ECE750: Usable Security and Privacy

Phishing

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

First, the news...

- First 5 minutes we talk about something interesting and recent
- You will not be tested on the news part of lecture
- You may use news as an example on tests
- Why do this?
    1. Some students show up late for various good reasons
    2. Reward students who show up on time
    3. Important to see real world examples

PHISHING: AN OVERVIEW

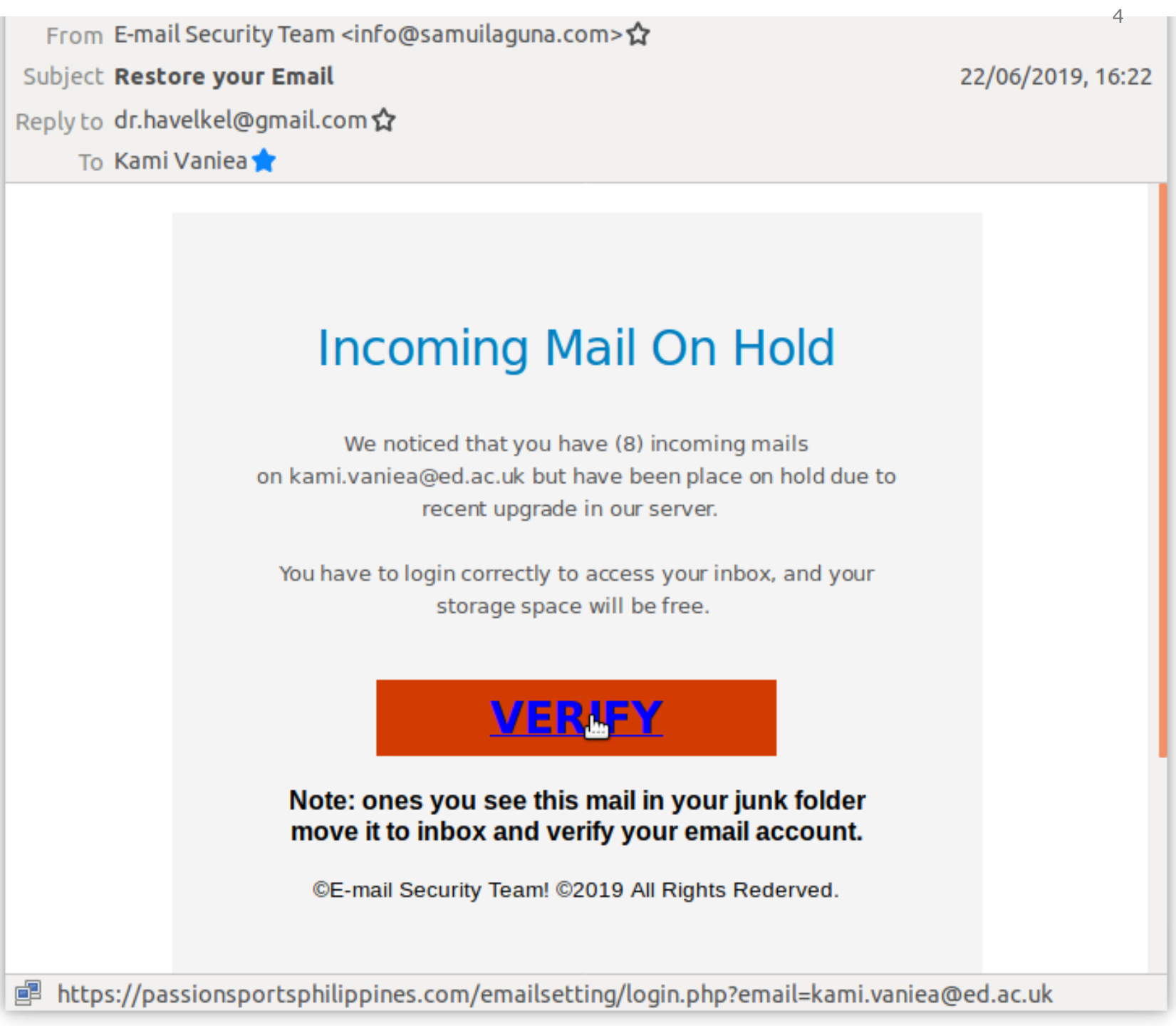
This is a phishing email

Look real

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

But

- Wrong URL
- Wrong From



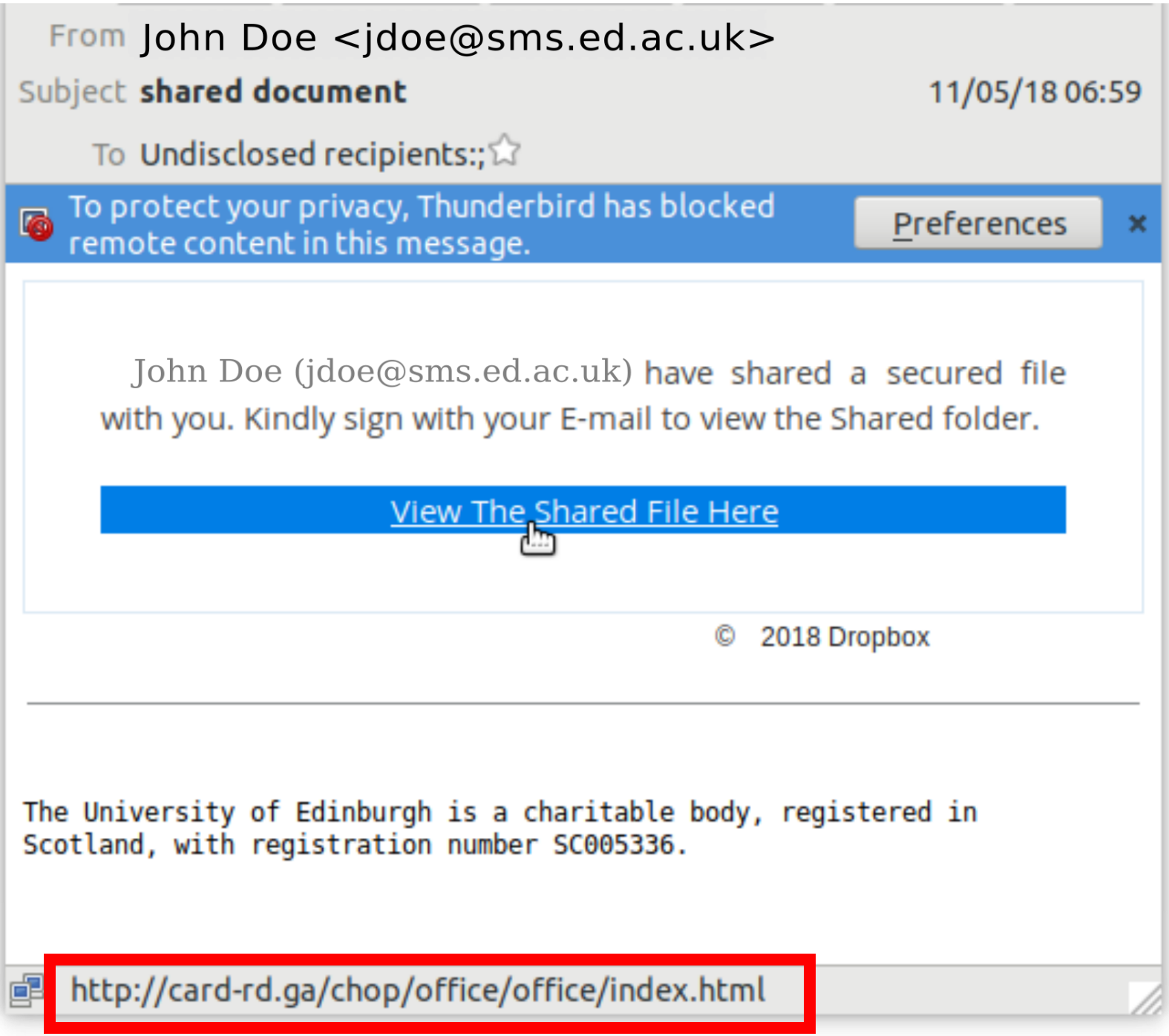
This is a phishing email

Look real

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

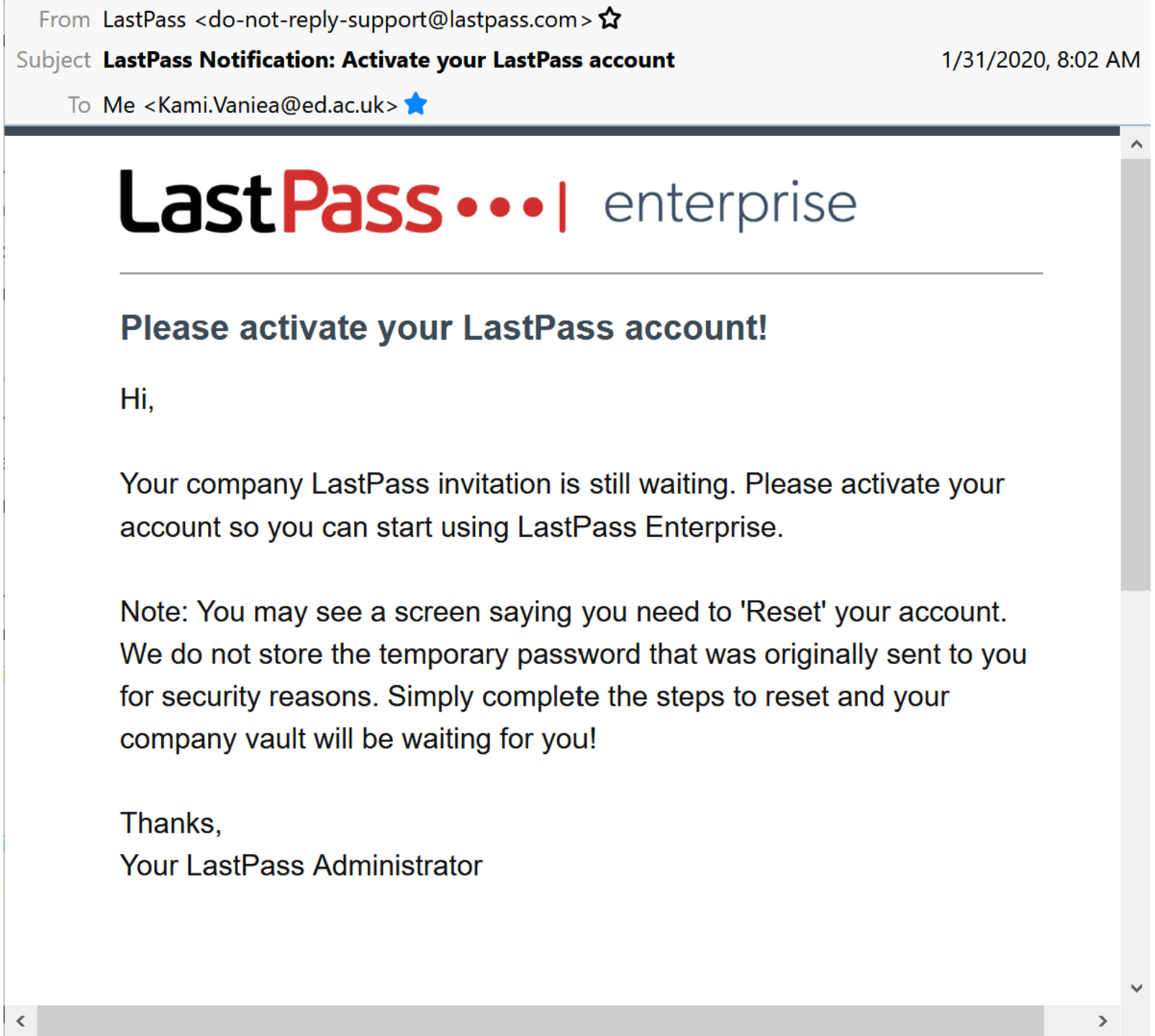
But

- 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
- Signed “LastPass Administrator”



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,

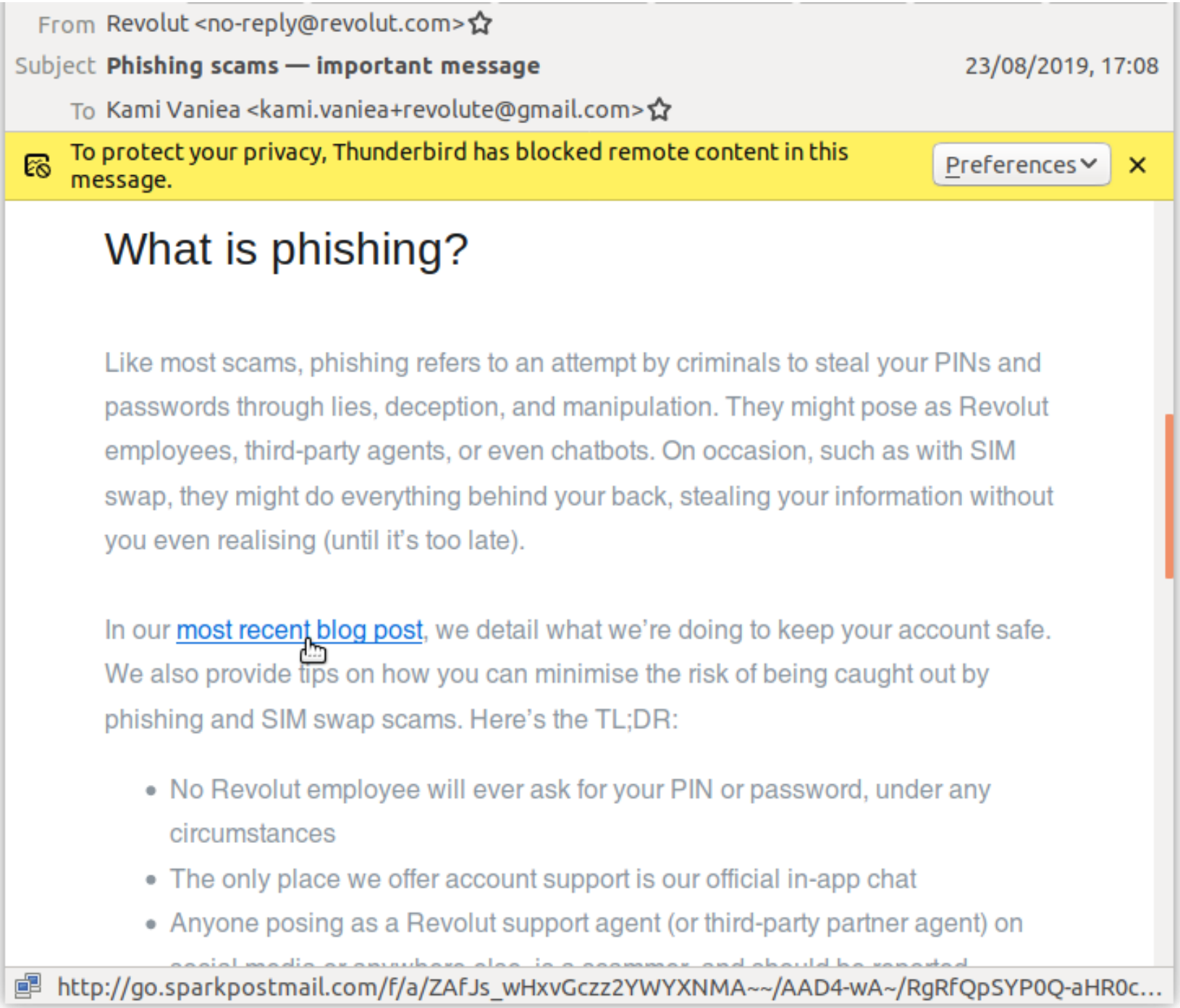
Your company LastPass invitation is still waiting. Please activate your account so you can start using LastPass Enterprise.

