

ECE458/ECE750T27: Computer Security

Phishing

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



UNIVERSITY OF
WATERLOO

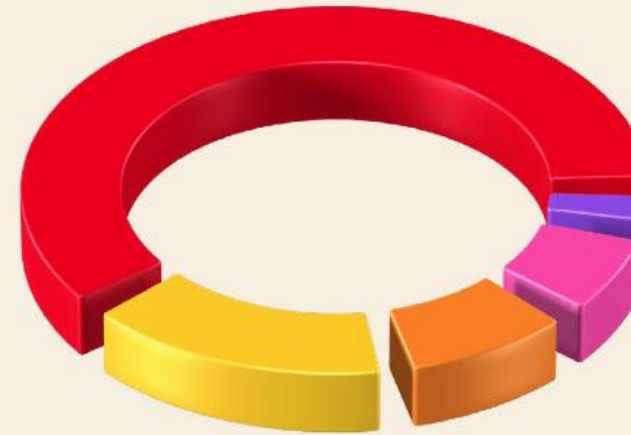
FACULTY OF
ENGINEERING



PHISHING: AN OVERVIEW

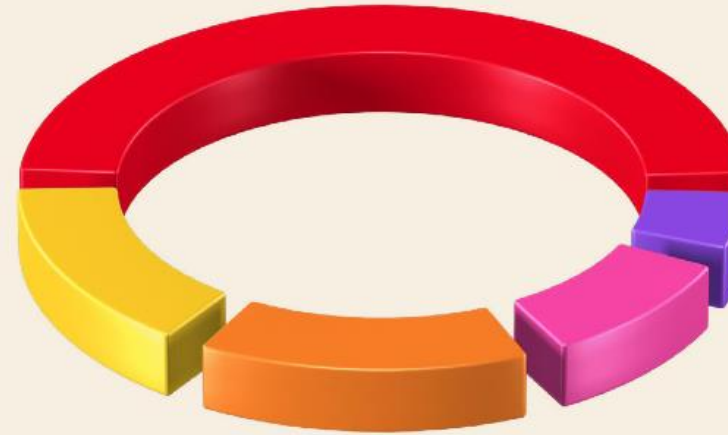
Causes of data breach

2026



- 61%** System Intrusion
- 17%** Social Engineering
- 10%** Basic Web Application Attacks
- 8%** Miscellaneous Errors
- 3%** Privilege Misuse

2025



- 53%** System Intrusion
- 18%** Basic Web Application Attacks
- 17%** Social Engineering
- 12%** Miscellaneous Errors
- 7%** Privilege Misuse

2024



- 36%** System Intrusion
- 25%** Miscellaneous Errors
- 22%** Social Engineering
- 9%** Basic Web Application Attacks
- 8%** Privilege Misuse

Initial access vectors

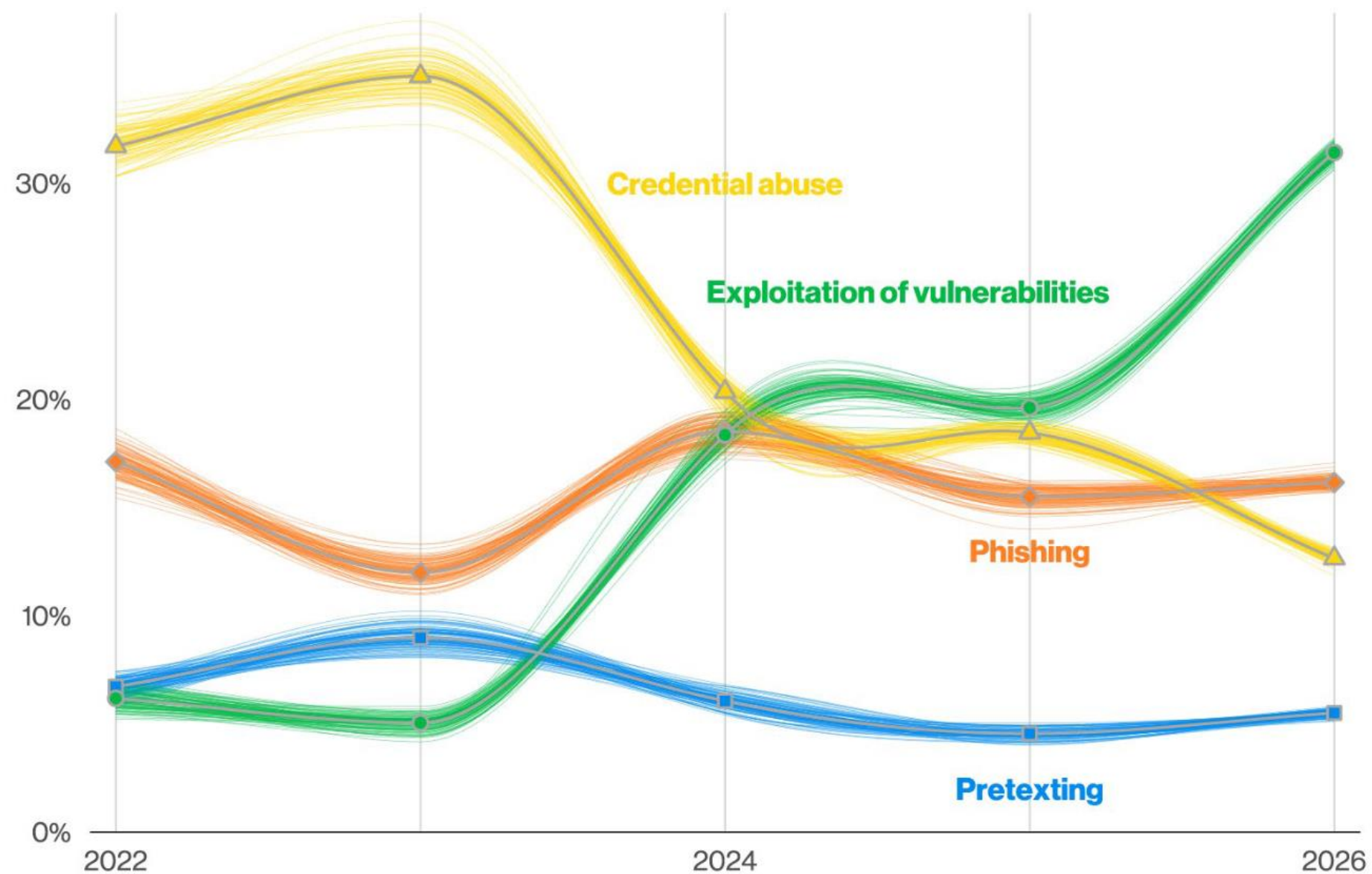
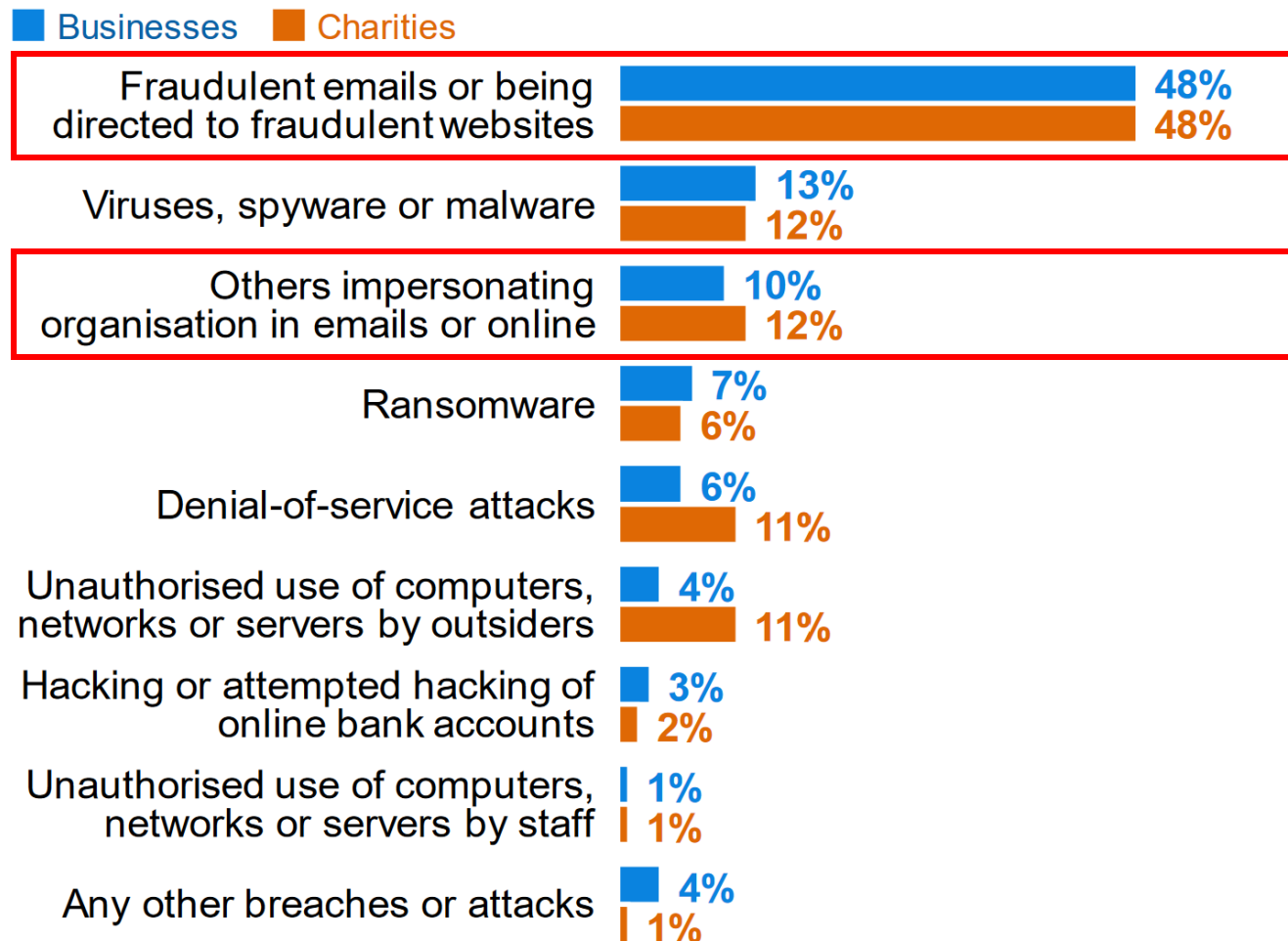


Figure 5. Known initial access vectors in non-Error, non-Misuse breaches over time (n for 2026 dataset=19,905)

Phishing is very common and very disruptive to 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?



