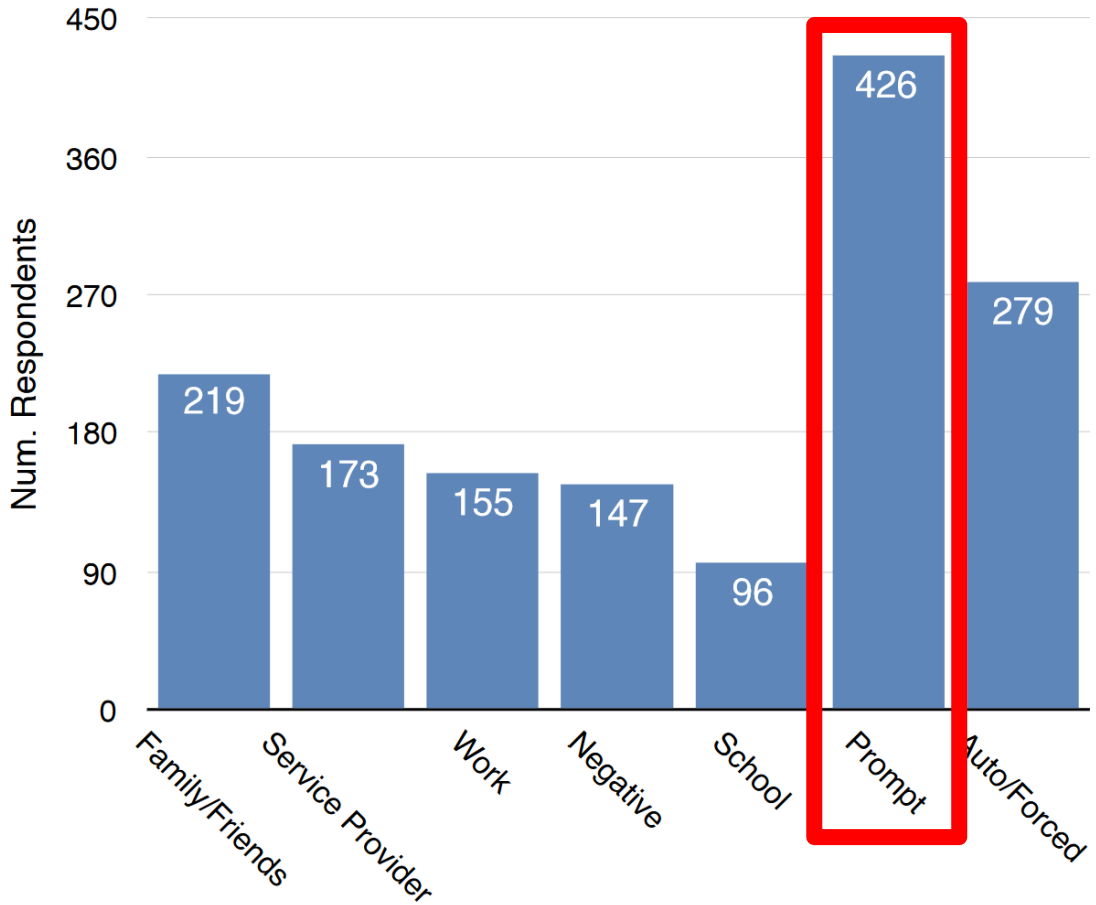


Figure 1: Prevalence of advice sources.

Redmiles, Elissa M., Sean Kross, and Michelle L. Mazurek. "**How I learned to be secure: a census-representative survey of security advice sources and behavior.**" Proceedings of the Conference on Computer and Communications Security. 2016.

Many different types of advice given in guidance

Lookout for:

- Requests for sensitive data
- Poor grammar
- Unusual senders
- Use of an alarming tone
- Has a link to a website
- Content is account related
- Content too good to be true

Protection actions:

- Check the URL in the address bar
- Check for HTTPS
- Type the URL yourself
- Check for a lock icon
- Bookmark sensitive websites

M. Mossano, K. Vaniea, L. Aldag, R. Düzgün, P. Mayer, M. Volkamer; "**Analysis of publicly available anti-phishing webpages: contradicting information, lack of concrete advice and very narrow attack vector**" In Proceedings of the 5th IEEE European Workshop on Usable Security (EuroUSEC). 2020.

In Conclusion:

- Usable security
  - Harder than it looks ☺
- Phishing only requires one side of the two way authentication to fail
- Passive indicators
  - Show information but do not block user tasks
  - Are easily ignored by users
- Active indicators
  - Block the user till they interact with the dialog in some way
  - Much more effective than passive indicators
  - Lead to habituation if a user sees the warning frequently, they stop reading it

Questions

Kami Vaniea

@kaniea
kvaniea@inf.ed.ac.uk
tulipslab.org

Active Indicator

A huge downside of active indicators is "habituation" where the user starts learning that the warnings always happen and starts ignoring them.

C. Bravo-Lillo, et al. Your Attention Please: Designing security-decision UIs to make genuine risks harder to ignore. In the Symposium On Usable Privacy and Security, 2013.

Your Attention Please

Designing security-decision UIs to make genuine risks harder to ignore

Cristian Bravo-Lillo
cbravo@cmu.edu

Lorrie Faith Cranor
lorrie@cmu.edu

Julie Downs
downs@cmu.edu

Saranga Komanduri
sarangak@cmu.edu

Robert W. Reeder
reeder@cs.cmu.edu

Stuart Schechter
stus@microsoft.com

Manya Sleeper
msleeper@cmu.edu

ABSTRACT

We designed and tested *attractors* for computer security dialogs: user-interface modifications used to draw users' attention to the most important information for making decisions. Some of these modifications were purely visual, while others temporarily inhibited potentially-dangerous behaviors to redirect users' attention to salient information. We conducted three between-subjects experiments to test the effectiveness of the attractors.

In the first two experiments, we sent participants to perform a task on what appeared to be a third-party site that required installation of a browser plugin. We presented them with what appeared to be an installation dialog from their operating system. Participants who saw dialogs that employed inhibitive attractors were significantly less likely than those in the control group to ignore clues that installing this software might be harmful.

In the third experiment, we attempted to habituate participants to dialogs that they knew were part of the experiment. We used attractors to highlight a field that was of no value during habituation trials and contained critical information after the habituation period. Participants exposed to inhibitive attractors were two to three times more likely to make an informed decision than those in the control condition.

1. INTRODUCTION

Like the boy who cried wolf from Aesop's Fables, today's computer systems perpetually cry for attention in the name of safety, and hundreds of cries may be heard without a real threat. *Did you want to open a file in a legacy file format? Is it OK that this certificate is out of date? Do you want to view content that was sent insecurely?* The inevitable result is that, like Aesop's villagers, users stop paying attention. When a security dialog does contain information that could alert users to a real risk, they are less likely to notice it.

Reducing the onslaught of interrupting security warning dialogs might help reduce the strain on users' attention. Some warnings can be removed by re-architecting systems to reduce the potential for harm, such as by building file parsers in type-safe languages or sandboxing unsafe code.

Yet inevitably, some decisions must eventually be made by users. One type of unavoidable decision is the choice to take a risk that some users may embrace and others may reject. For example, some users may want to share their location with an application that others would not share their location with. In other cases, users have knowledge, which the system does not have, that is essential to making a correct choice. For example, the user may know that a particular wireless network is operated by somebody they trust.

Designing user interfaces to facilitate necessary security decisions is especially difficult given that the damage caused