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

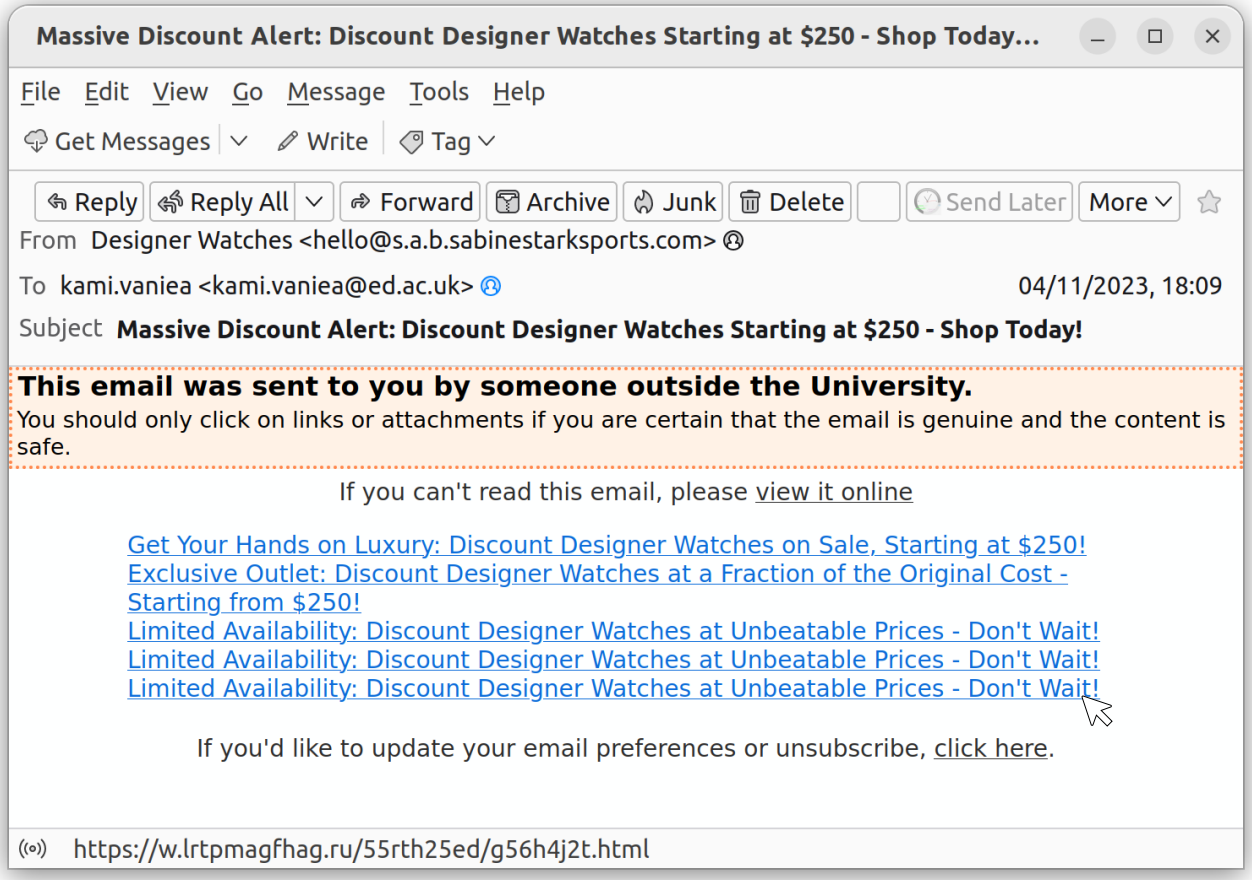
This is not a phishing email

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



Is this email phishing? A scam? A great deal?

- Is the URL: w.lrtpmagfhag.ru safe?



Raw Whois Data

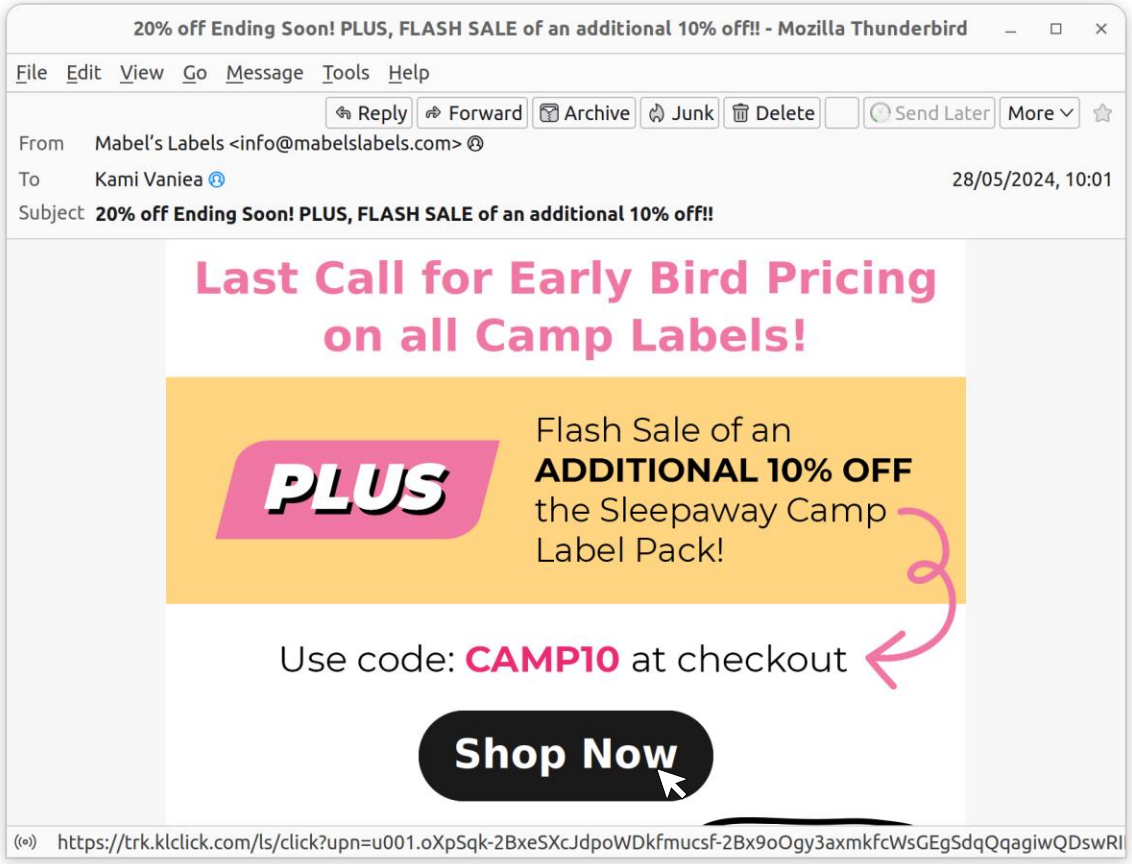
```
% TCI Whois Service. Terms of use:
% https://tcinet.ru/documents/whois_ru_rf.pdf (in Russian)
% https://tcinet.ru/documents/whois_su.pdf (in Russian)

domain:         LRTPMAGFHAG.RU
nserver:        mark.ns.cloudflare.com.
nserver:        stephane.ns.cloudflare.com.
state:          REGISTERED, DELEGATED, VERIFIED
person:         Private Person
registrar:      R01-RU
admin-contact: https://partner.r01.ru/contact_admin.khtml
created:        2023-09-26T12:36:33Z
paid-till:      2024-09-26T12:36:33Z
free-date:      2024-10-27
source:         TCI

Last updated on 2024-06-27T16:11:30Z
```

Is this email phishing? A scam? A great deal?

- Is the URL: trk.klclick.com safe?

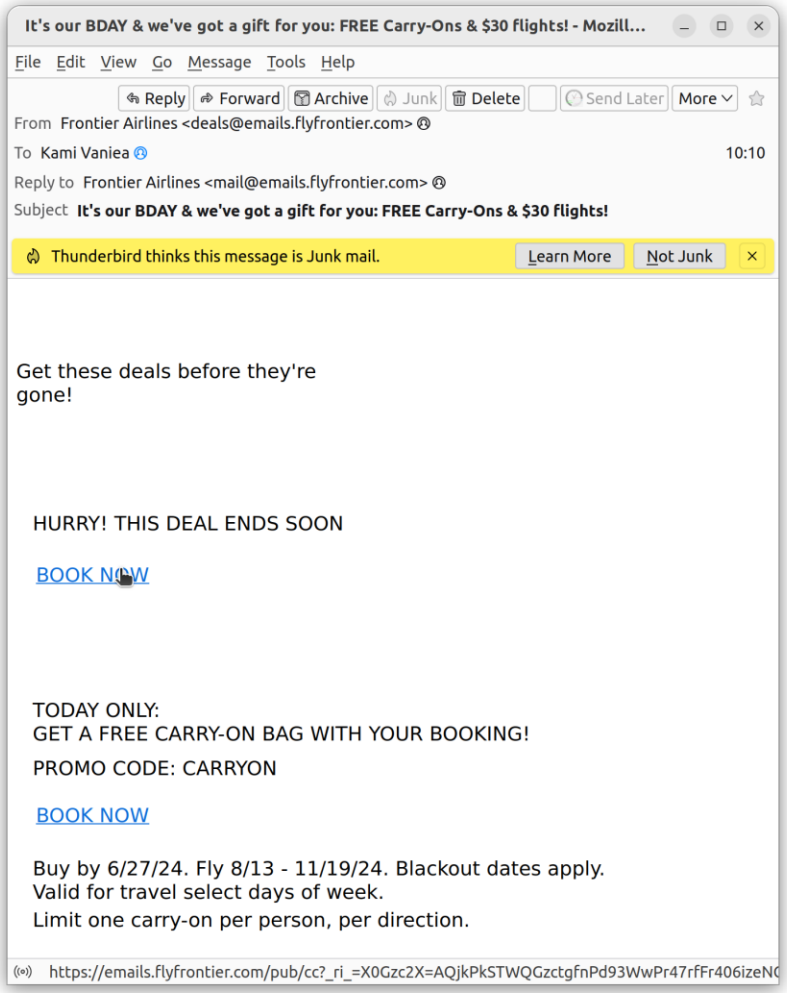


Raw Whois Data

```
Domain name: klclick.com
Registry Domain ID: 2068516775_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2018-01-10T06:58:25.00Z
Creation Date: 2016-10-24T17:39:03.00Z
Registrar Registration Expiration Date: 2026-10-24T17:39:03.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.9854014545
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Redacted for Privacy Purposes
```

Is this email phishing? A scam? A great deal?

Is the URL: emails.flyfrontier.com safe?

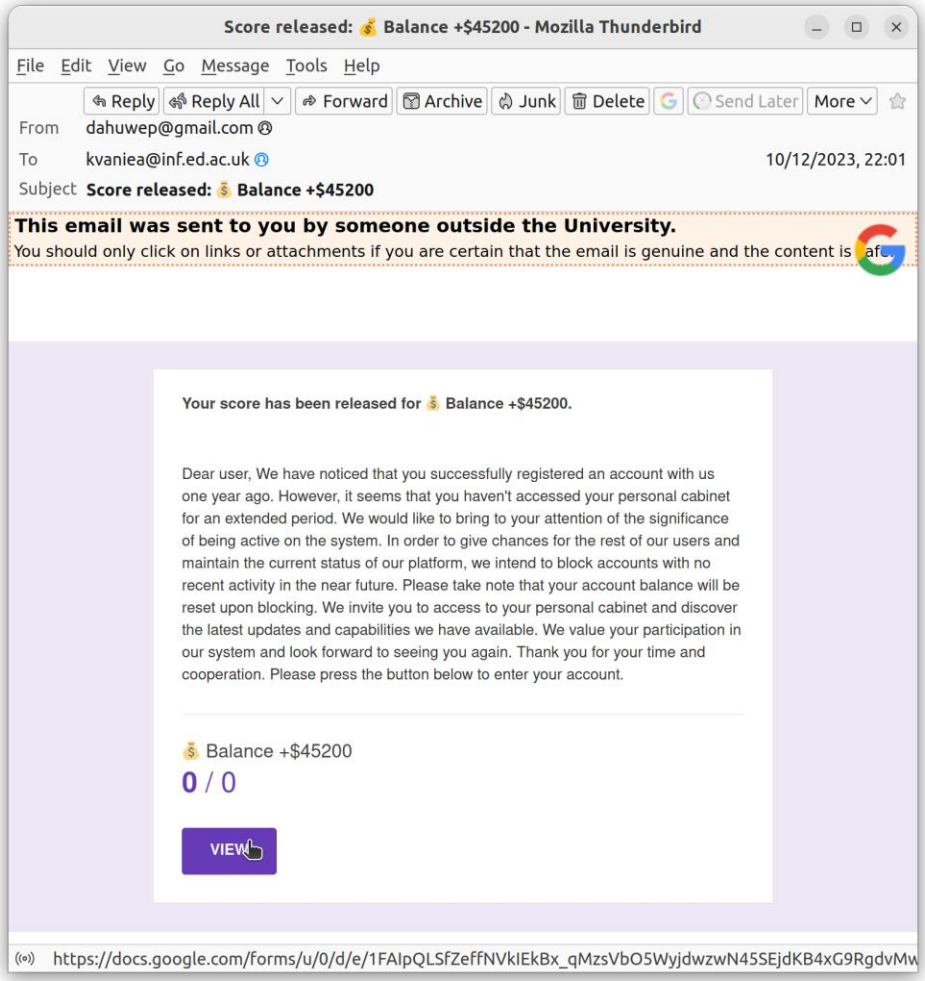


Raw Whois Data

```
Domain Name: FLYFRONTIER.COM
Registry Domain ID: 1487103_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2023-02-16T19:13:43Z
Creation Date: 1996-04-26T04:00:00Z
Registrar Registration Expiration Date: 2026-04-27T04:00:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32256
Registrant Country: US
Registrant Phone: +1.5707088622
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: ku63f9e75ww@networksolutionsprivateregistration.com
Registry Admin ID:
```

Is this email phishing? A scam? A great deal?

- Is the URL: docs.google.com safe?