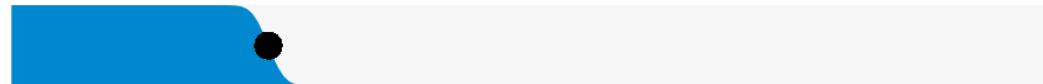
Bases: 778 businesses that identified a breach or attack in the last 12 months; 218 charities

Commonalities among breaches in 2018.

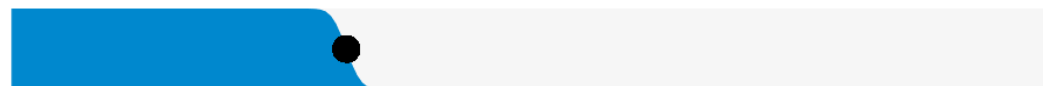
71% of breaches were financially motivated



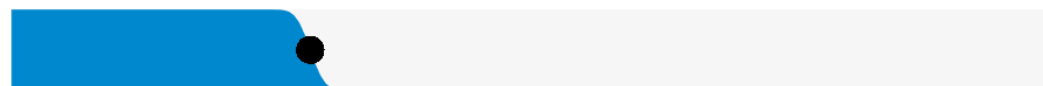
25% of breaches were motivated by the gain of strategic advantage (espionage)



32% of breaches involved phishing



29% of breaches involved use of stolen credentials



56% of breaches took months or longer to discover



0% 20% 40% 60% 80% 100%

Breaches

Figure 5. What are other commonalities?