Domain Information

Domain:	google.com
Registrar:	MarkMonitor Inc.
Registered On:	1997-09-15
Expires On:	2028-09-13
Updated On:	2019-09-09
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	ns1.google.com ns2.google.com ns3.google.com ns4.google.com

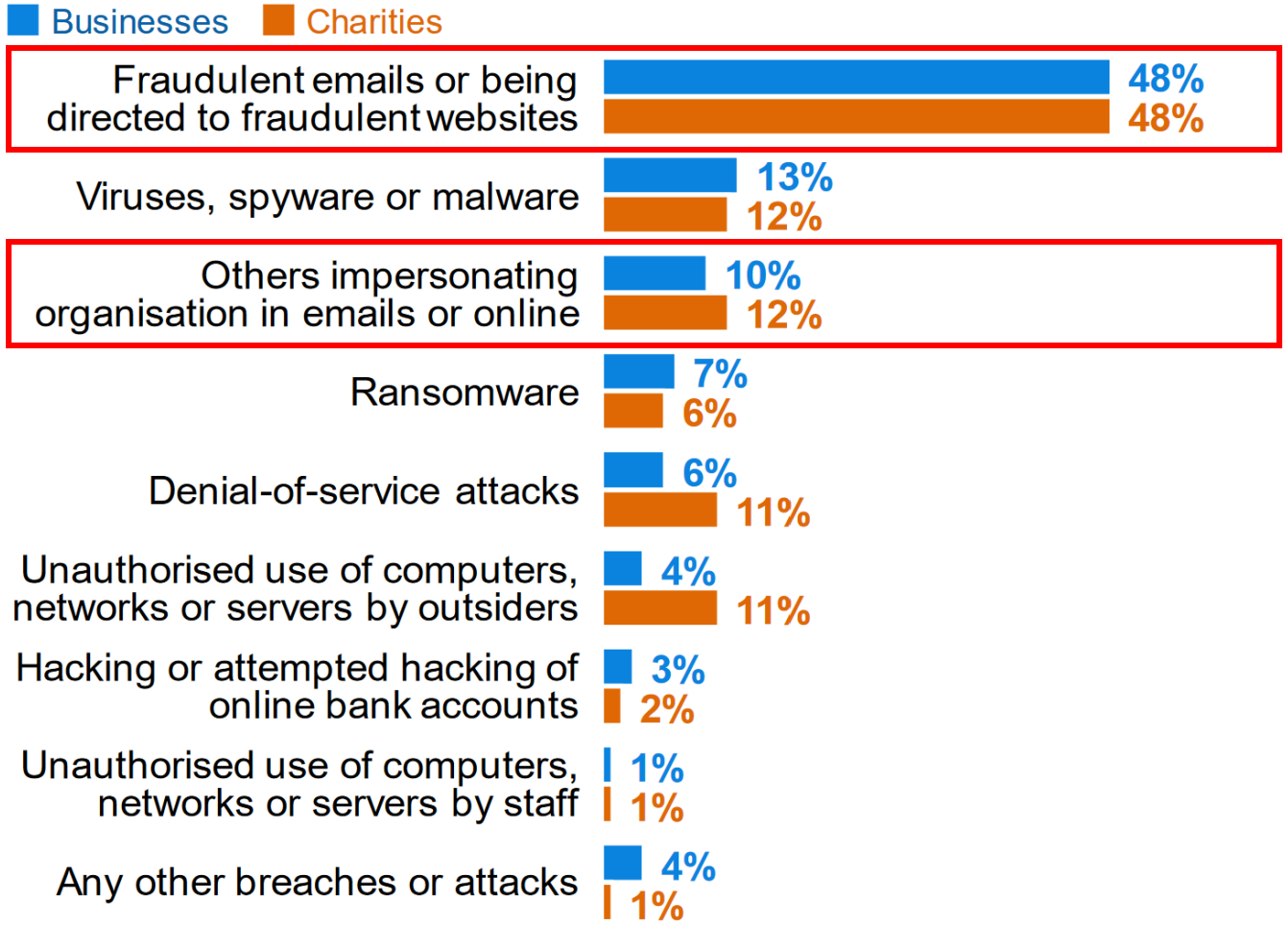
Registrant Contact

Organization:	Google LLC
State:	CA
Country:	US
Email:	Select Request Email Form at https://domains.markmonitor.com/whois/google.com

Phishing is very common and very disruptive

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.

UK is starting to think about "cyber hygiene" not just "vulnerabilities" and "defense".

Cyber hygiene

The most common cyber threats are relatively unsophisticated, so government guidance advises businesses and charities to protect themselves using a set of “cyber hygiene” measures. A majority of businesses and charities have a broad range of these measures in place. The most common are updated malware protection, password policies, cloud back-ups, restricted admin rights and network firewalls - each administered by at least seven in ten businesses and around half of charities or more. Compared to 2023, the deployment of various controls and procedures has risen slightly among businesses:

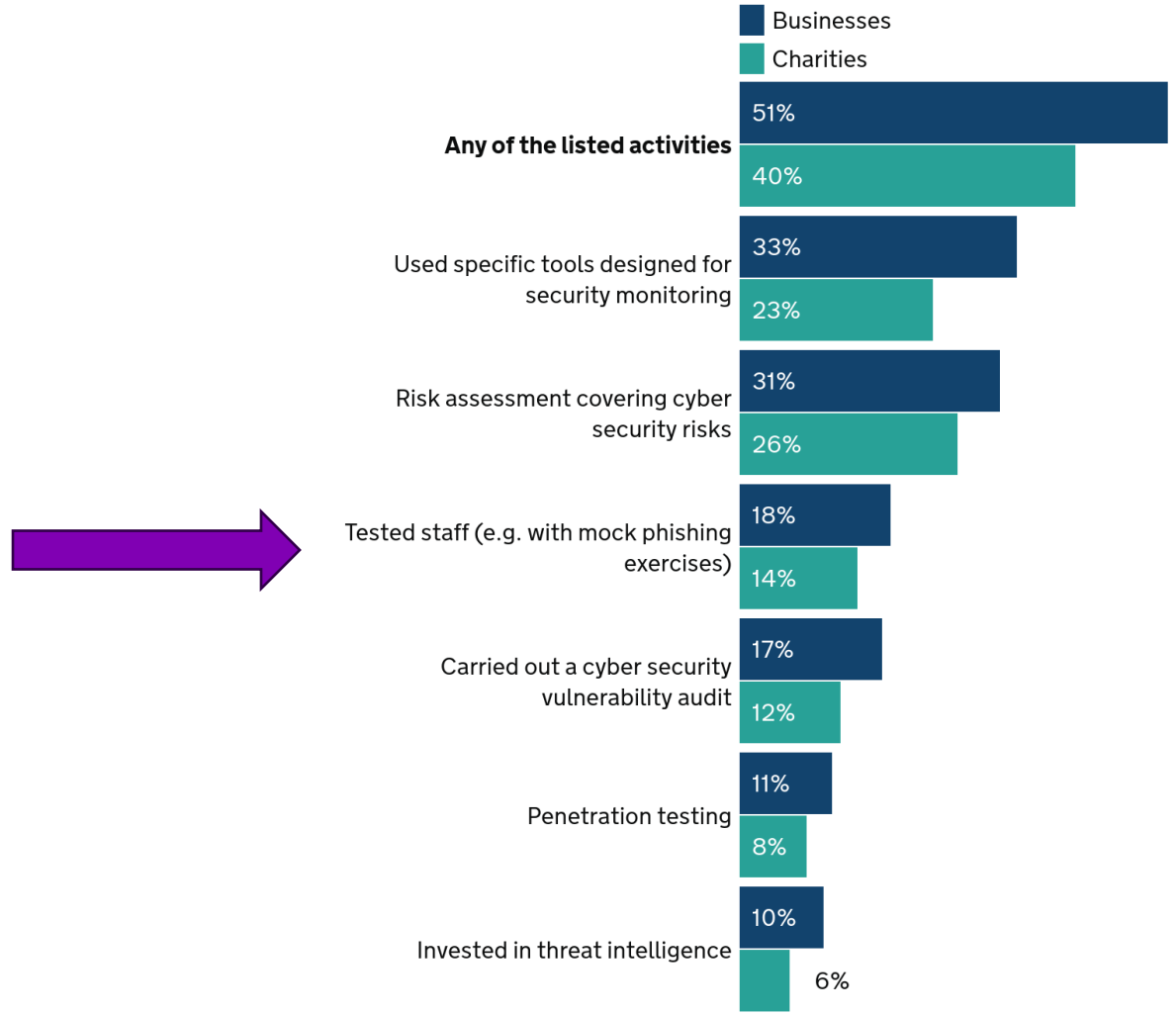
- using up-to-date malware protection (up from 76% to 83%)
- restricting admin rights (up from 67% to 73%)
- network firewalls (up from 66% to 75%)
- agreed processes for phishing emails (up from 48% to 54%).

These trends represent a partial reversal of the pattern seen in the previous three years of the survey, where some areas had seen consistent declines among businesses. The changes mainly reflect shifts in the micro business population and, to a lesser extent, small and medium businesses.

Testing staff with mock phishing is (unfortunately) considered best practice.

Figure 3.1: Percentage of organisations that have carried out the following activities to identify cyber security risks in the last 12 months

Change to table and accessible view



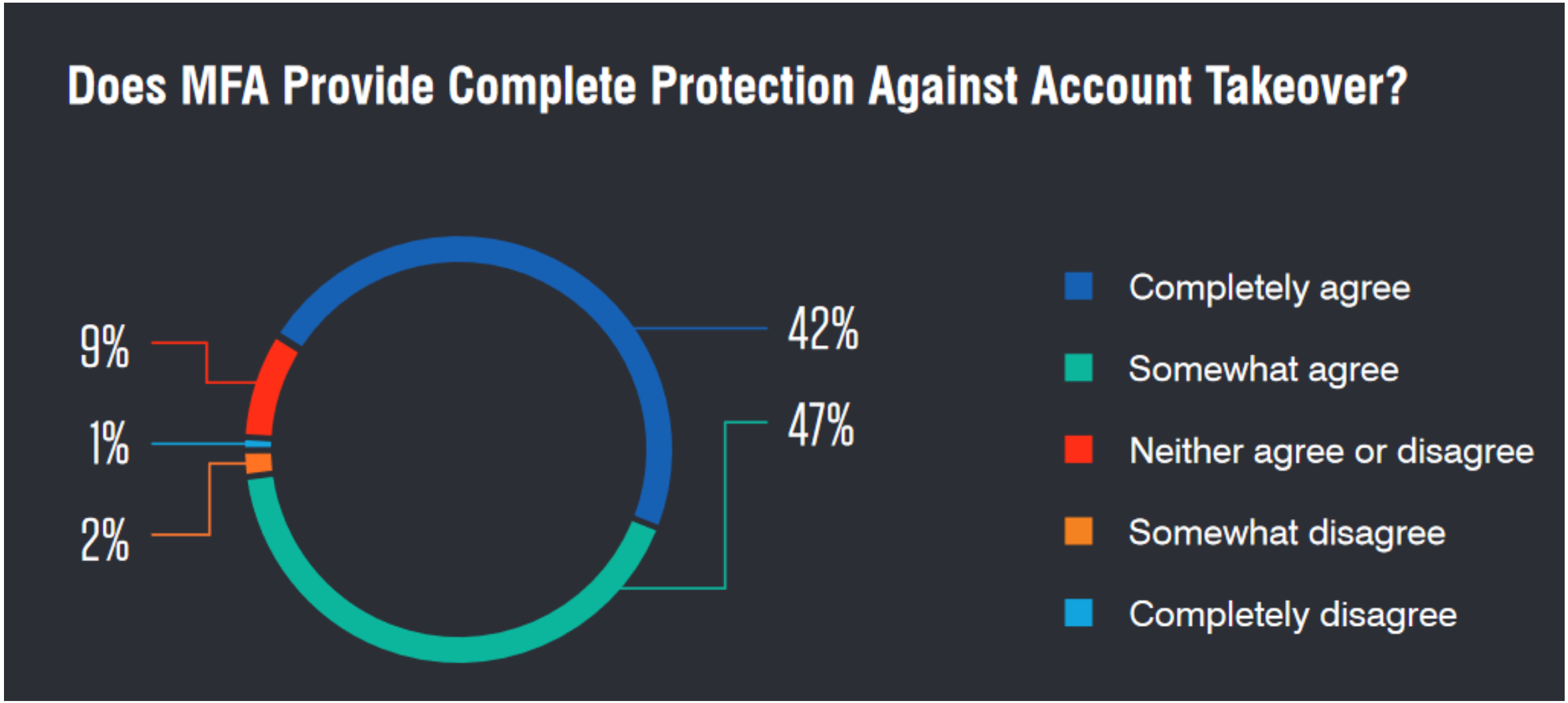
Bases: 2,000 UK businesses; 1,004 charities

MFA = Multi factor authentication

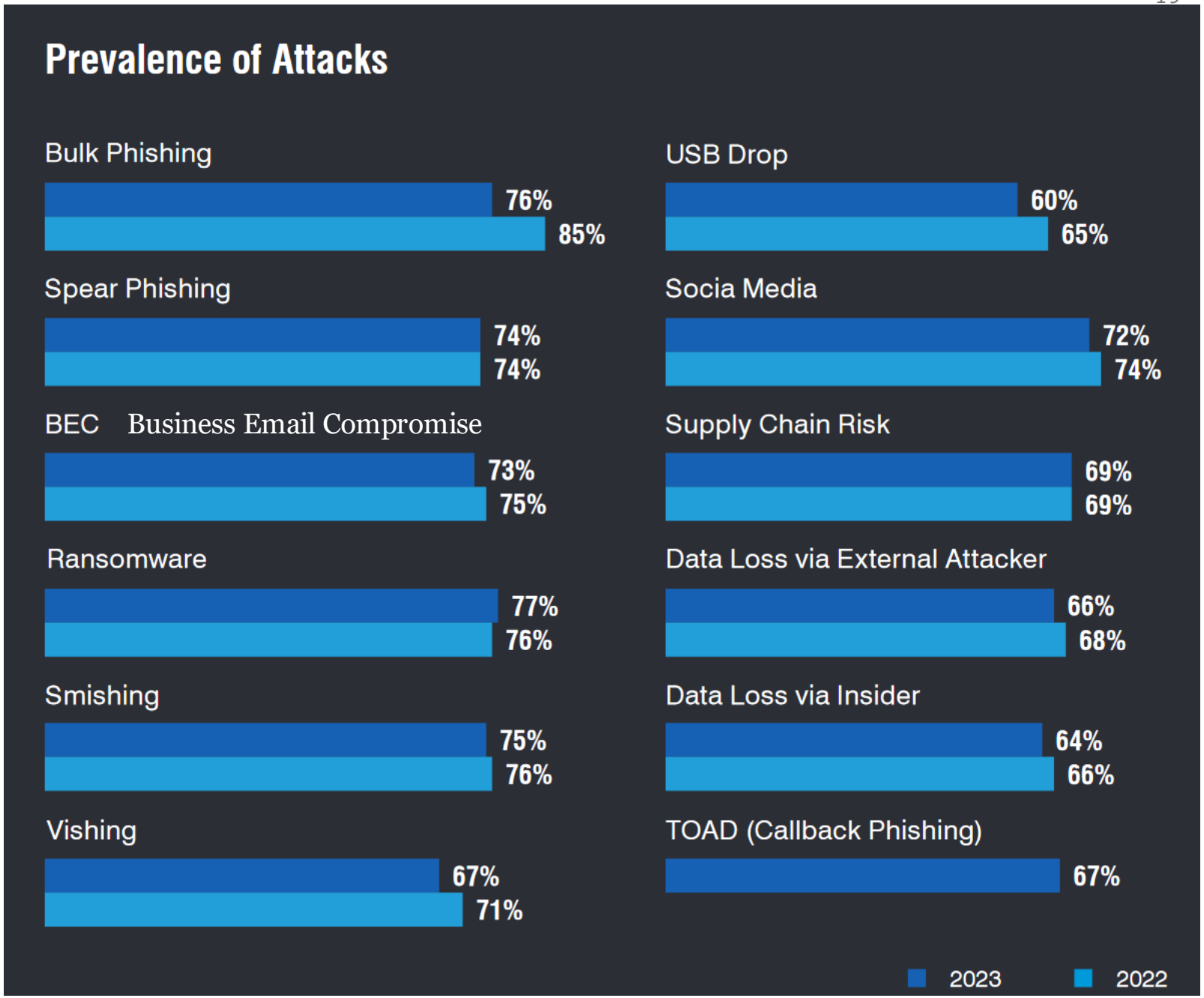
Users knowingly take risky actions

Proofpoint, 2024 State of the Phish

89% believe that MFA provides complete protection



Many types of phishing attacks can lead to a security problem.



Proofpoint, 2024 State of the Phish

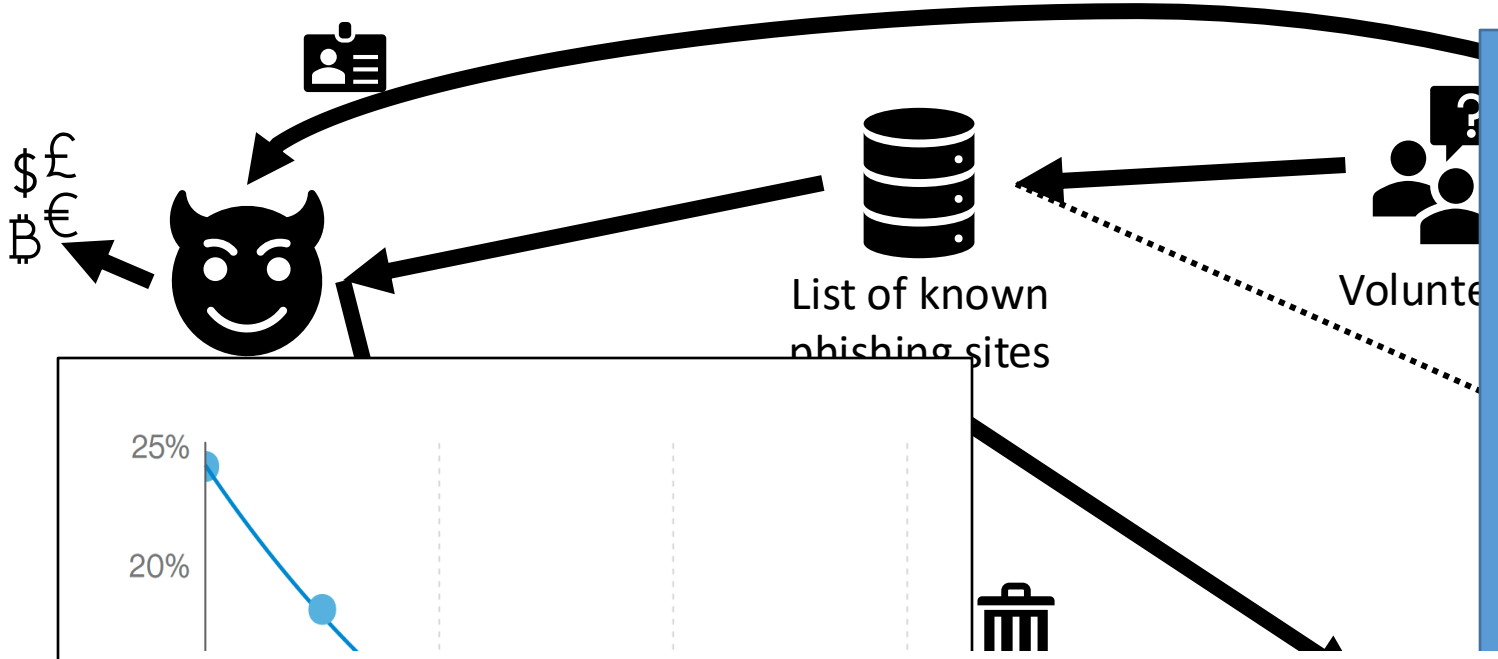
Phishing attacks are expensive

Proofpoint, 2024 State of the Phish

Who is responsible for security?

Proofpoint, 2024 State of the Phish

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

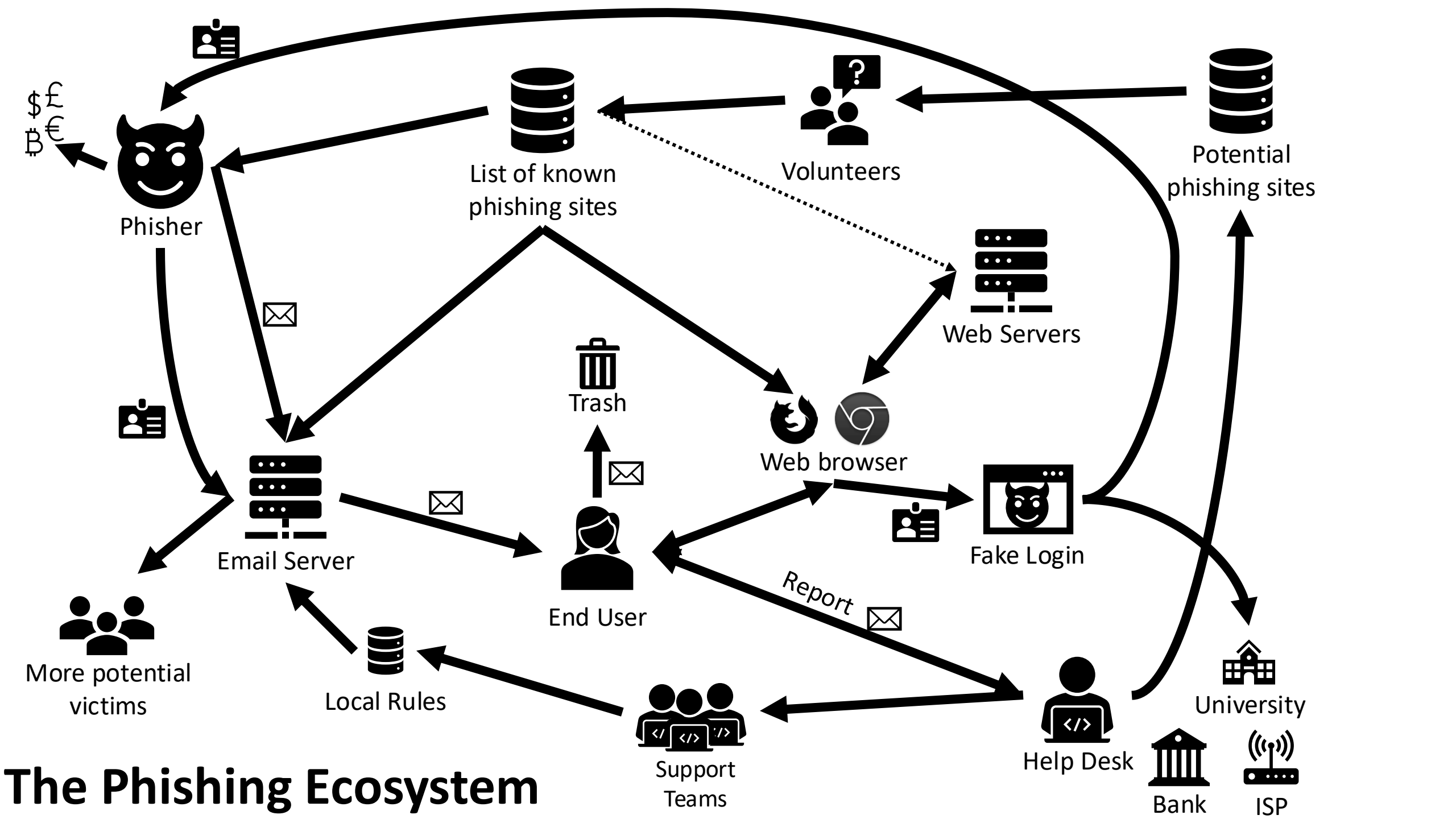
APWG. Phishing Activity Trends Report, 2nd Quarter 2019.

Report. p16

Verizon. 2019 Data Breach Investigation Report. P32.

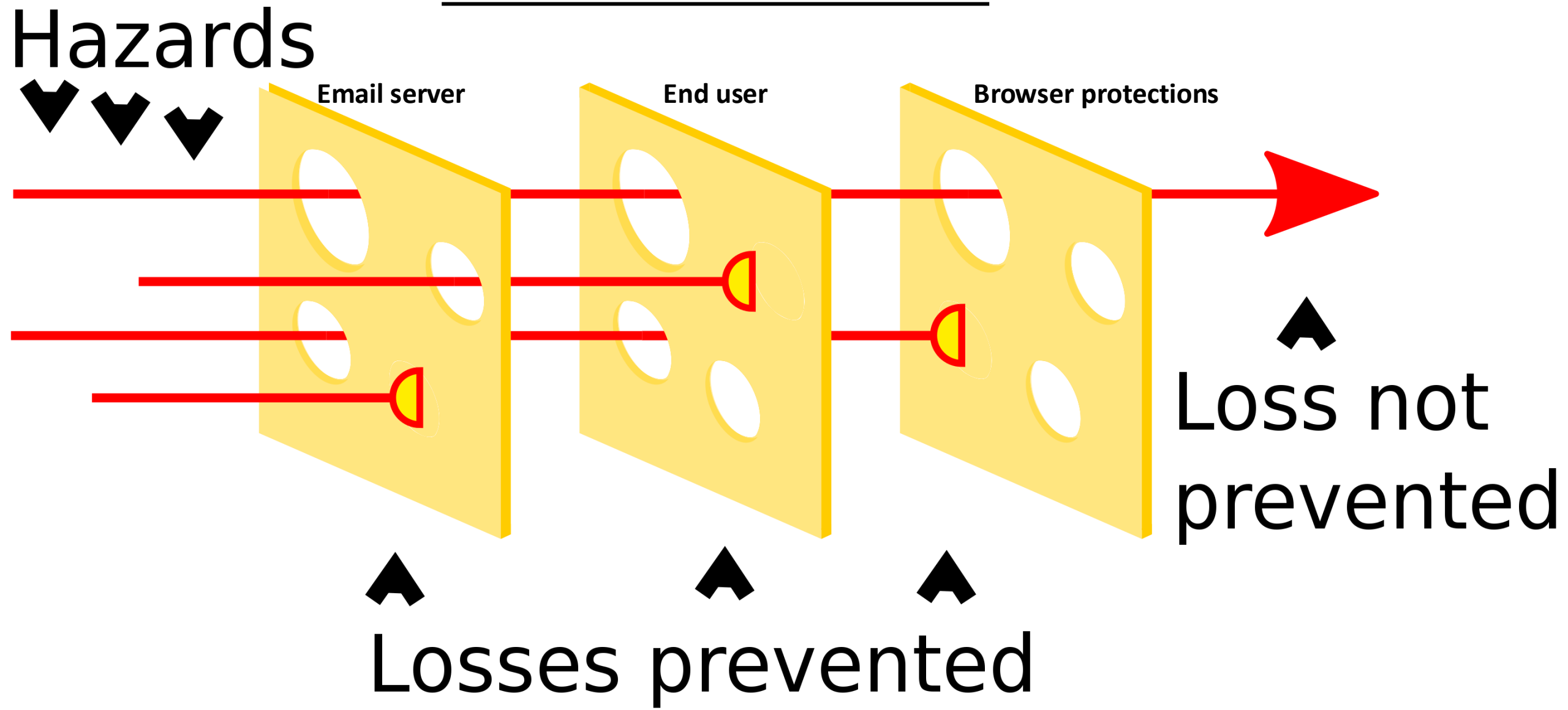
Bank ISP

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”

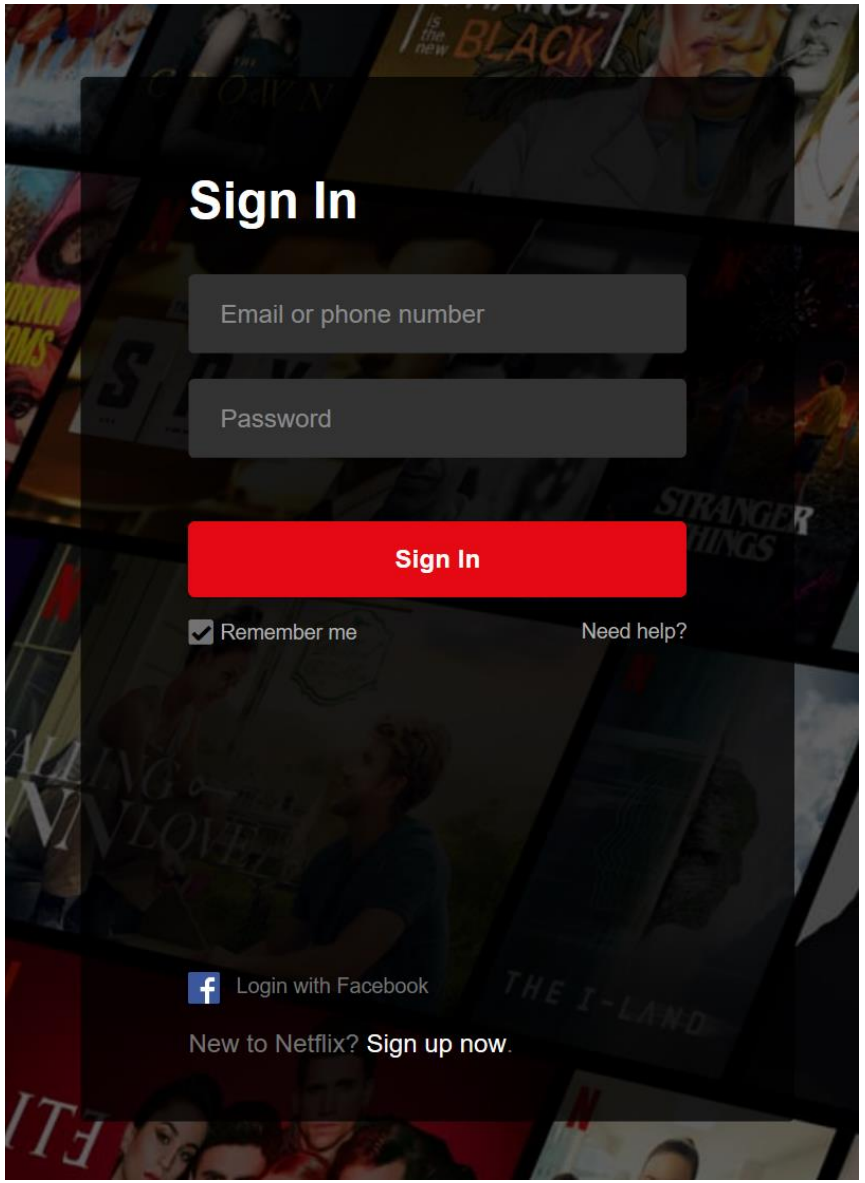
- Automatically block attacks using filters
  - Stop email from even arriving in inboxes
  - Block people from visiting known bad websites
- Train users
  - Provide users with training on how to identify phishing attacks
- Support users
  - Show UI indicators to help users tell the difference between 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?