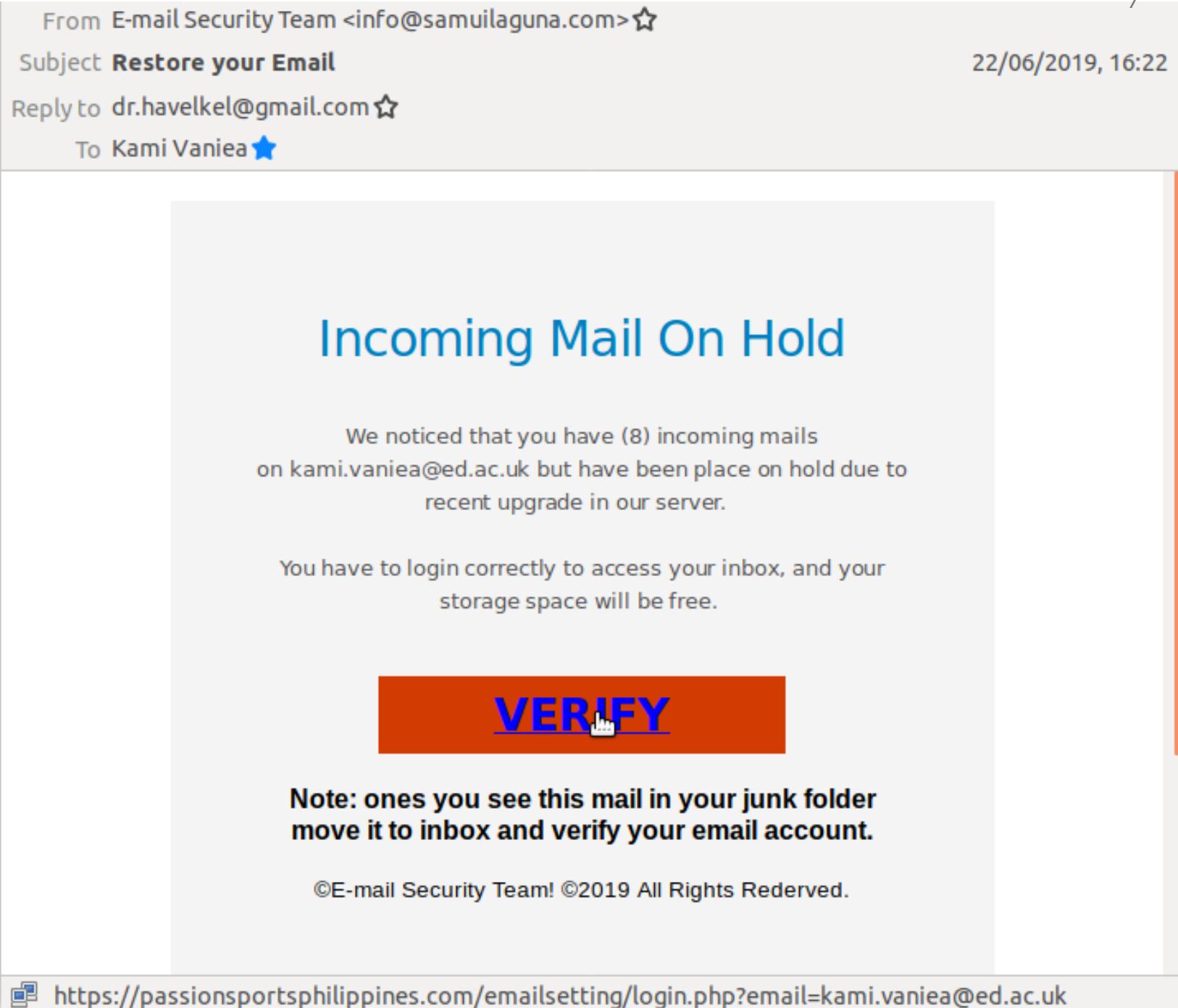
This is a phishing email

Look real

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

But

- Wrong URL
- Wrong From



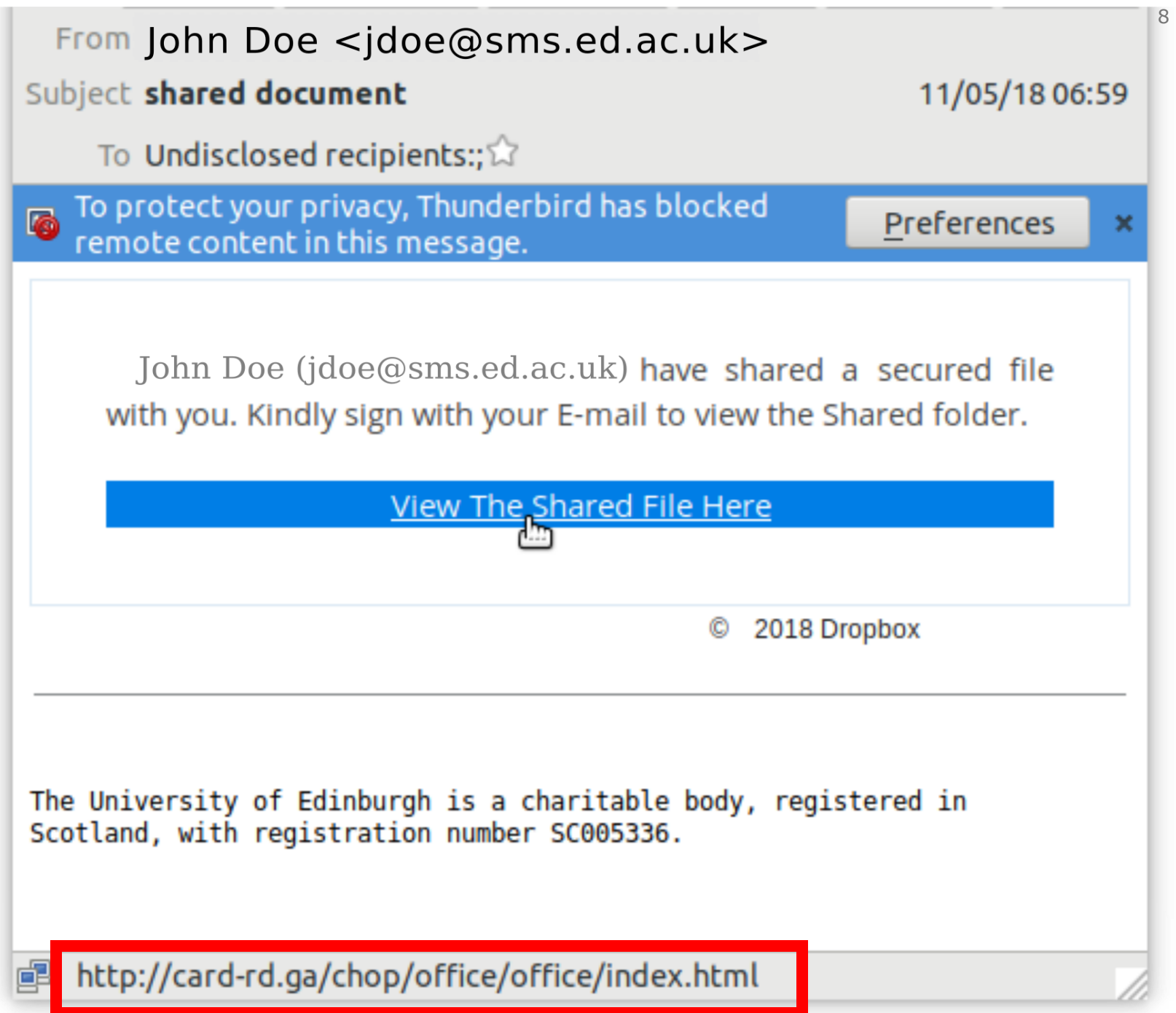
This is a phishing email

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,

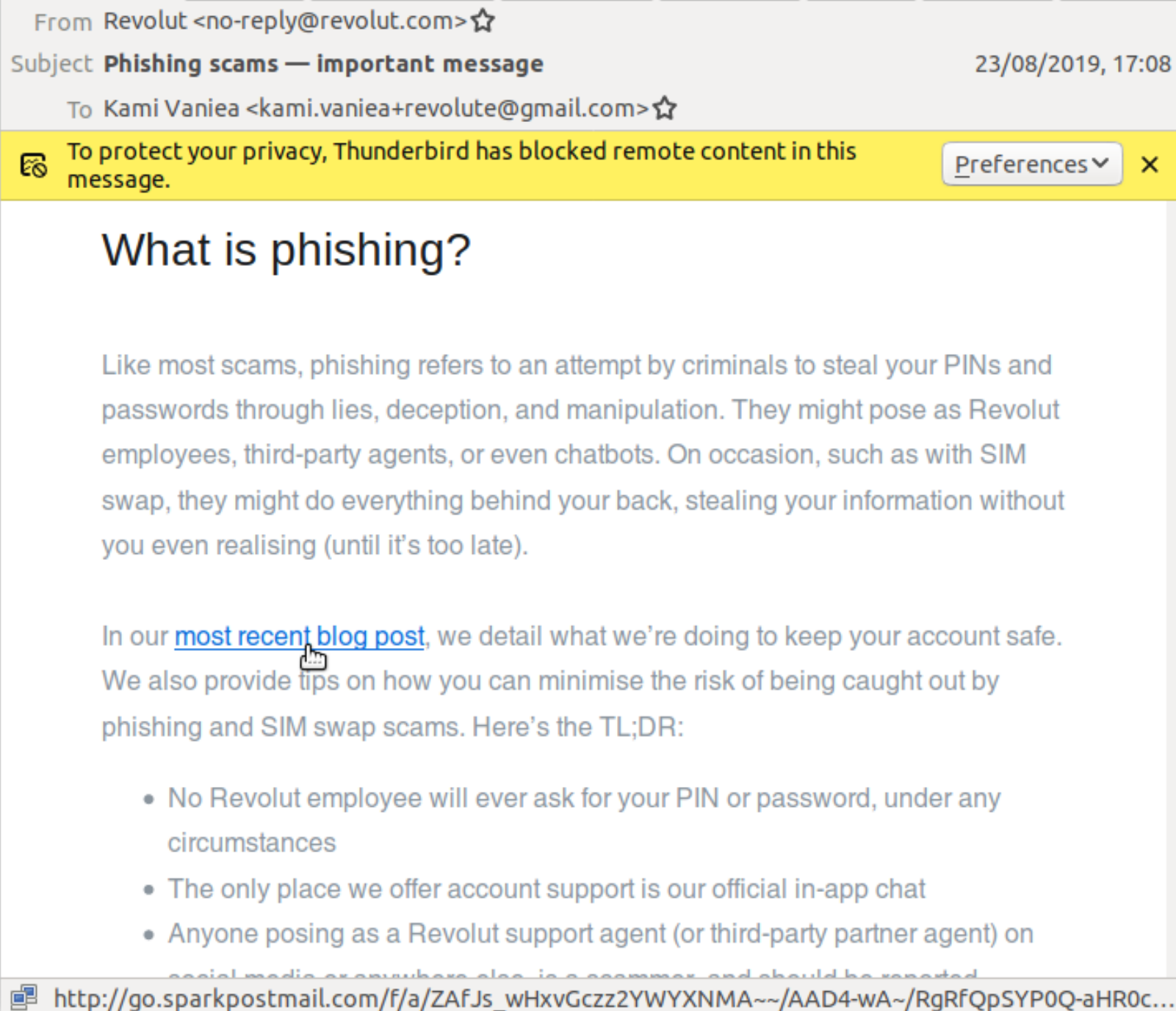
Your company LastPass invitation is still waiting. Please activate your account so you can start using LastPass Enterprise.

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



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)

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



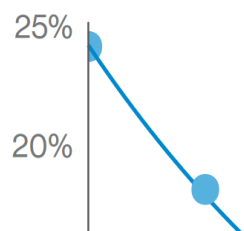
PHISHING ECOSYSTEM



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

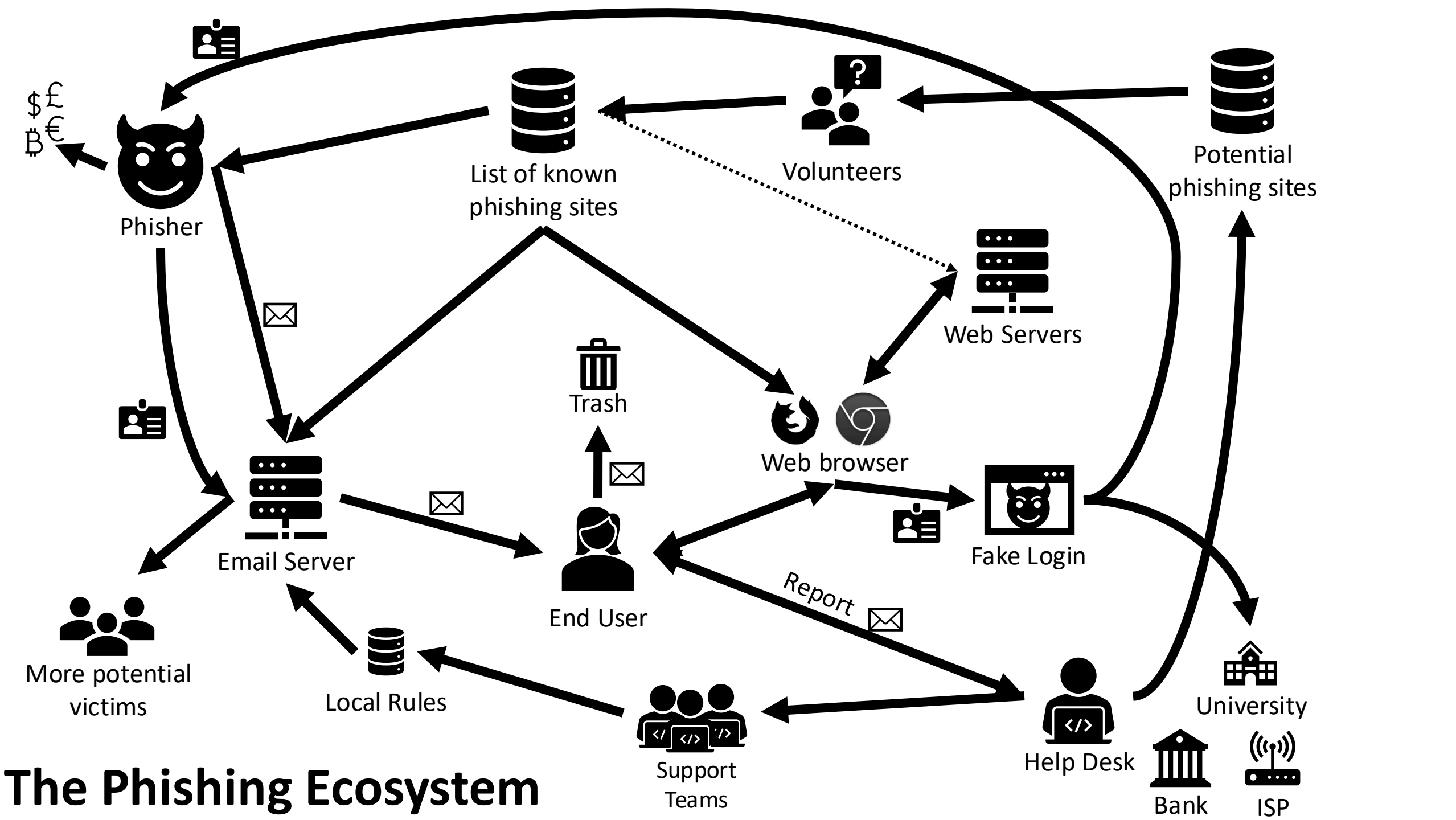
APWG. Phishing Activity Trends Report, 2nd Quarter 2019.

Report. p16

Verizon. 2019 Data Breach Investigation Report. P32.