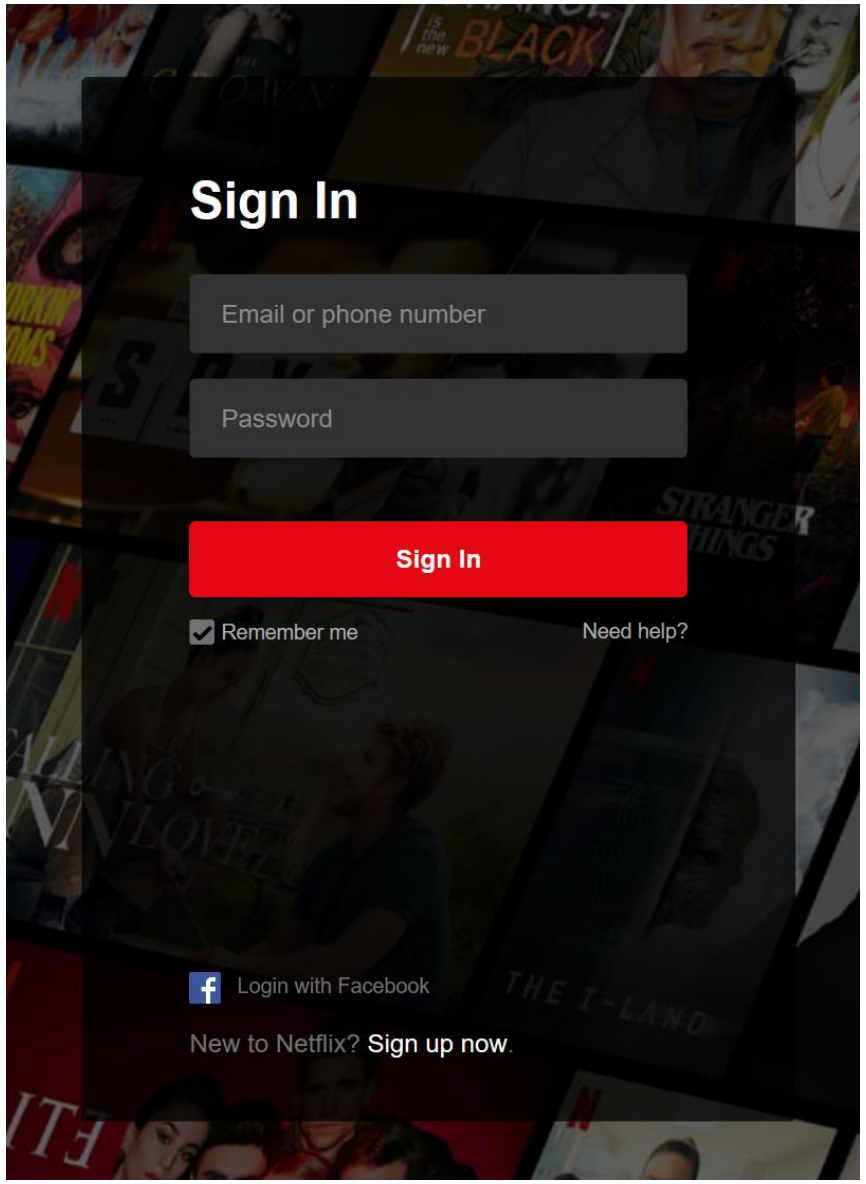
Authentication is very broken

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

We normally think of authentication as one directional

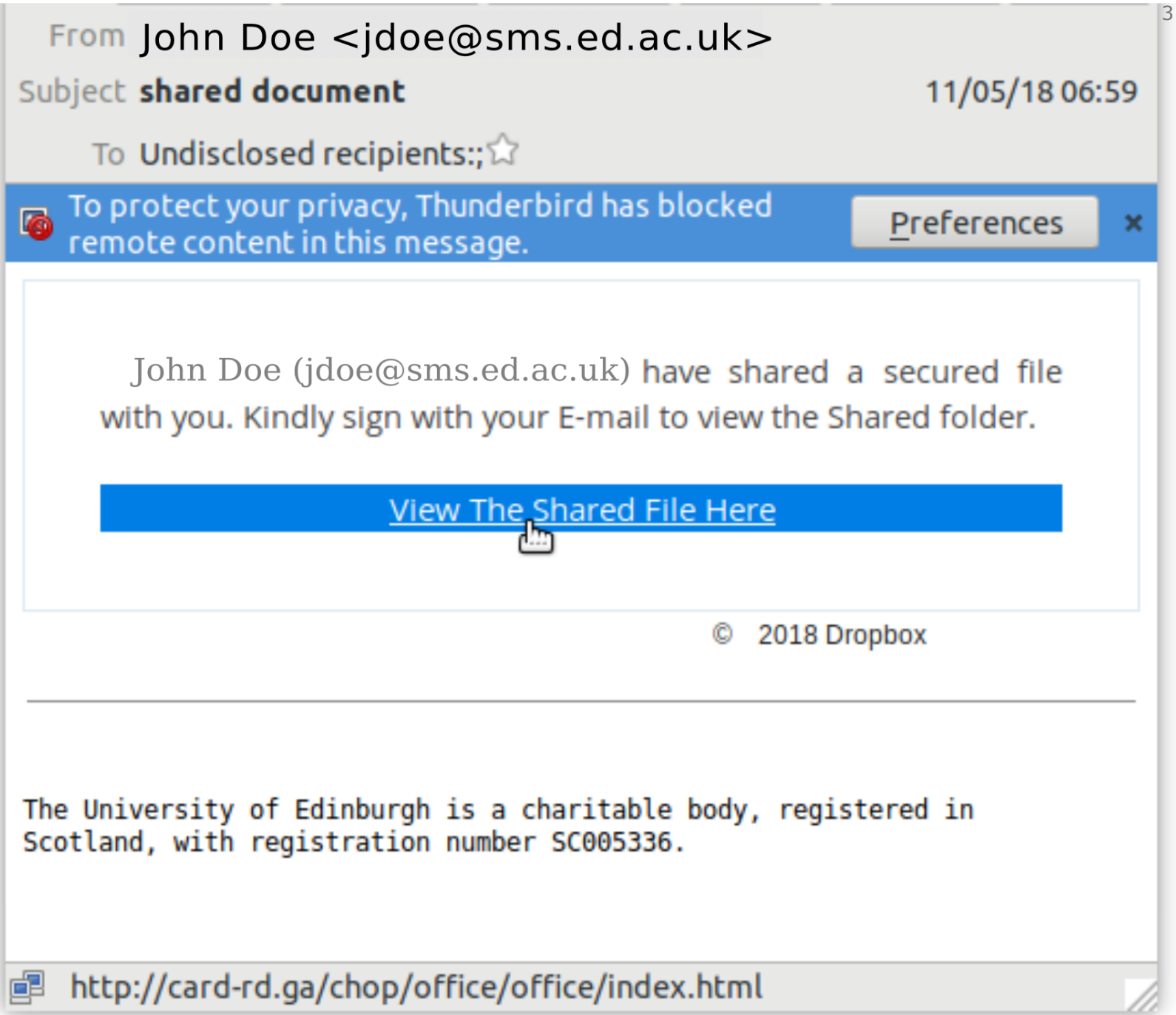


But it is actually two directional



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

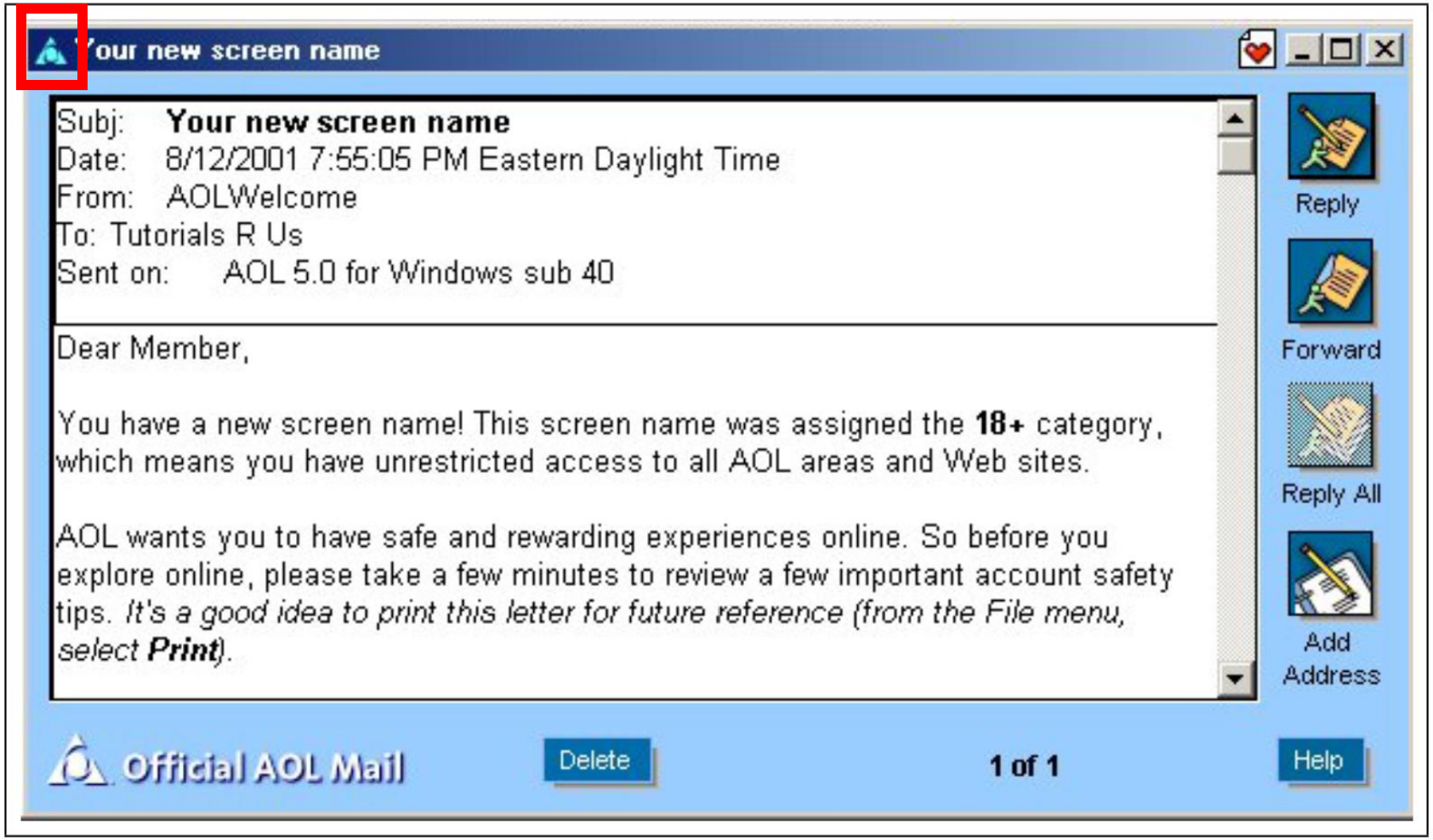
the easy-to-use software that made it the darling of computer novices, Prodigy sprinted another length ahead this week.

Modem speeds, which doubled and re-

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

AOHell

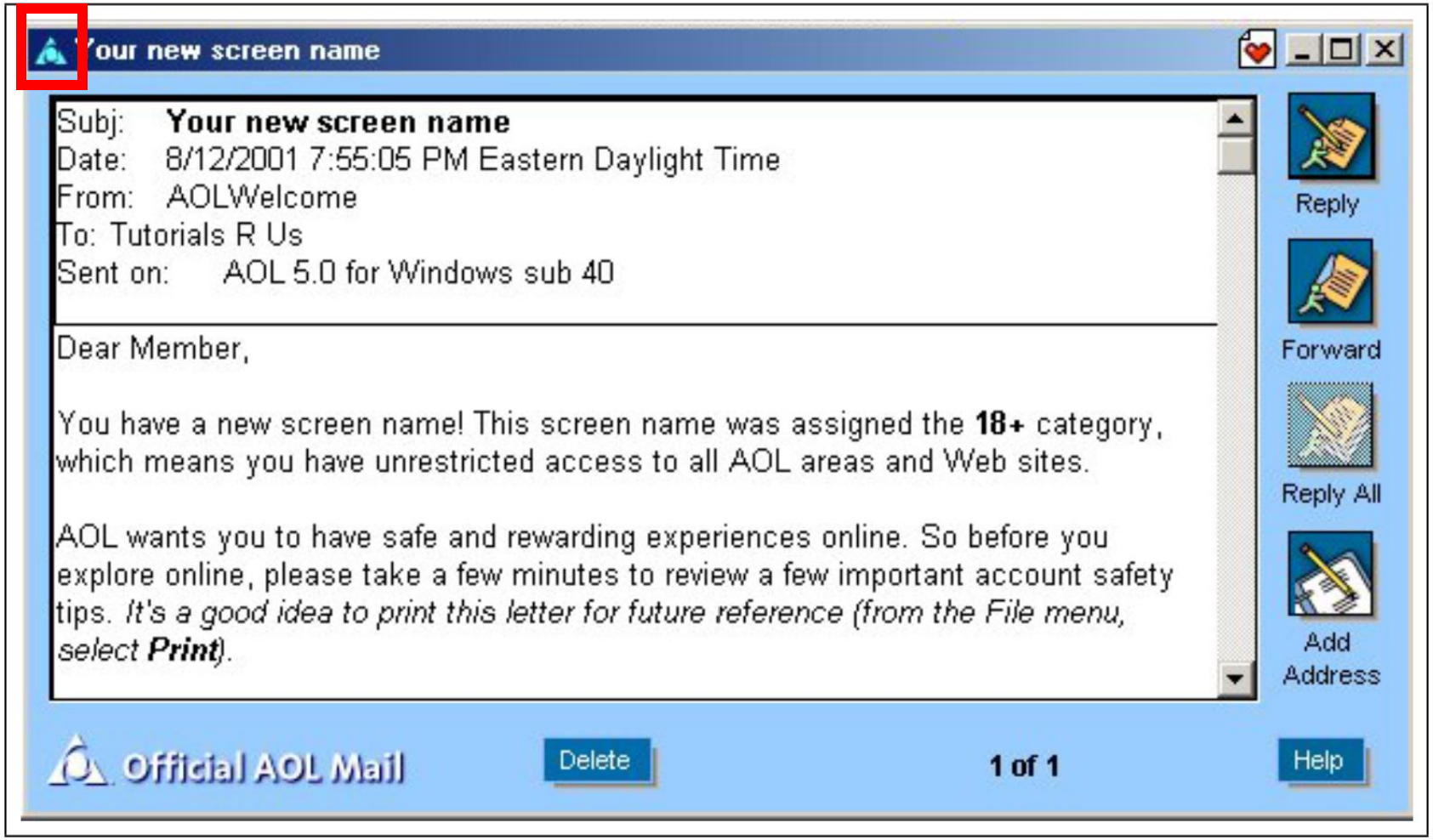
Then, AOL started using a blue icon to distinguish official AOL messages from other users' messages.