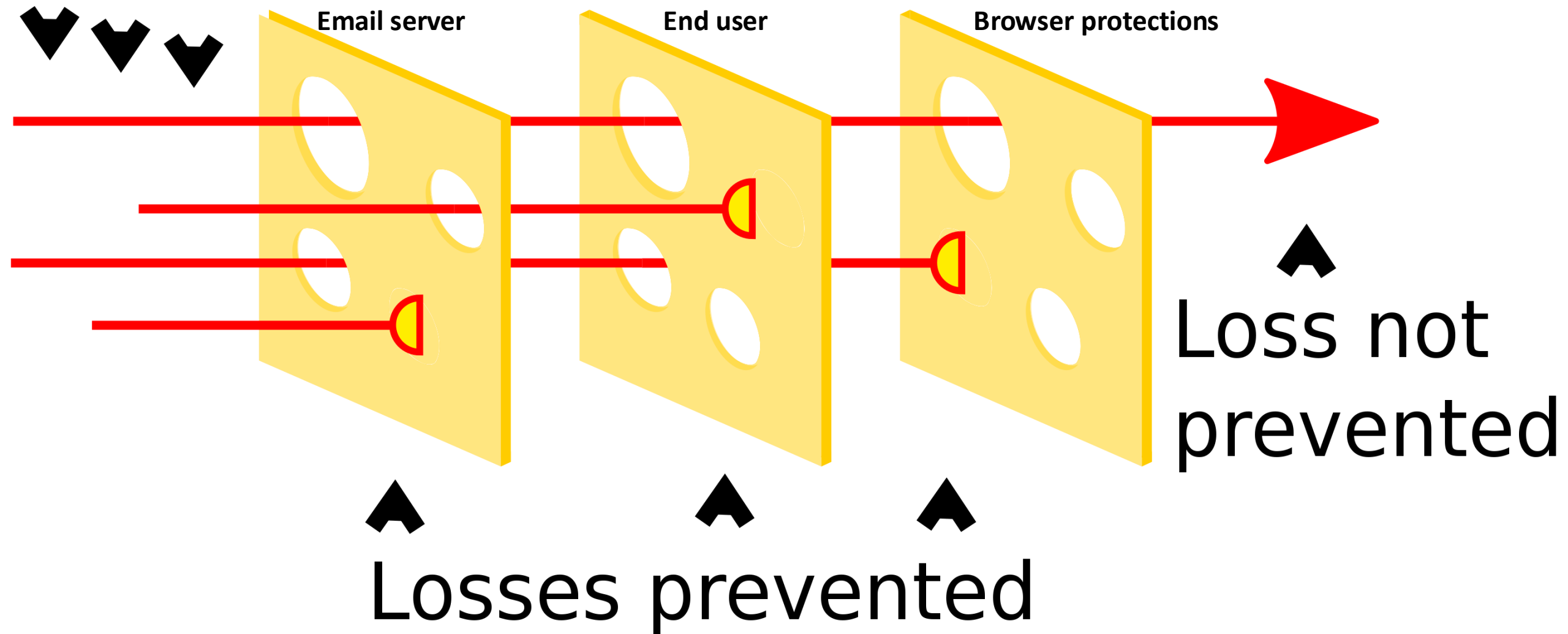
The Phishing Ecosystem

Bank
ISP



Swiss Cheese Model

Hazards



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

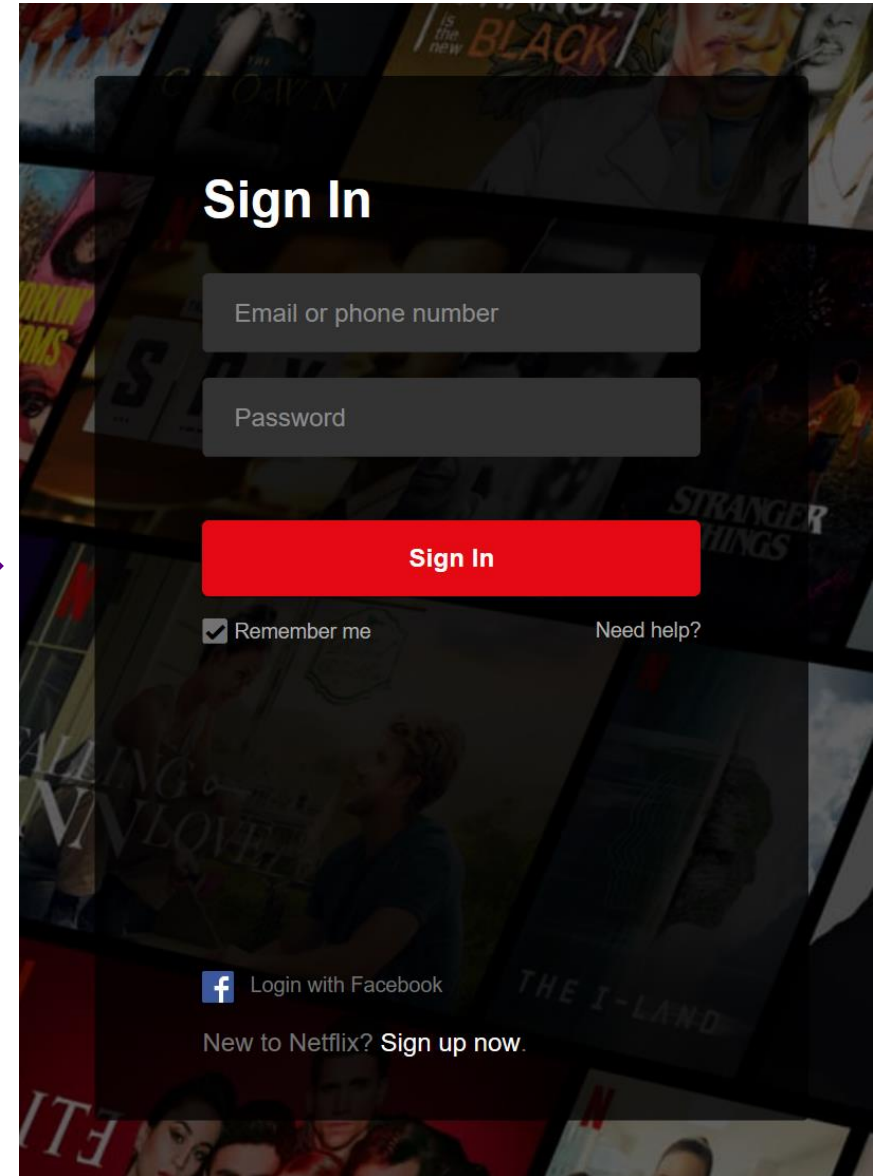
**WHY DOES PHISHING WORK?
AUTHENTICATION IS VERY BROKEN**

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

We normally think of authentication as one directional

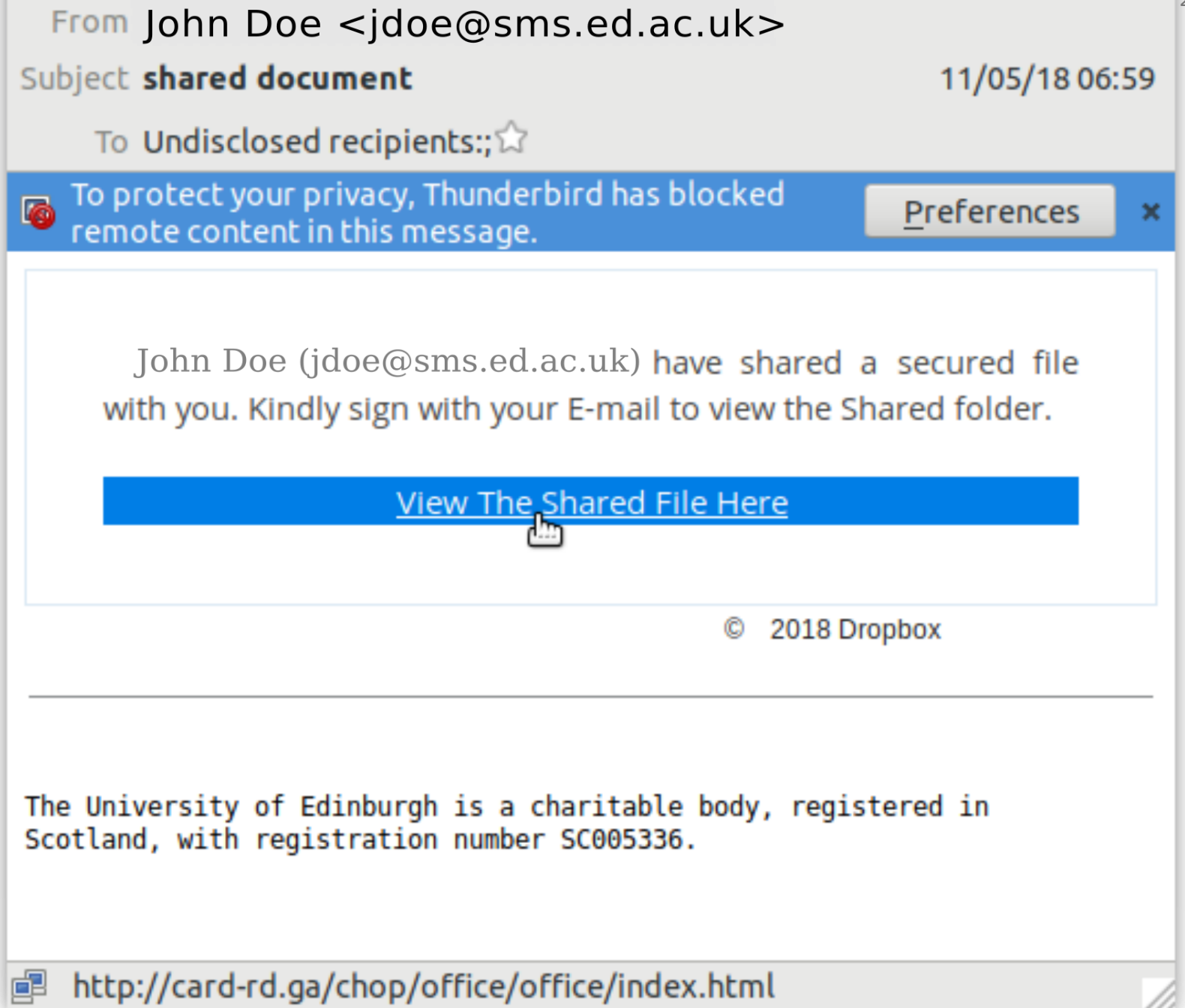
A screenshot of a Netflix sign-in form overlaid on a background of movie posters. The form includes fields for 'Email or phone number' and 'Password', a red 'Sign In' button, a 'Remember me' checkbox, a 'Need help?' link, a 'Login with Facebook' option, and a 'Sign up now' link for new users. The background posters include titles like 'BLACK', 'STRANGER THINGS', and 'THE I-LAND'.

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 com-

mand 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 redoubled in recent years, have hit a ceiling

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 com-

mand 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-

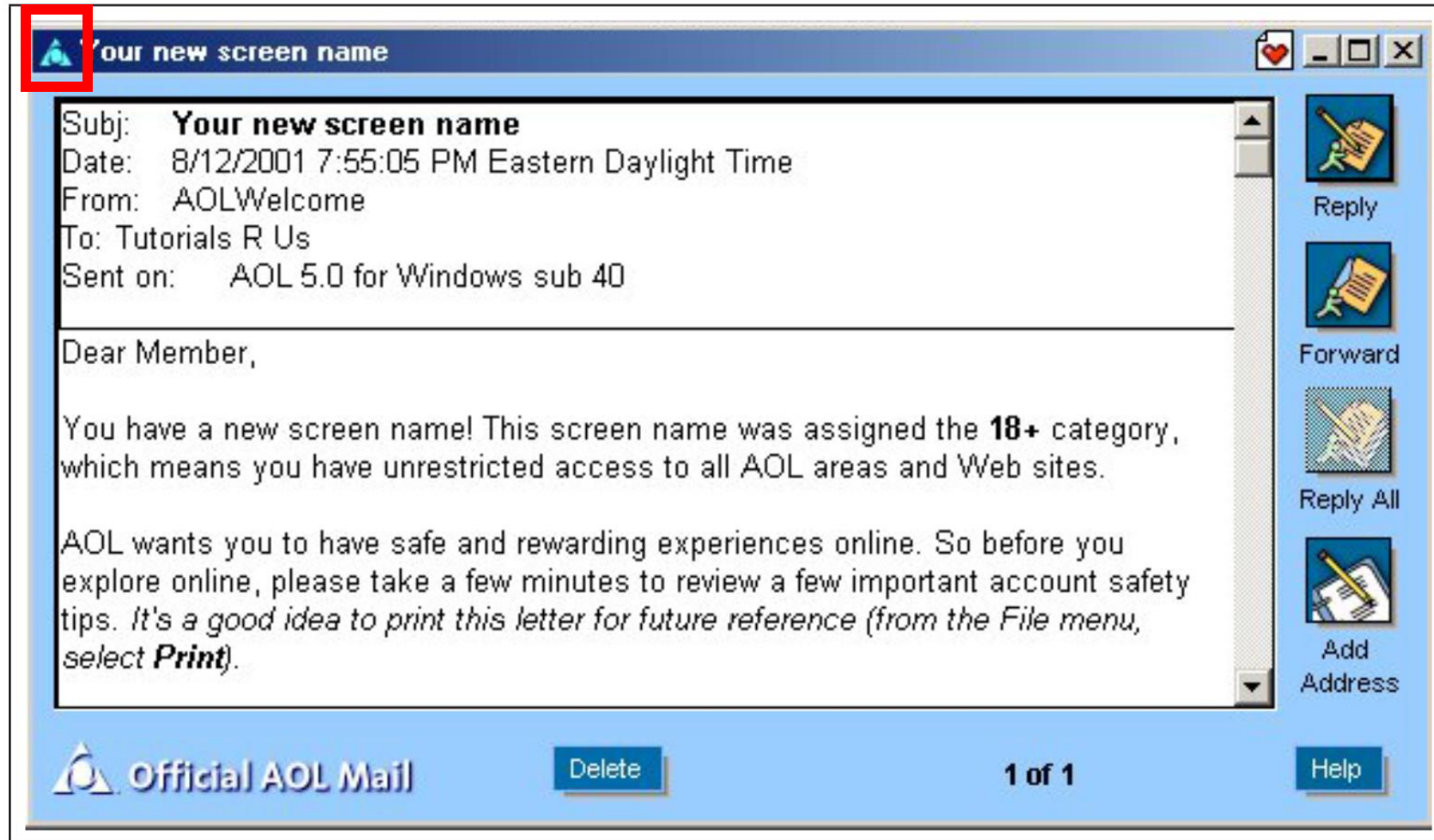
Local companies frequently put together software bundles they know will work with their systems and offer them to customers to ease the once-daunting task

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 redoubled in recent years, have hit a ceiling

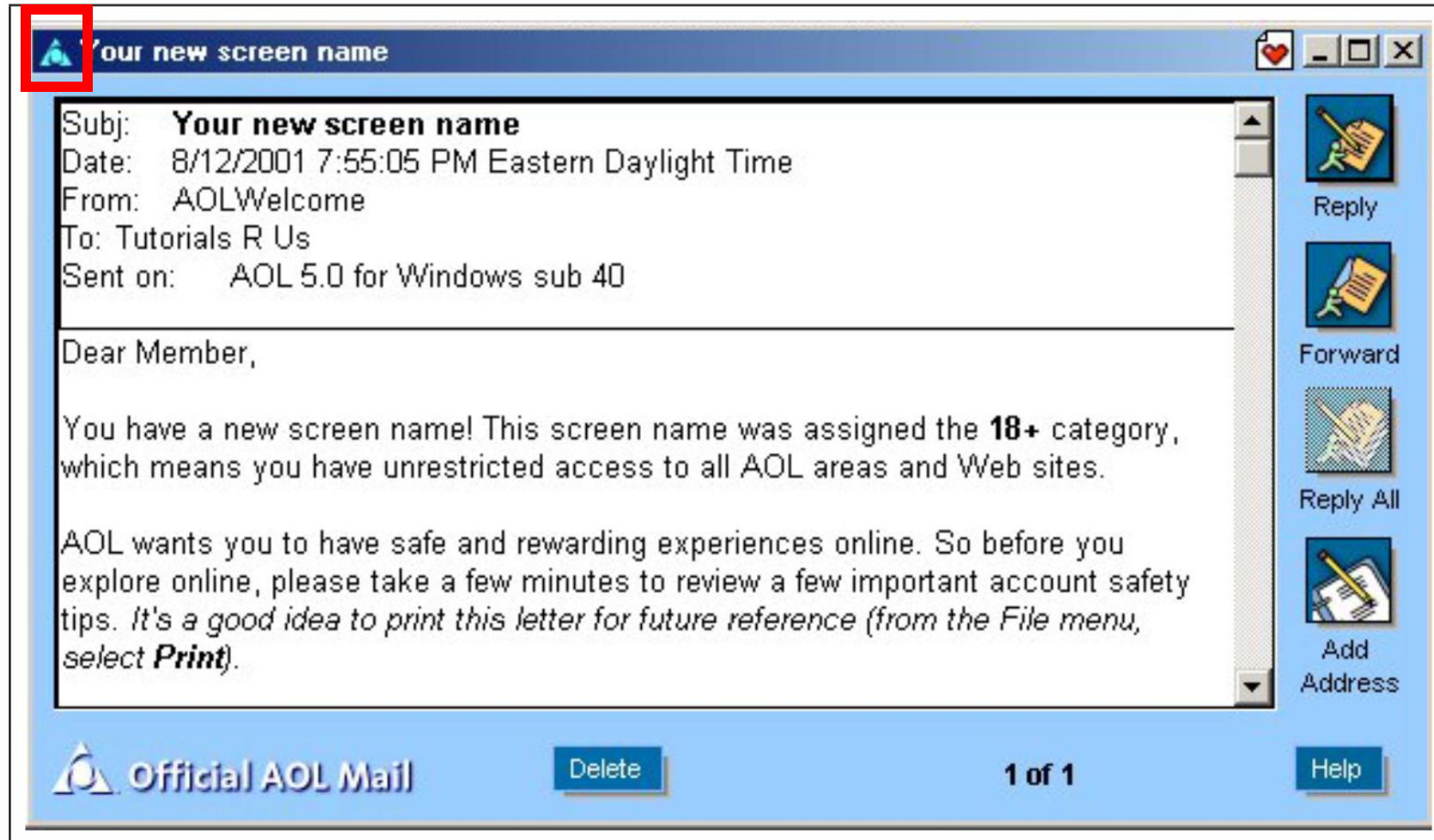
AOHell

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



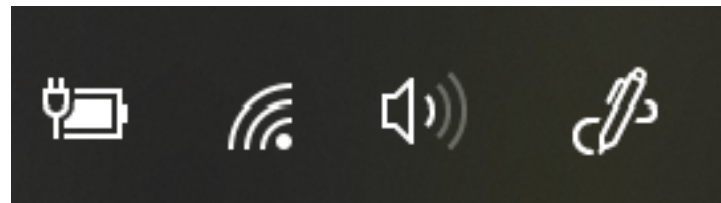
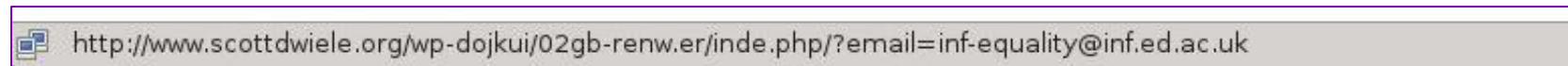
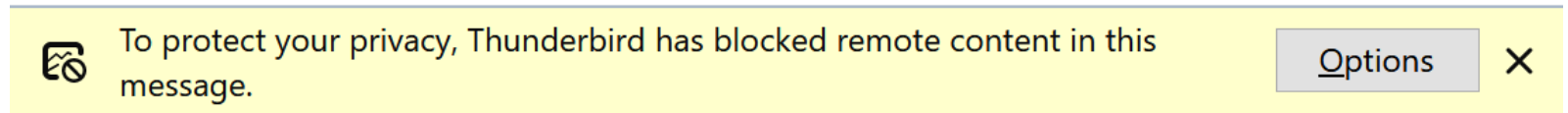
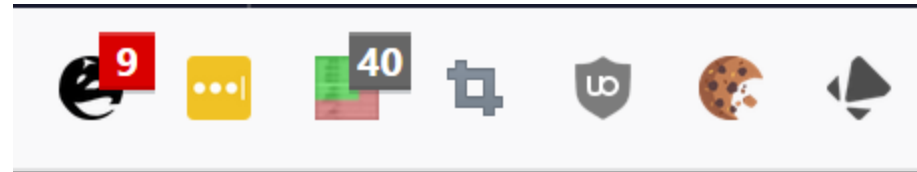
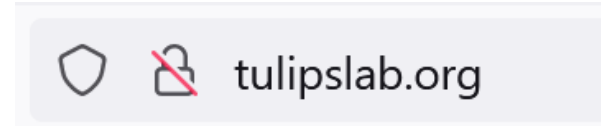
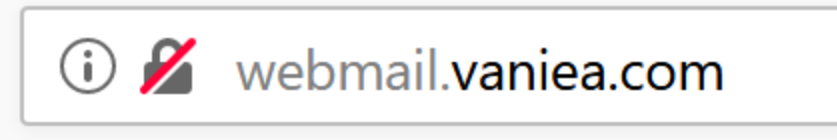
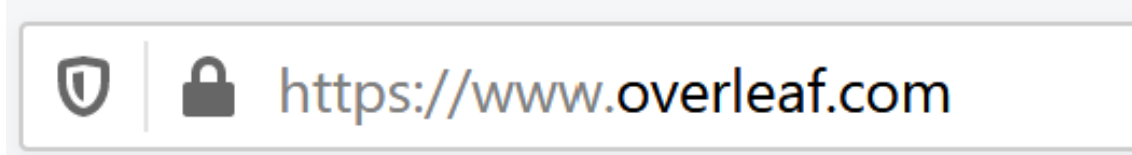
Passive Indicator