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

Passive Indicator

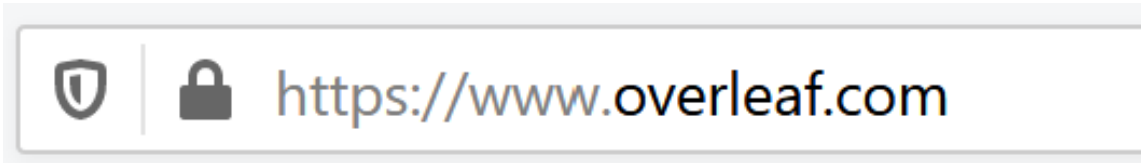
A UI element that provides information, but the user is not forced to look at or interact with.

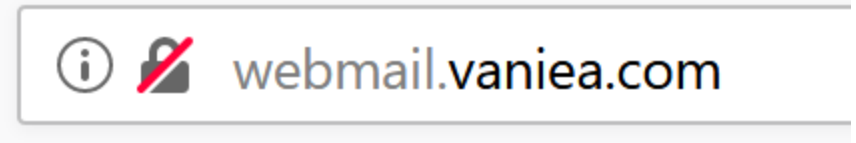


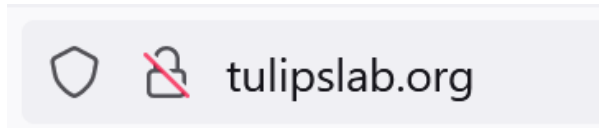
Garfinkel, Simson. Design principles and patterns for computer systems that are simultaneously secure and usable. 2005.

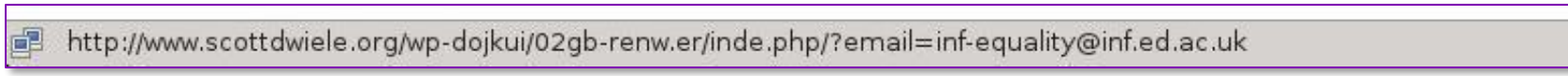
Passive Indicator

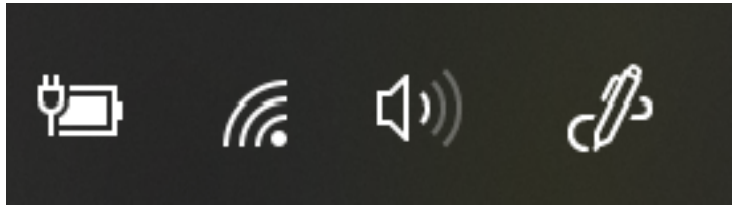
A UI element that provides information, but the user is not forced to look at or interact with.



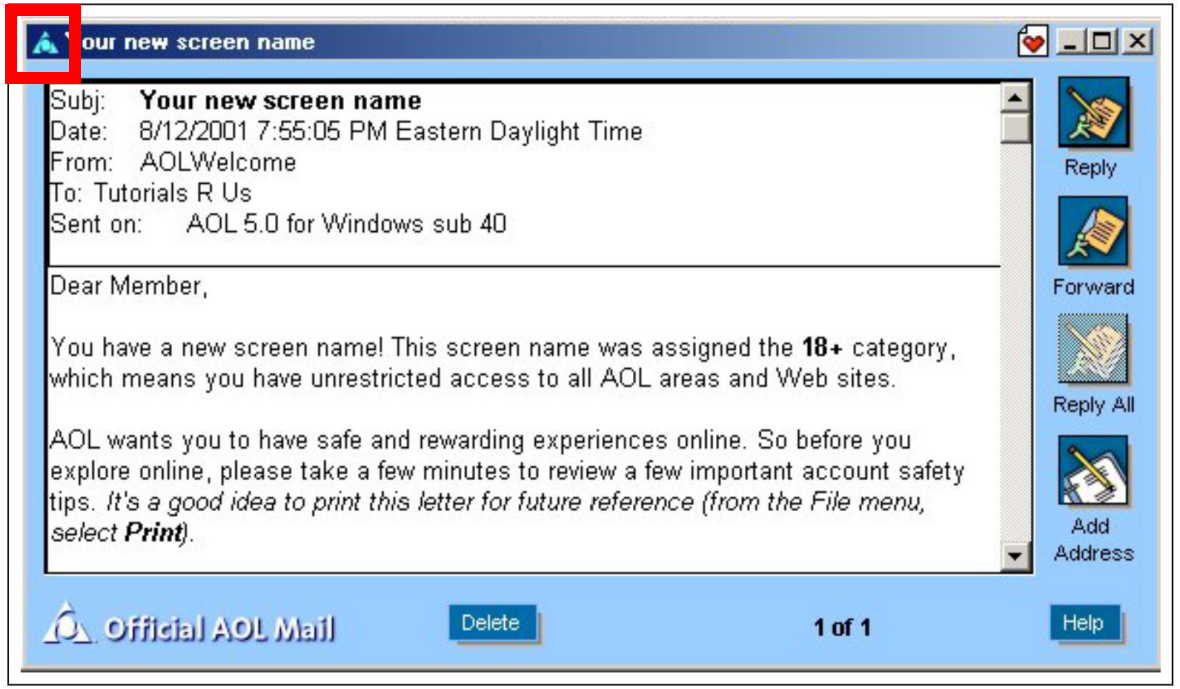




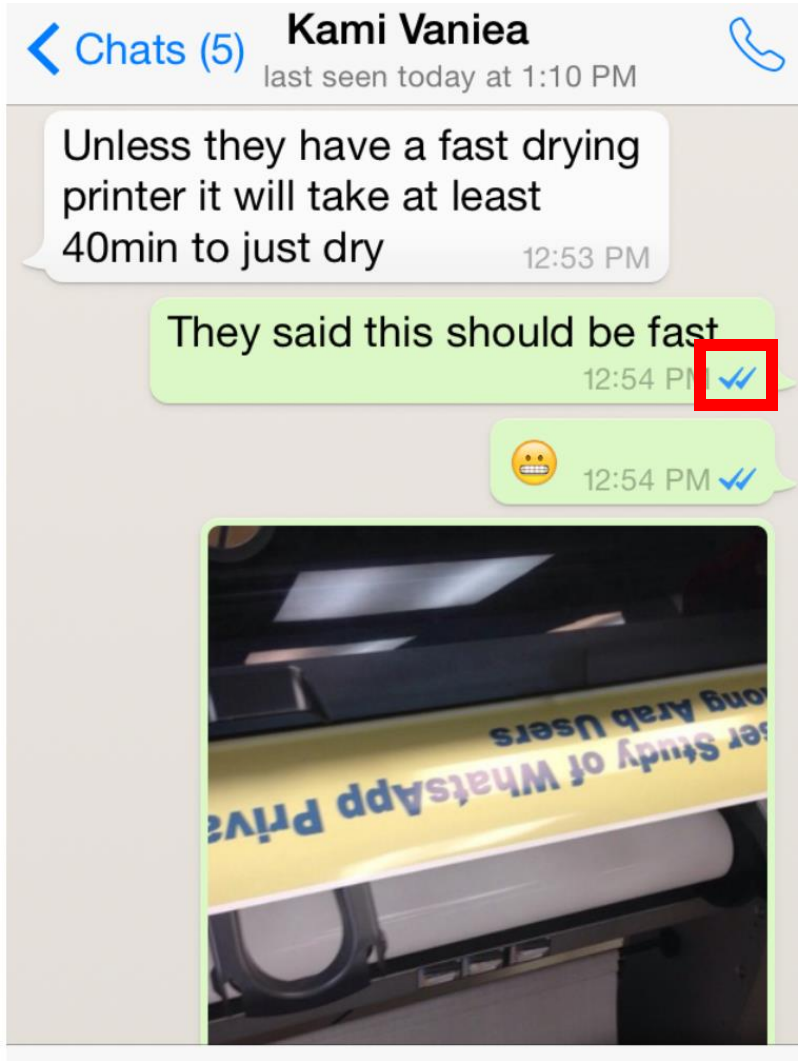




Passive indicators are used in many places and can drastically impact how we interpret information



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



2003: 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

2003: 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

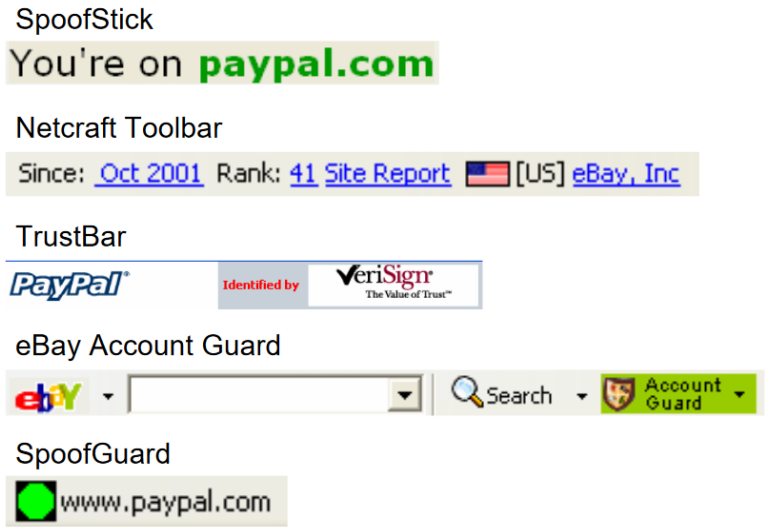


Figure 1. Existing security toolbars

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.

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

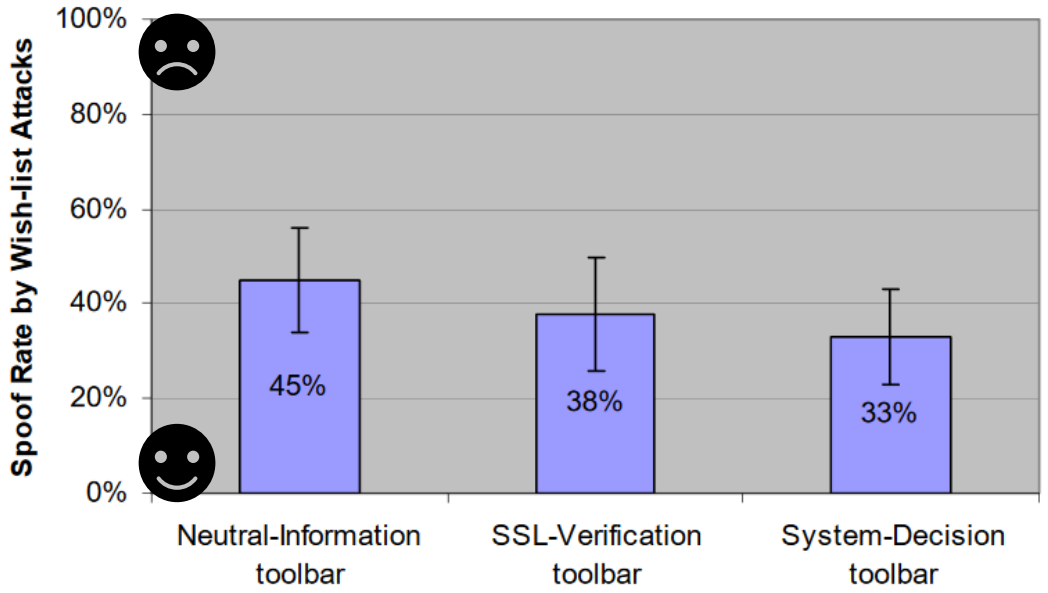


Figure 5. Spoof rates with different toolbars

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].

Passive security indicators were not working…

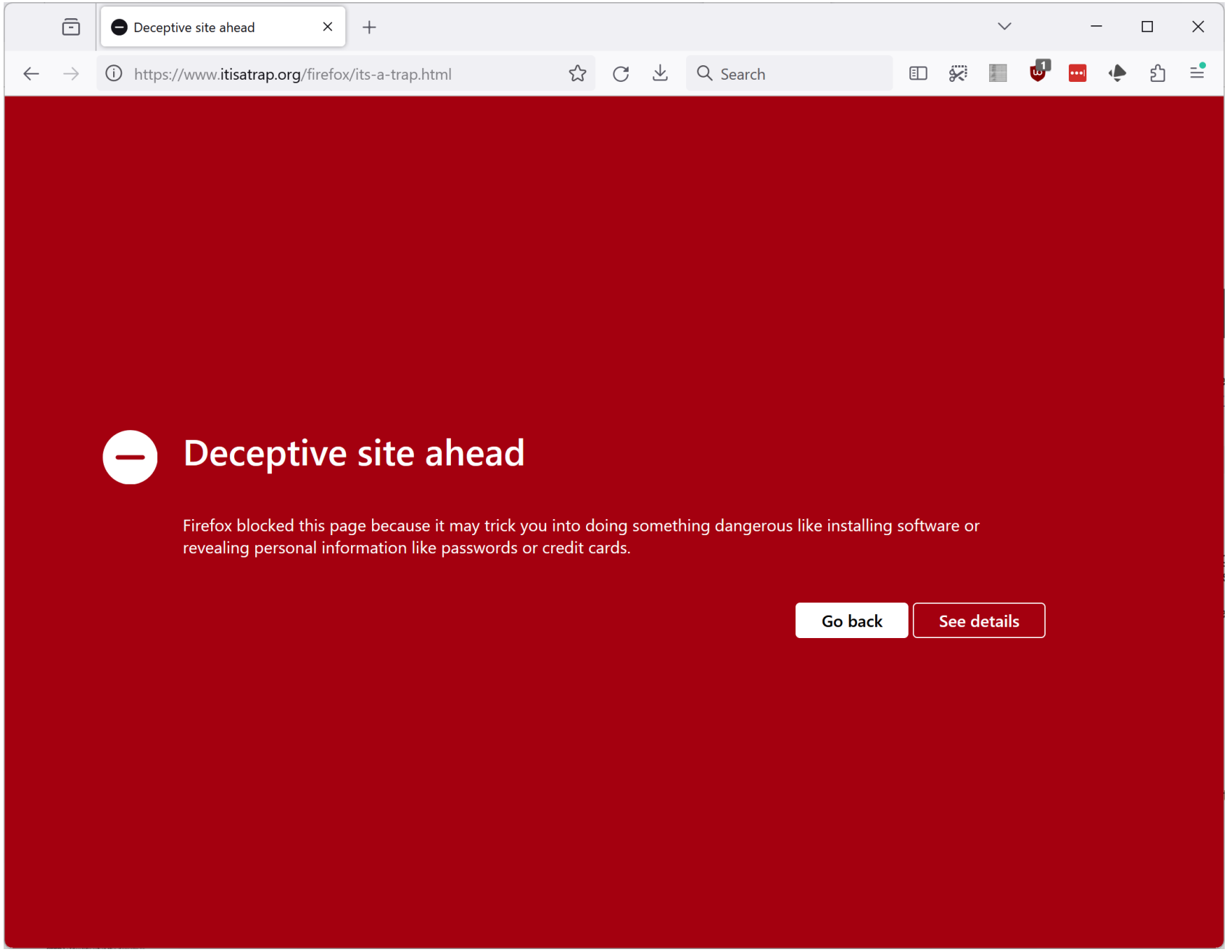
So indicators started getting more obvious and intrusive.

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.