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

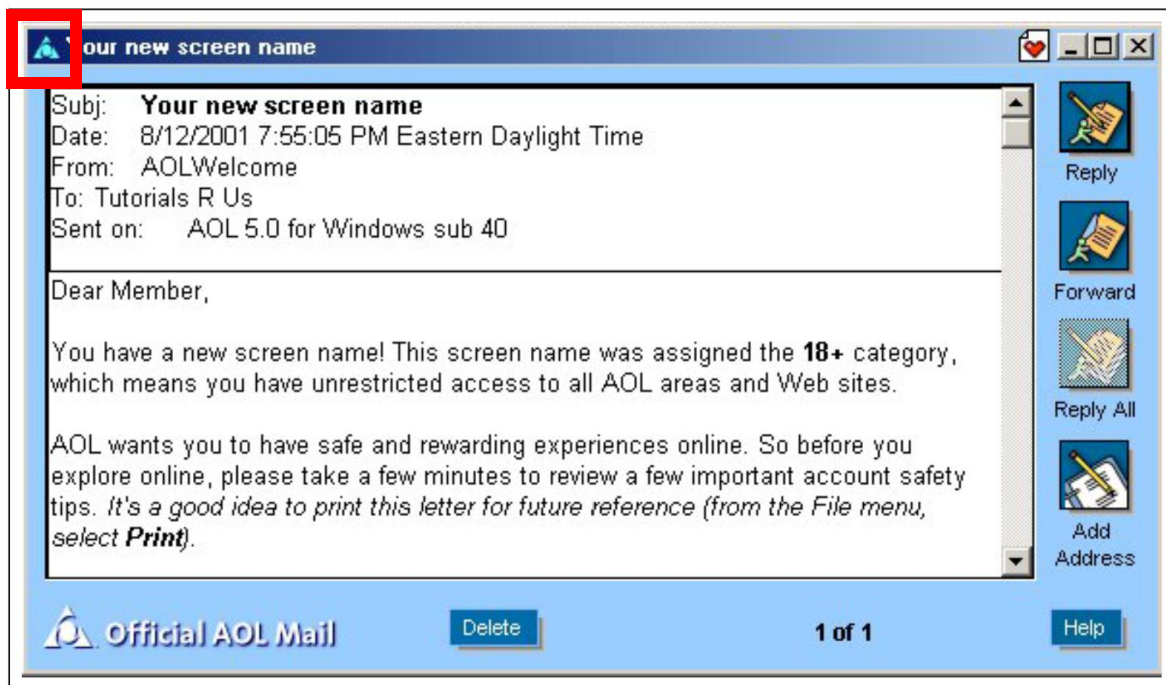


Passive Indicator

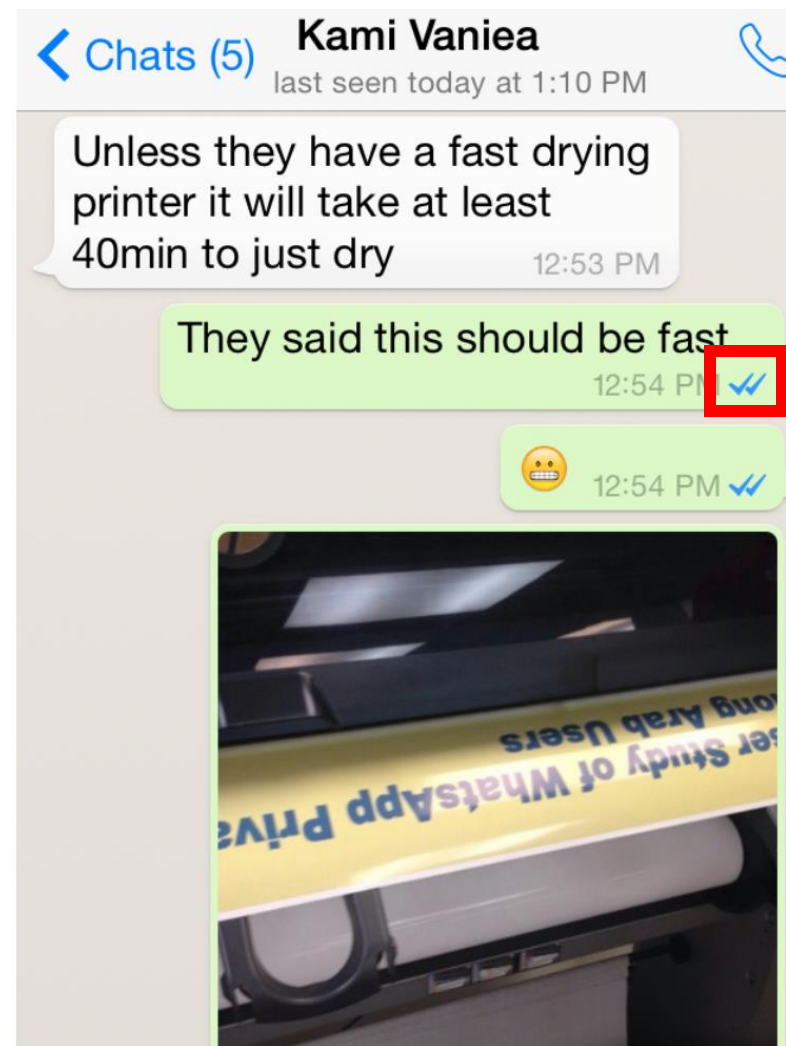
A UI element that provides information, but the user is not forced to look at or interact with.



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.



Phishing moves to email

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

News & Trends



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

information 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

News & Trends



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

information 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

News & Trends

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

SpoofStick

You're on **paypal.com**

Netcraft Toolbar

Since: [Oct 2001](#) Rank: [41](#) [Site Report](#)  [US] [eBay, Inc](#)

TrustBar



eBay Account Guard



SpoofGuard

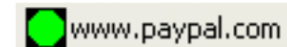


Figure 1. Existing security toolbars

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 `cgil.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
32 Vassar Street, Cambridge, MA 02139



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 `cgil.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

ABSTRACT

Security tool information attacks. Because, they should use these toolbars providing per studies of three indicators and phishing attacks attention to the disregarded content of web many subjects how sophisticated

Author Keywords

World Wide Study, User Interface

ACM Classification

H.5.2 User Interface Security and Privacy

INTRODUCTION

Phishing has Phishing attacks emails and personal or financial information also be tricked

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

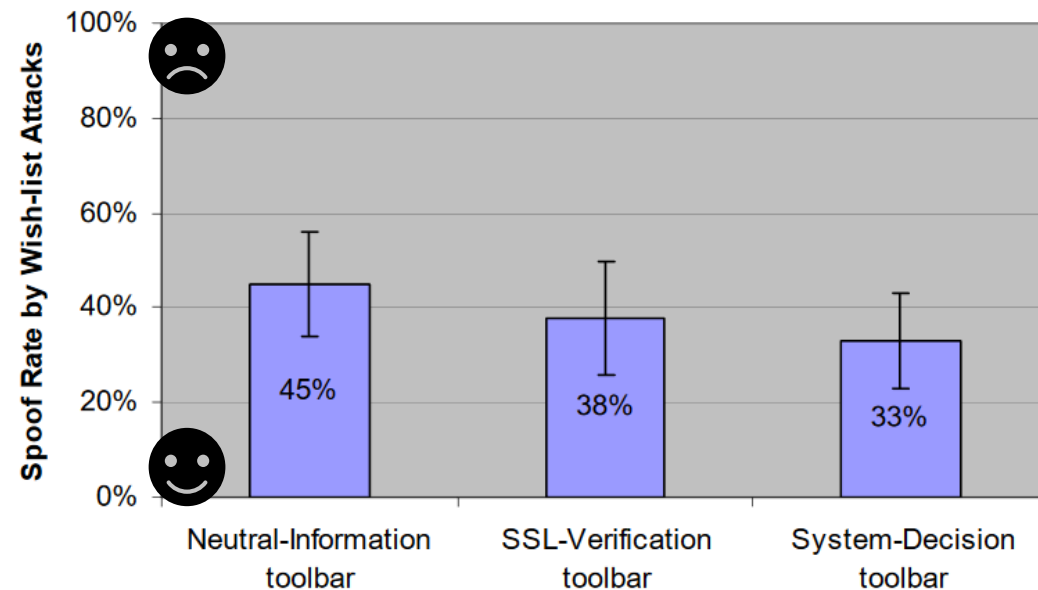


Figure 5. Spoof rates with different toolbars

Attacks?

[US] eBay, Inc

Search Account Guard

toolbars

data to a phishing estimated \$500 million

any phishing attacks. eBay customers, first starts with an email information is invalid the 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:

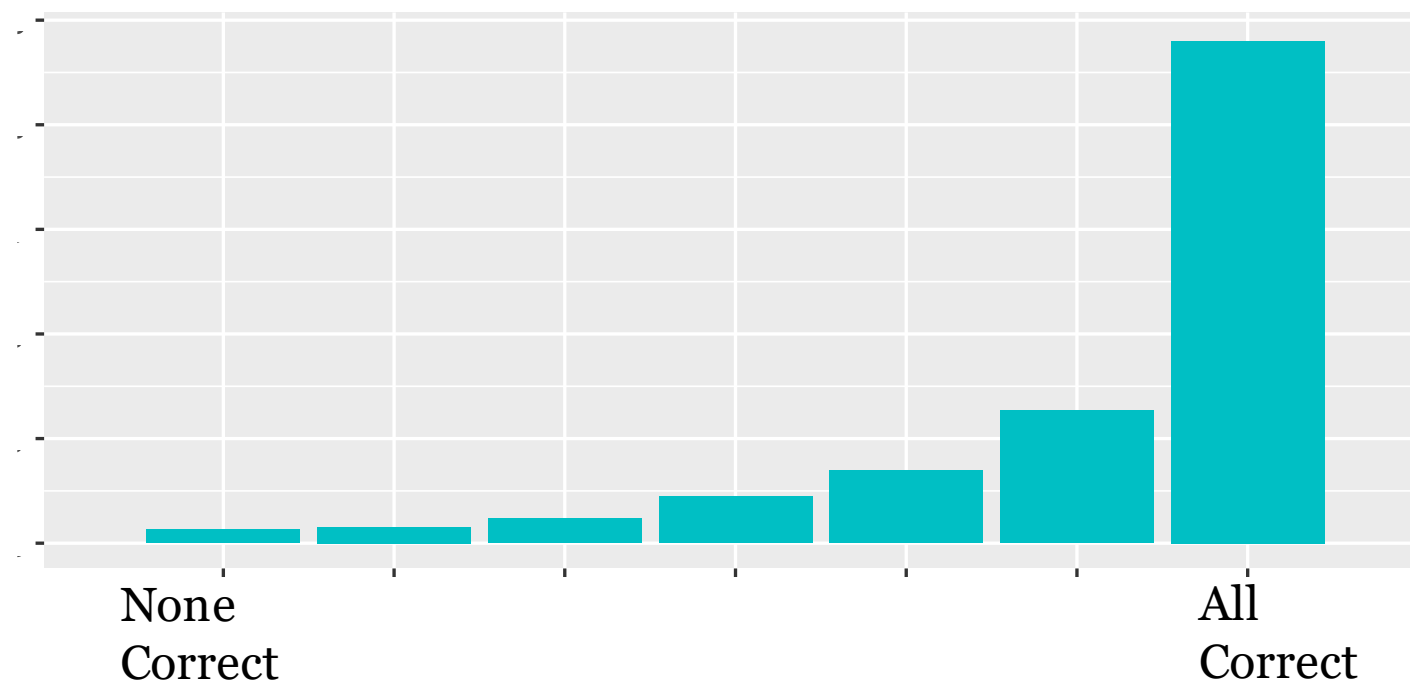
www.ssl-yahoo.com is a subdirectory of Yahoo!, like mail.yahoo.com.

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].



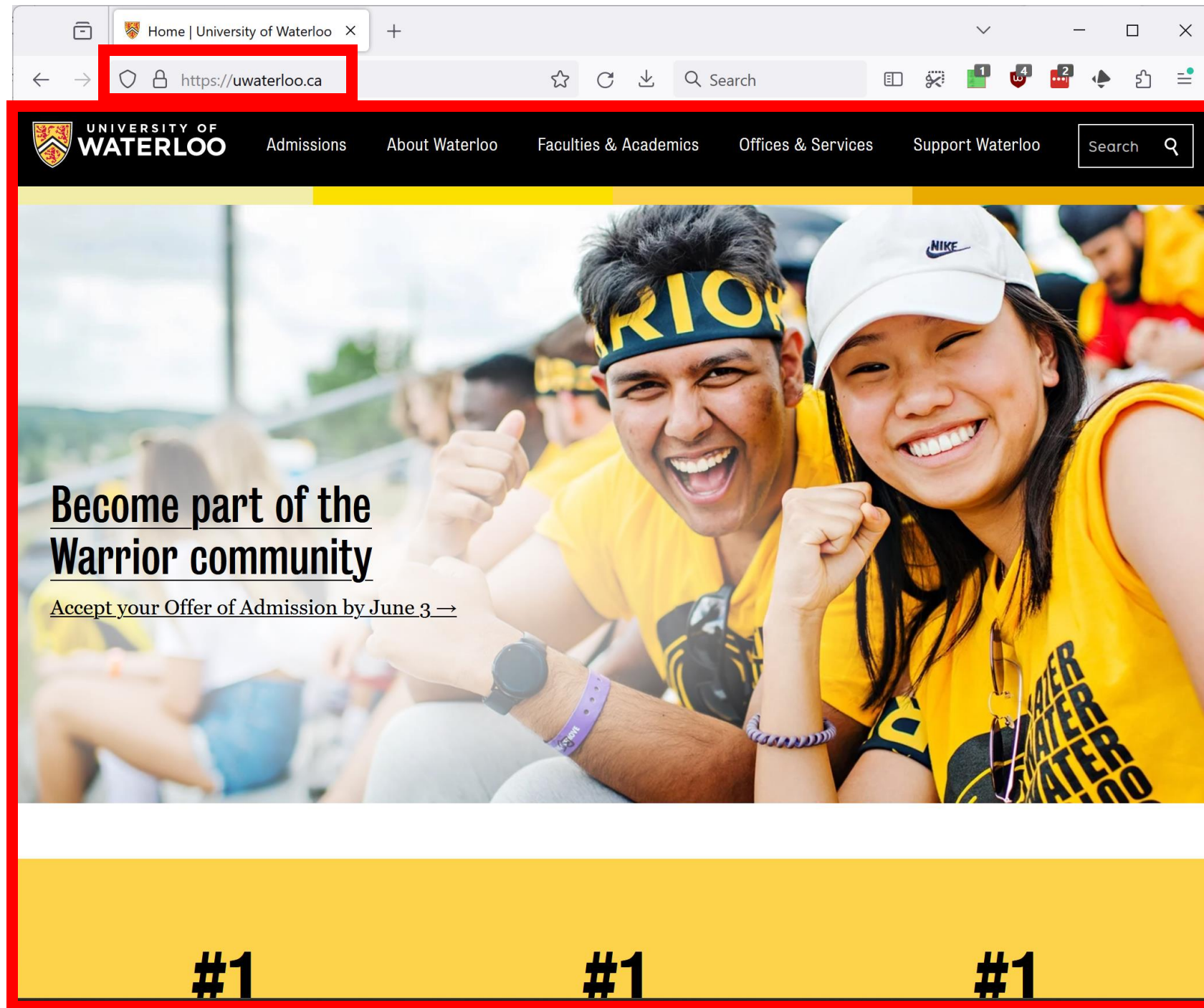
Name in domain
i.e. profile.**facebook**.com
mobile.**paypal**.com