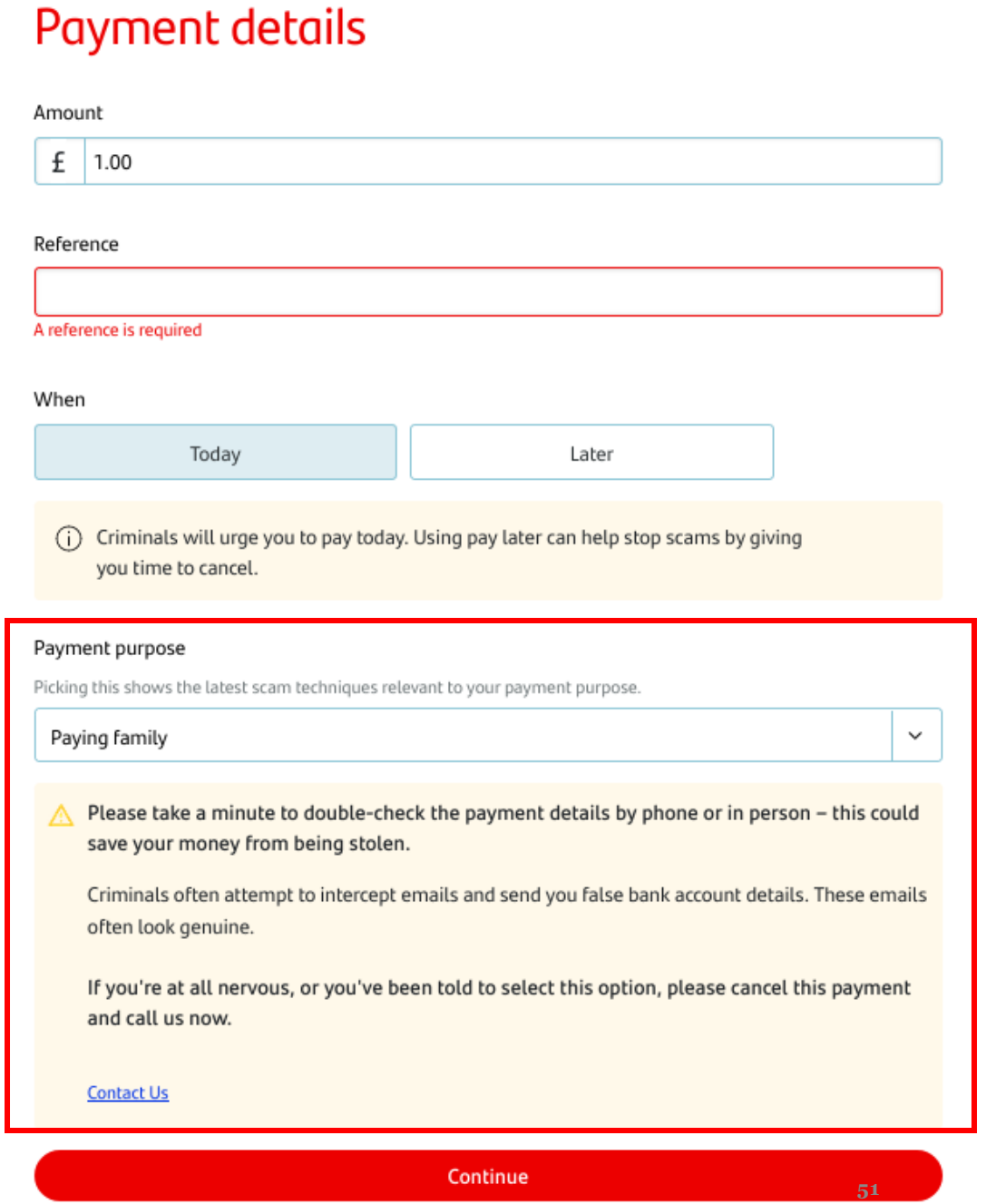
Condition Name	Size	Clicked	Phished
Firefox	20	20 (100%)	0 (0%)
Active IE	20	19 (95%)	9 (45%)
Passive IE	10	10 (100%)	9 (90%)
Control	10	9 (90%)	9 (90%)

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.

Active indicators are alive and well in 2024

- 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

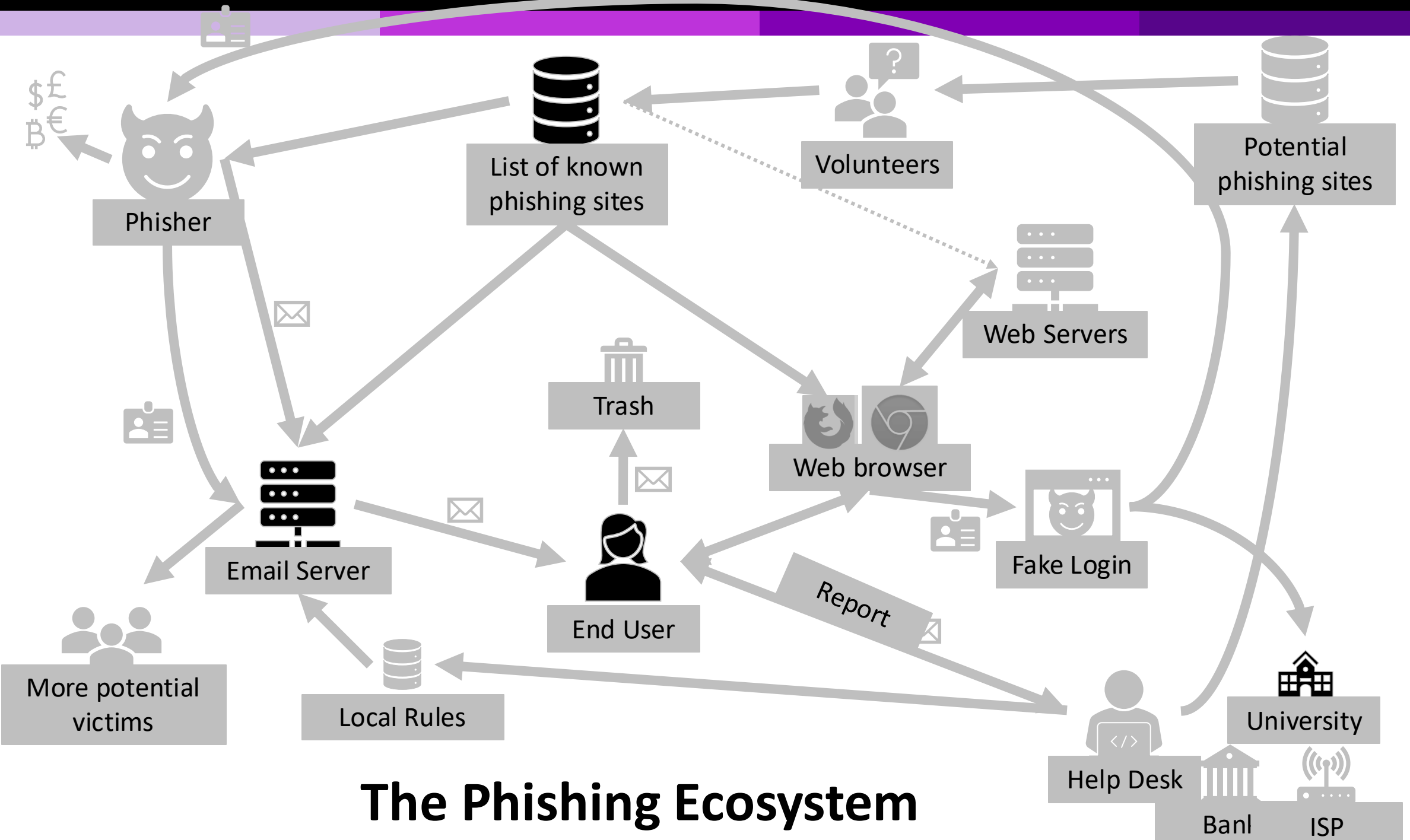
⚠ **Please take a minute to double-check the payment details by phone or in person – this could save your money from being stolen.**

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

SOLVING PHISHING



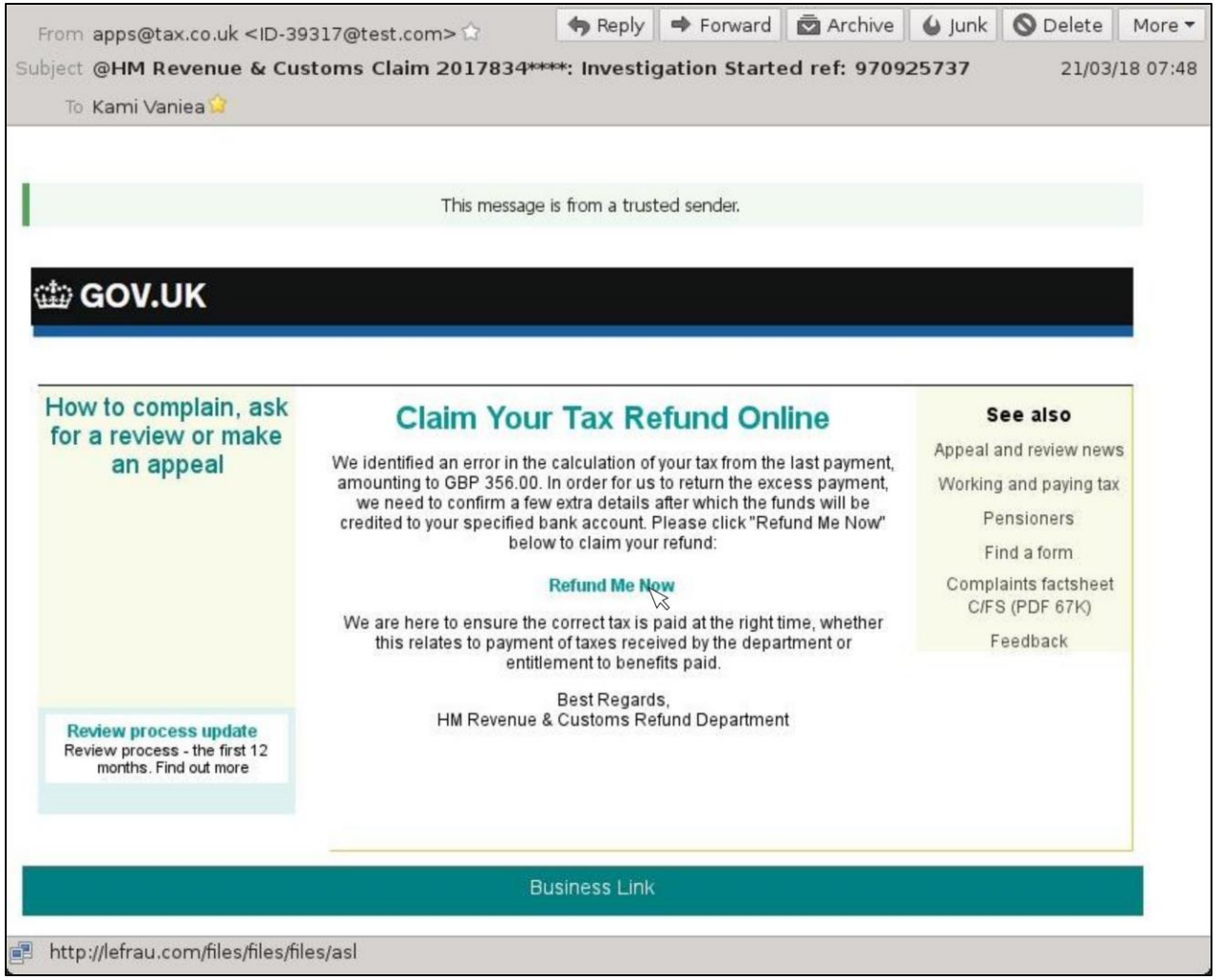
The Phishing Ecosystem

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

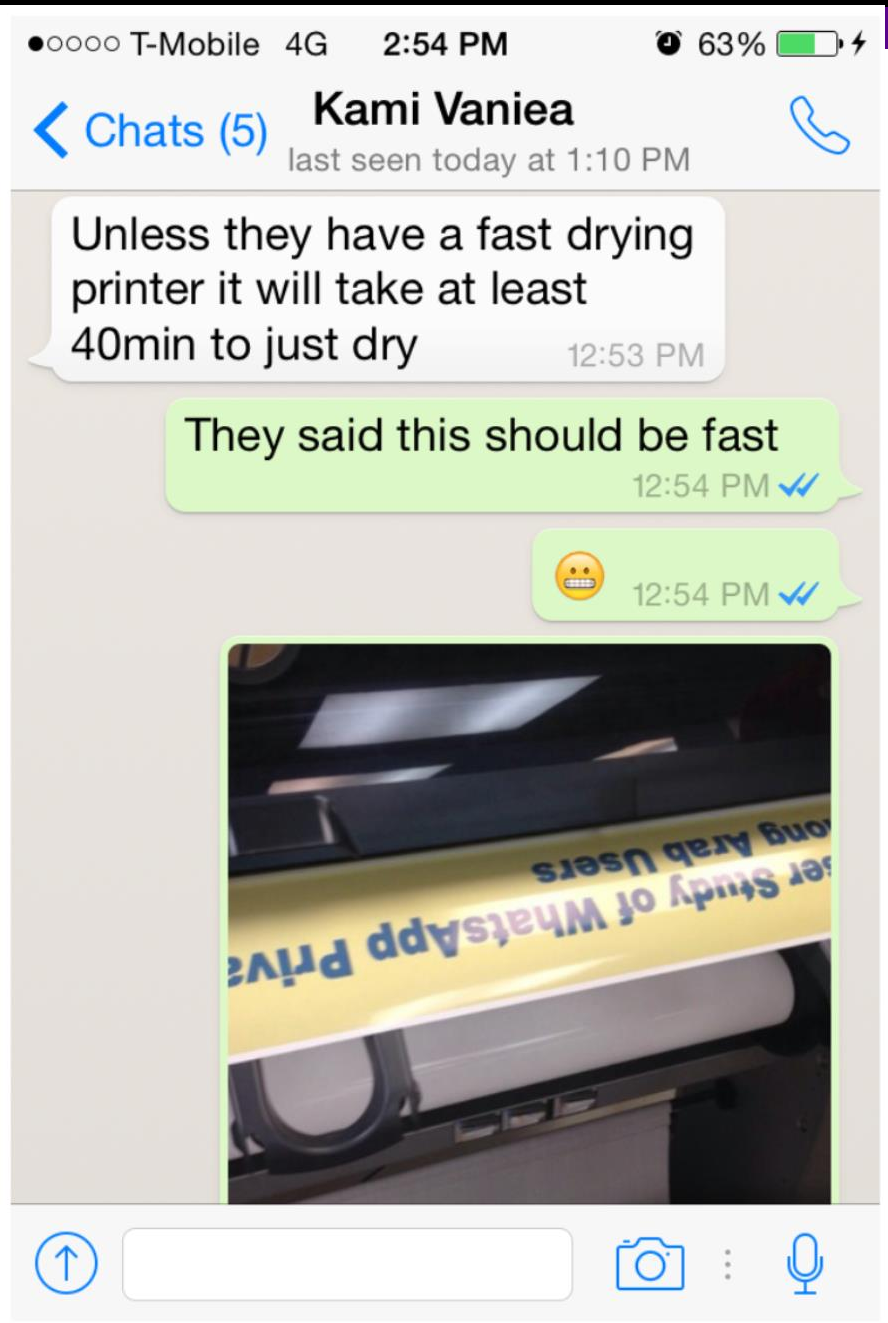
Automation

- Automatically scan all incoming emails for features
  - Attachments for malware
  - URLs for links to phishing pages
  - Spoofed from addresses from highly targeted companies (Paypal)
- Low tolerance for errors
- Low delay also important



Automation + Encryption

- "Going dark" due to encryption isn't just a problem for law enforcement.
- Encryption also makes scanning for phishing more challenging.
- Do users know that their more private WhatsApp chats may have more dangerous content than in web browsers or emails?