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.

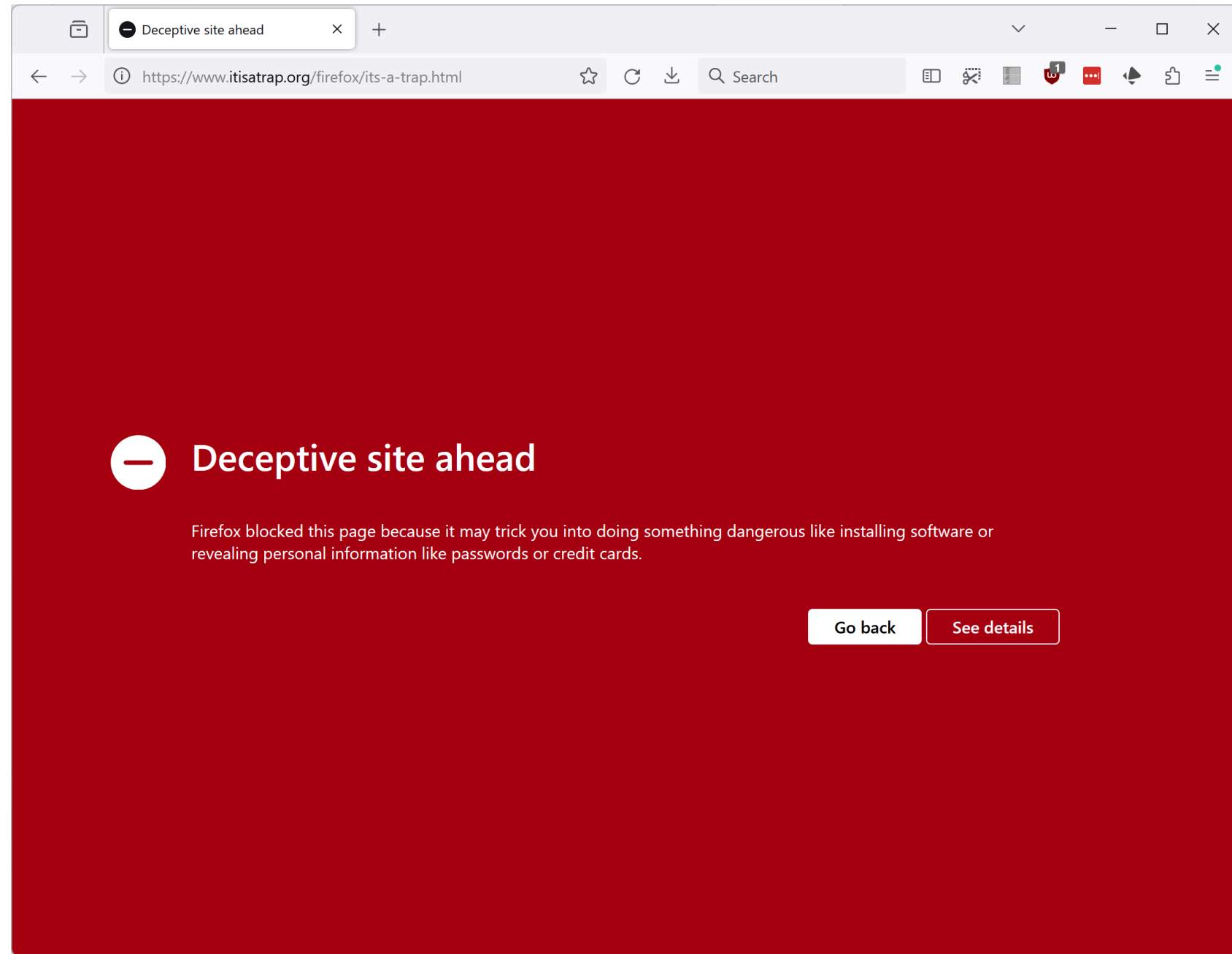
So indicators started getting more obvious and intrusive.

Being passive isn't working....

So lets be active.

Active Indicator

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



Quick side note: There are several special URLs that exist only for testing

- example.com, example.net, example.org, example.edu
 - Reserved by the Internet Assigned Numbers Authority (IANA)
 - https://en.wikipedia.org/wiki/Special-use_domain_name
- itisatrap.org
 - Fake phishing site run by Mozilla that will let developers safely access a site on the known phishing list

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.

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.

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 details

Amount

Reference

A reference is required

When

☒ Today

☐ Later

 Criminals will urge you to pay today. Using pay later can help stop scams by giving you time to cancel.

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](#)

Continue

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](#)