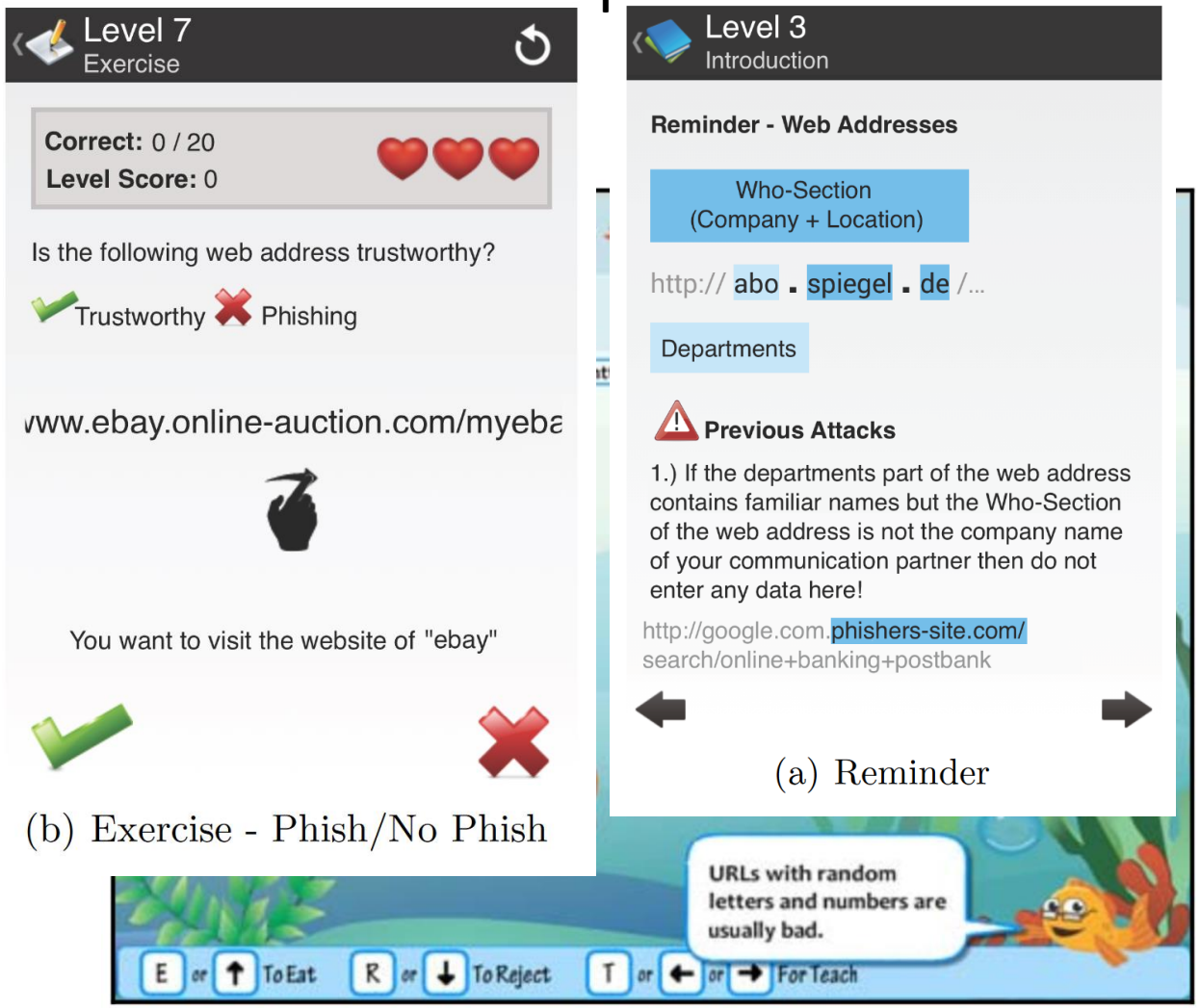
Main “solutions”

- 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

Training users

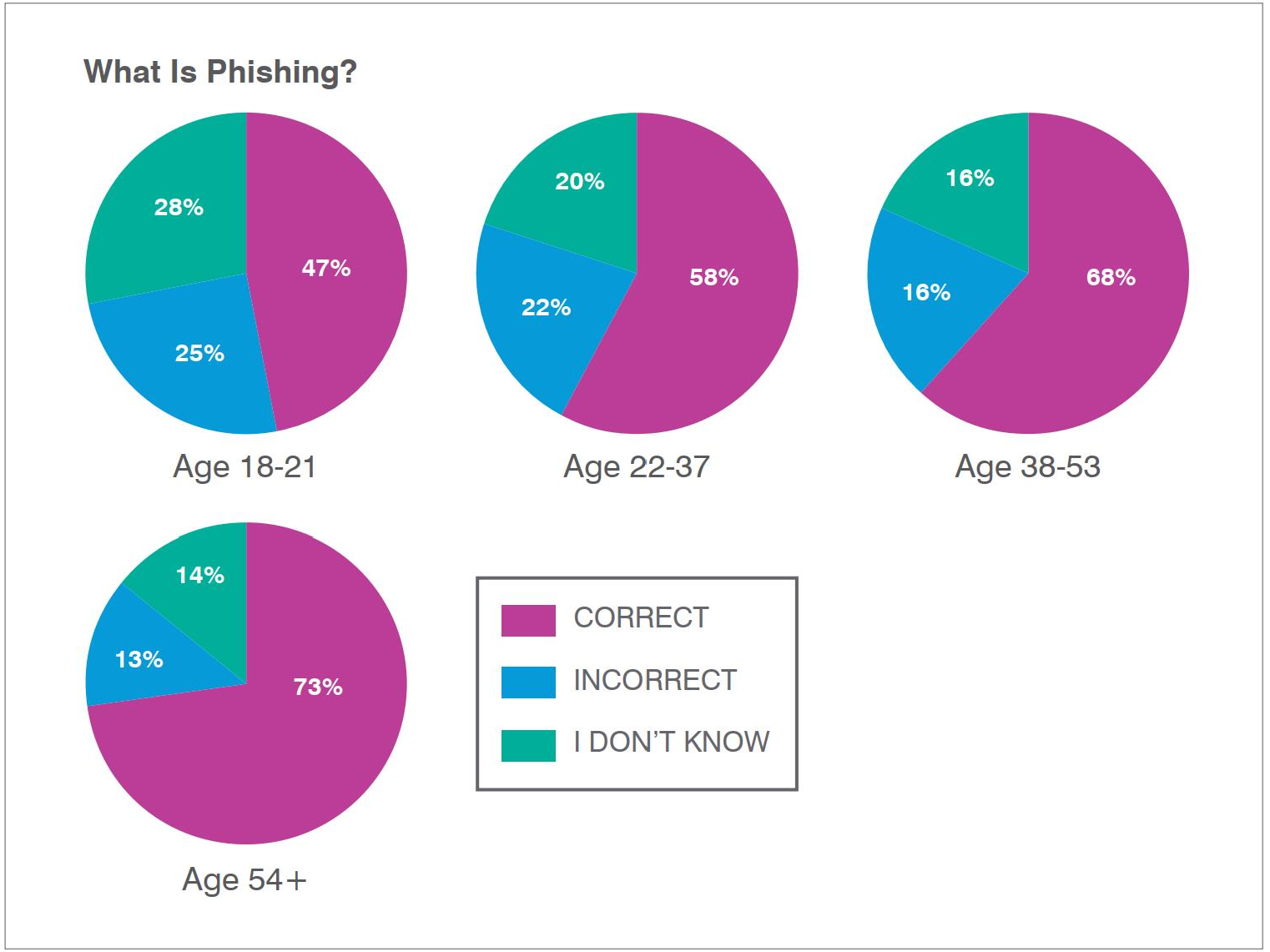
- Up-front training
  - Games
  - Advice web pages
  - Training videos
- Embedded training
  - Information provided in websites
  - Feedback given by help desk to phishing reports
- Evaluate impact of training
  - Send out fake phishing emails to test staff
  - Measure reporting behaviors

NoPhish anti-phishing training app



The older generation is surprisingly aware of phishing as compared to younger people.

The difference is likely due to life experience with fraud.



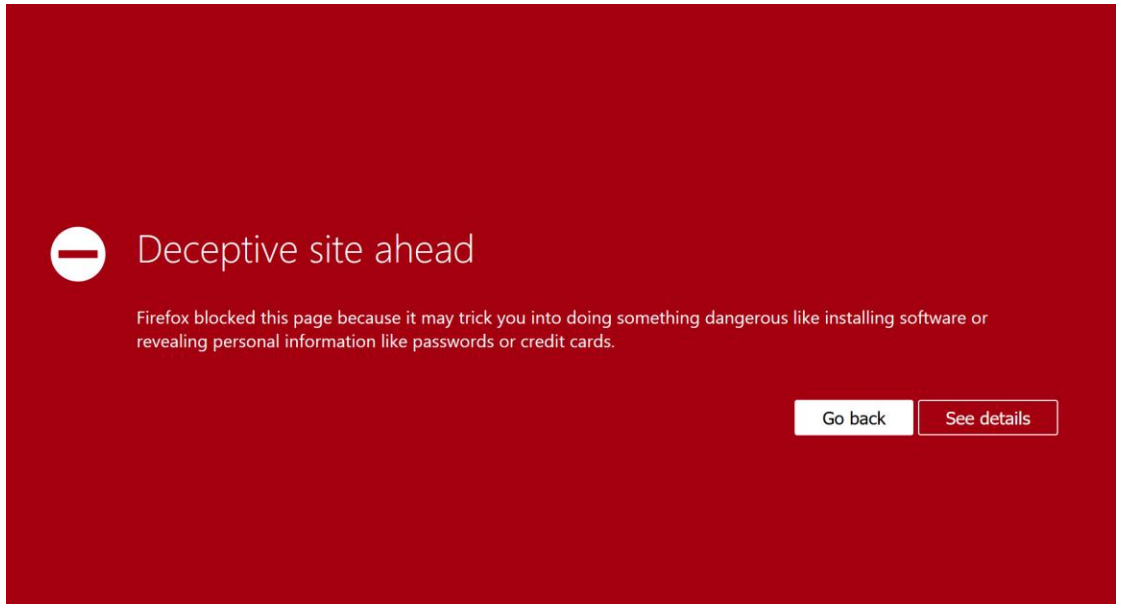
Note: According to Pew Research, millennials fell into the 22-37 age bracket and baby boomers were 54 and older in 2018.

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

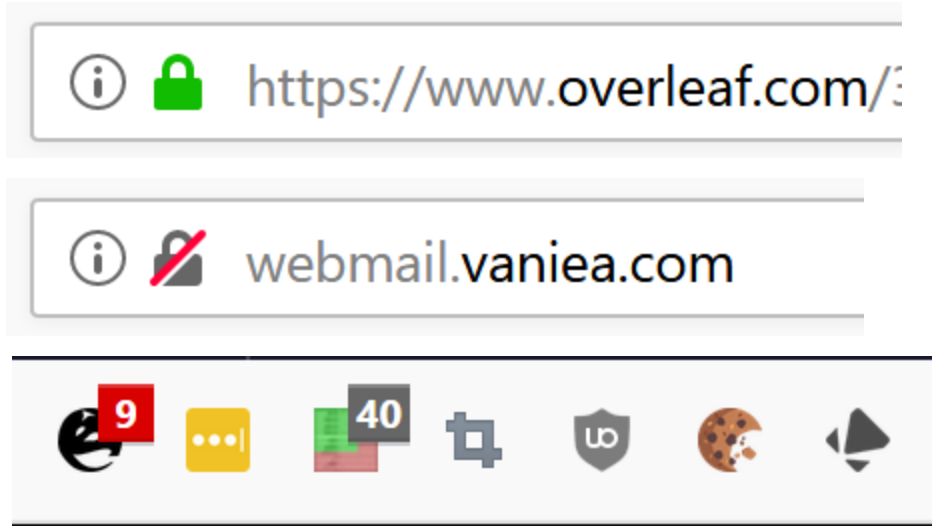
Managing phishing

- Block people from visiting sites
  - Browser blocks sites automatically
  - ISPs take down sites
- Provide indicators to help people differentiate between intended and malicious websites
  - Lock icon
  - Plugins with feedback
  - Show only the URL domain to reduce confusion
  - Stating what email server sent an email

Active Warning



Passive Warnings



A well designed phishing site fools 90% of people. Security cues in the browser are not seen, ignored, or not understood.

Why Phishing Works

Rachna Dhamija
rachna@deas.harvard.edu
Harvard University

J. D. Tygar
tygar@berkeley.edu
UC Berkeley

Marti Hearst
hearst@sims.berkeley.edu
UC Berkeley

ABSTRACT

To build systems shielding users from fraudulent (or *phishing*) websites, designers need to know which attack strategies work and why. This paper provides the first empirical evidence about which malicious strategies are successful at deceiving general users. We first analyzed a large set of captured phishing attacks and developed a set of hypotheses about why these strategies might work. We then assessed these hypotheses with a usability study in which 22 participants were shown 20 web sites and asked to determine which ones were fraudulent. We found that 23% of the participants did not look at browser-based cues such as the address bar, status bar and the security indicators, leading to incorrect choices 40% of the time. We also found that some visual deception attacks can fool even the most sophisticated users. These results illustrate that standard security indicators are not effective for a substantial fraction of users, and suggest that alternative approaches are needed.

Author Keywords

Security Usability, Phishing.

ACM Classification Keywords

H.1.2 [User/Machine Systems]: Software psychology; K.4.4 [Electronic Commerce]: Security.

INTRODUCTION

What makes a web site credible? This question has been addressed extensively by researchers in computer-human interaction. This paper examines a twist on this question: what makes a *bogus* website credible? In the last two years, Internet users have seen the rapid expansion of a scourge on the Internet: *phishing*, the practice of directing users to fraudulent web sites. This question raises fascinating questions for user interface designers, because both phishers and anti-phishers do battle in user interface space. Successful phishers must not only present a high-credibility web presence to their victims; they must create a presence that is so impressive that it causes the victim to fail to recognize security measures installed in web browsers.

Data suggest that some phishing attacks have convinced up to 5% of their recipients to provide sensitive information to spoofed websites [21]. About two million users gave information to spoofed websites resulting in direct losses of $1.2 billion for U.S. banks and card issuers in 2003 [20].[1]

If we hope to design web browsers, websites, and other tools to shield users from such attacks, we need to understand which attack strategies are successful, and what proportion of users they fool. However, the literature is sparse on this topic.

This paper addresses the question of why phishing works. We analyzed a set of phishing attacks and developed a set

Managing phishing

- **Make it invisible**
  - Auto filter emails (Email provider)
  - Block phishing sites (ISP, browser, plugins)
  - Take down the phishing sites
- Better interfaces
  - Passive indicators
  - Active indicators
  - Better match to workflows and needs
- Train the user
  - Up-front training
  - Embedded training

QUESTIONS?