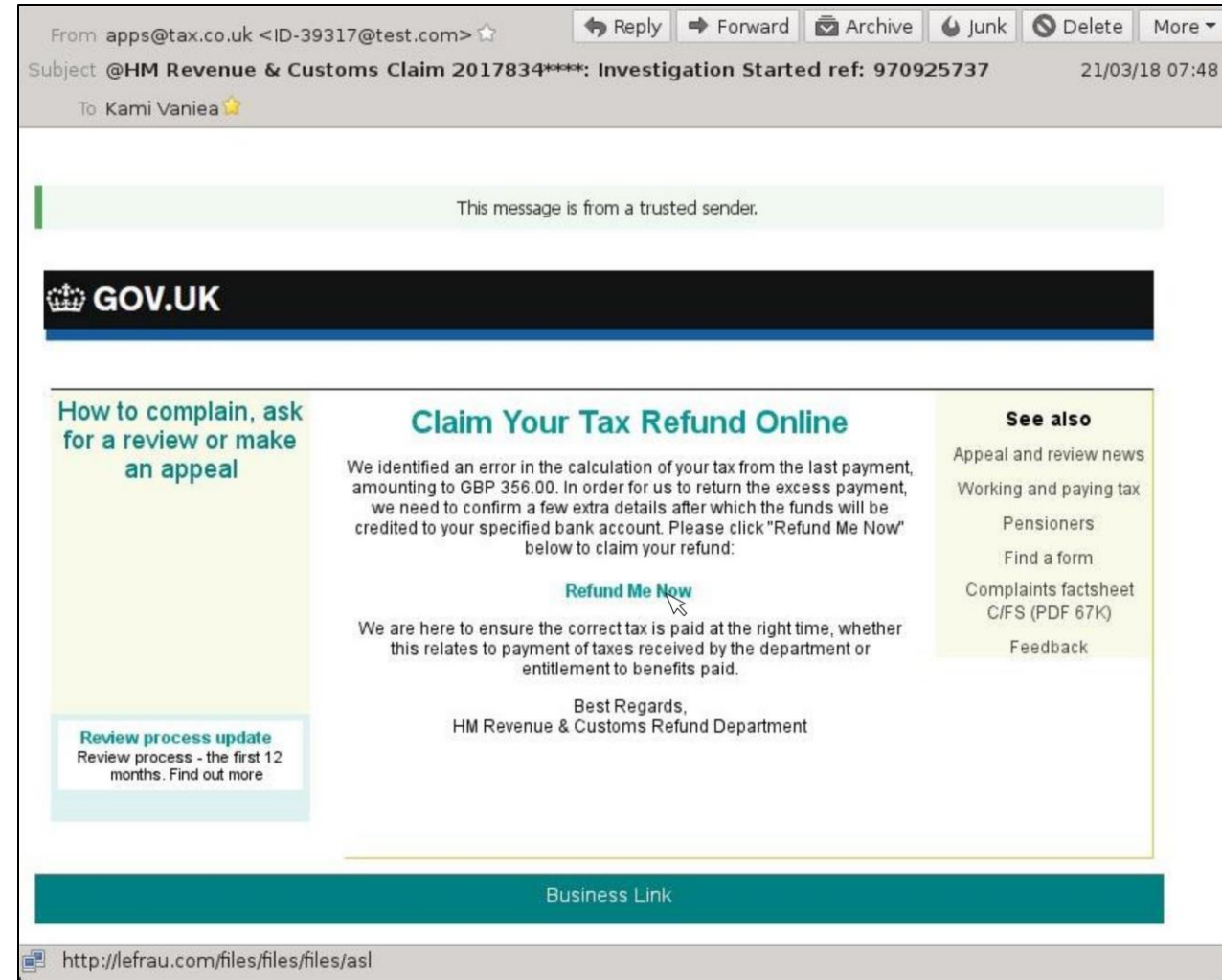
SOLVING PHISHING

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

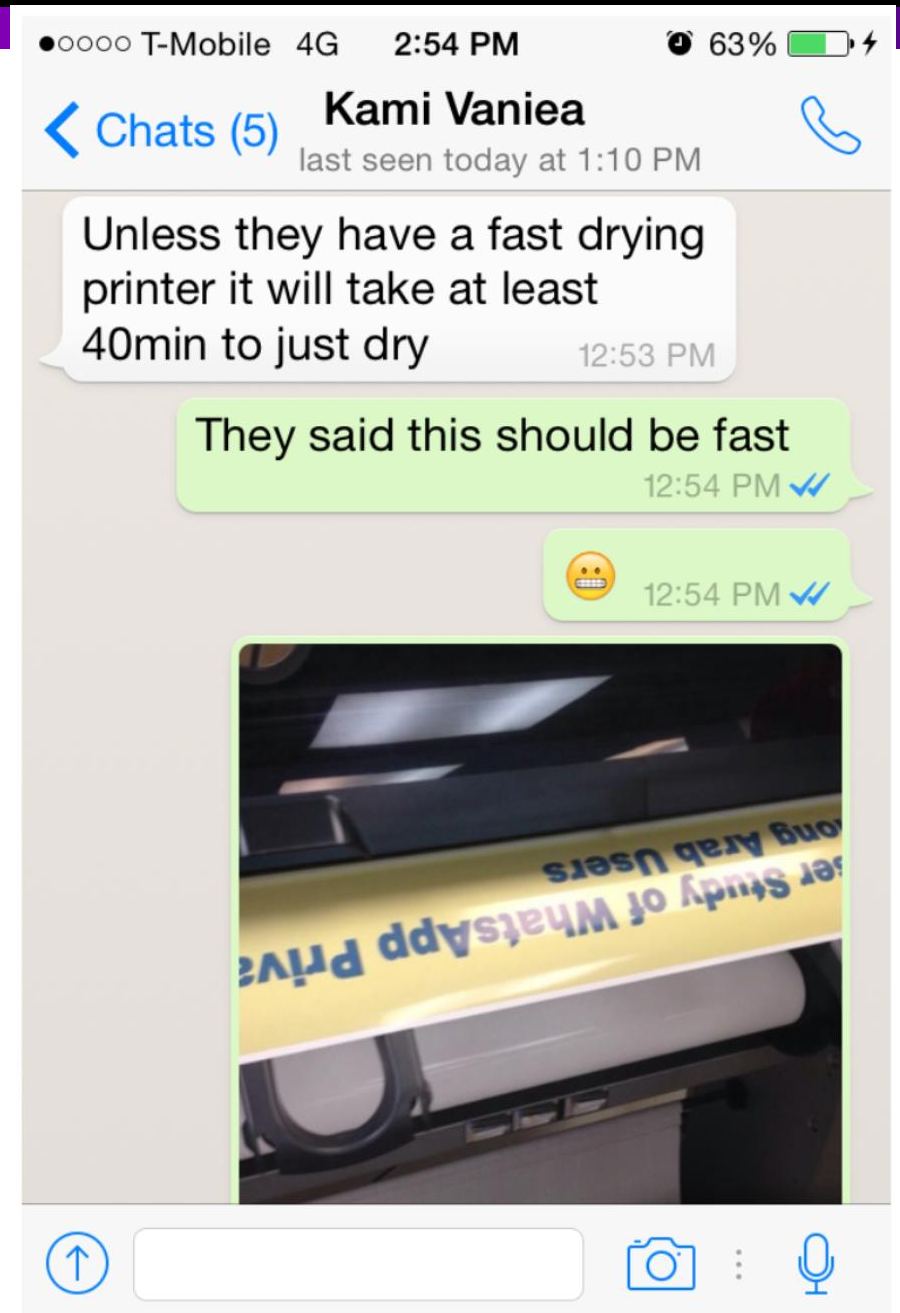


Features for phishing URL detection

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

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?

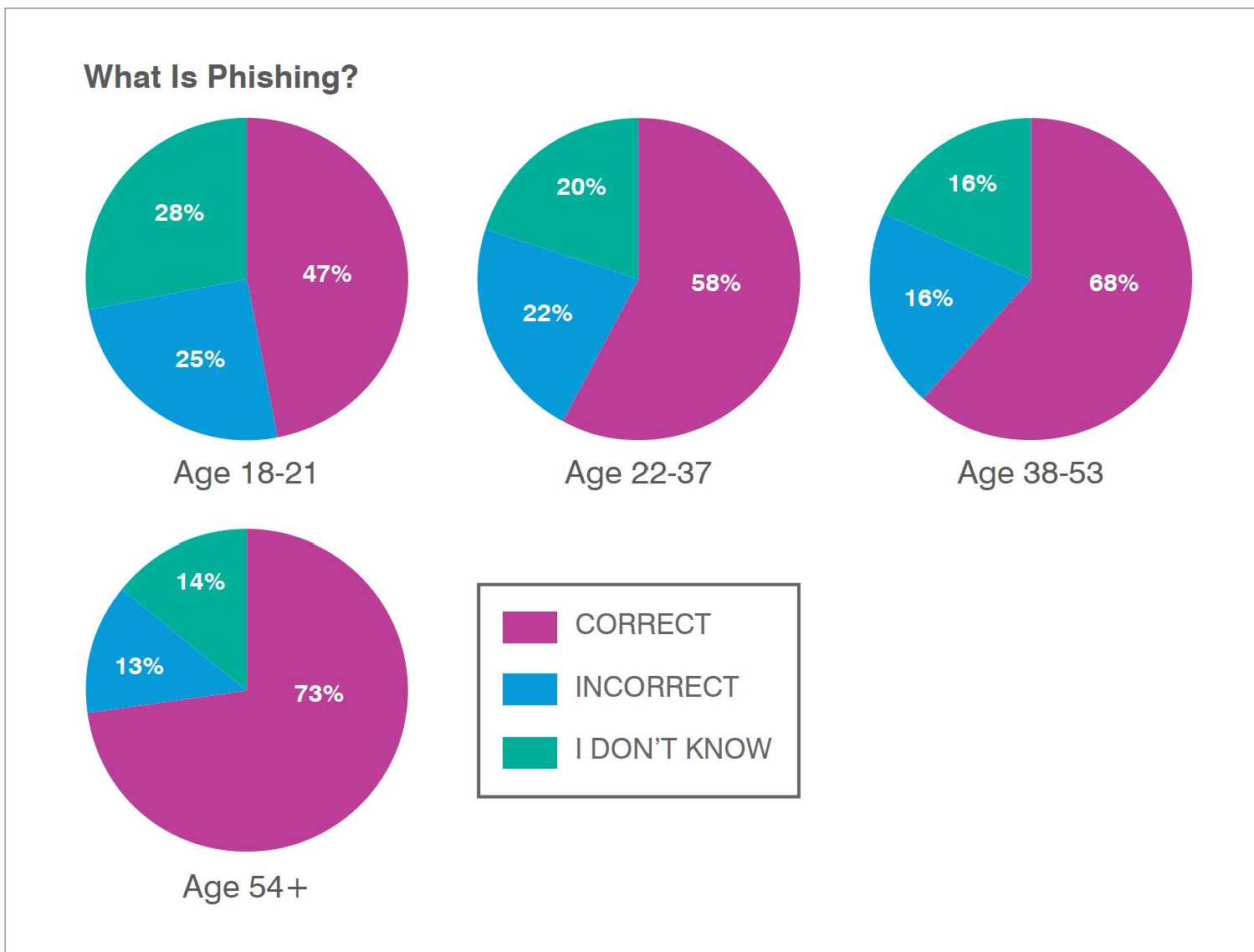


Main “solutions”

- 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

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

The difference is likely due to life experience with fraud.

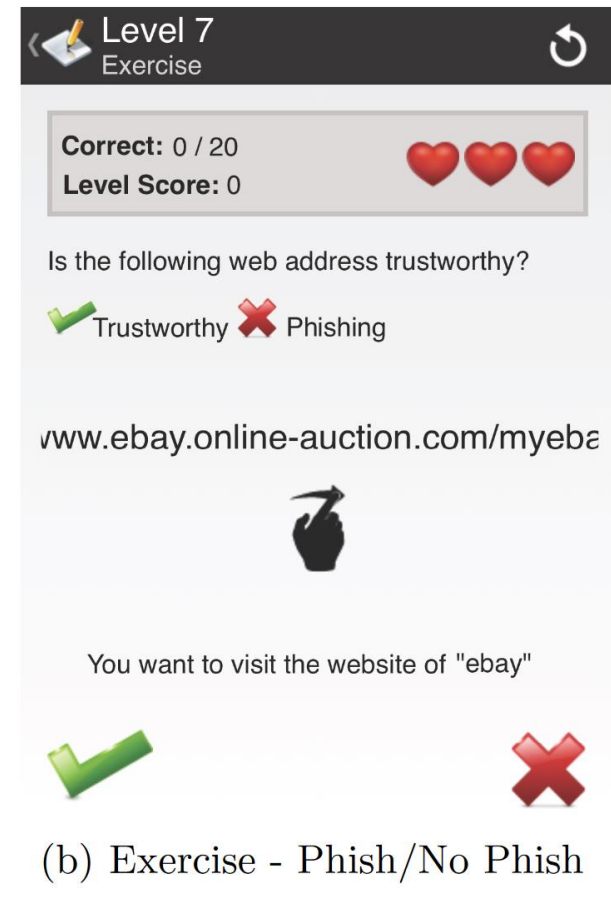


Note: According to Pew Research, millennials fell into the 22-37 age bracket and baby boomers were 54 and older in 2018.

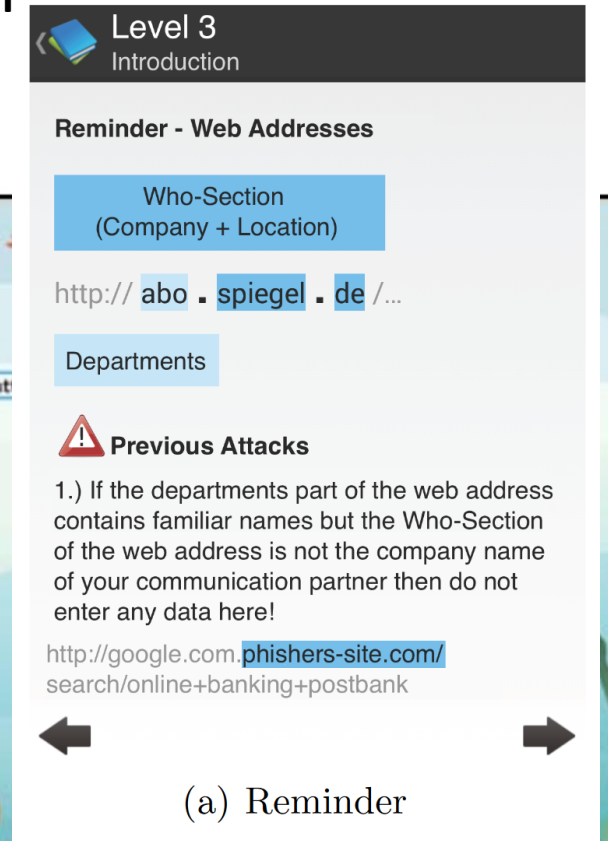
Training users

- 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



(b) Exercise - Phish/No Phish



(a) Reminder

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:

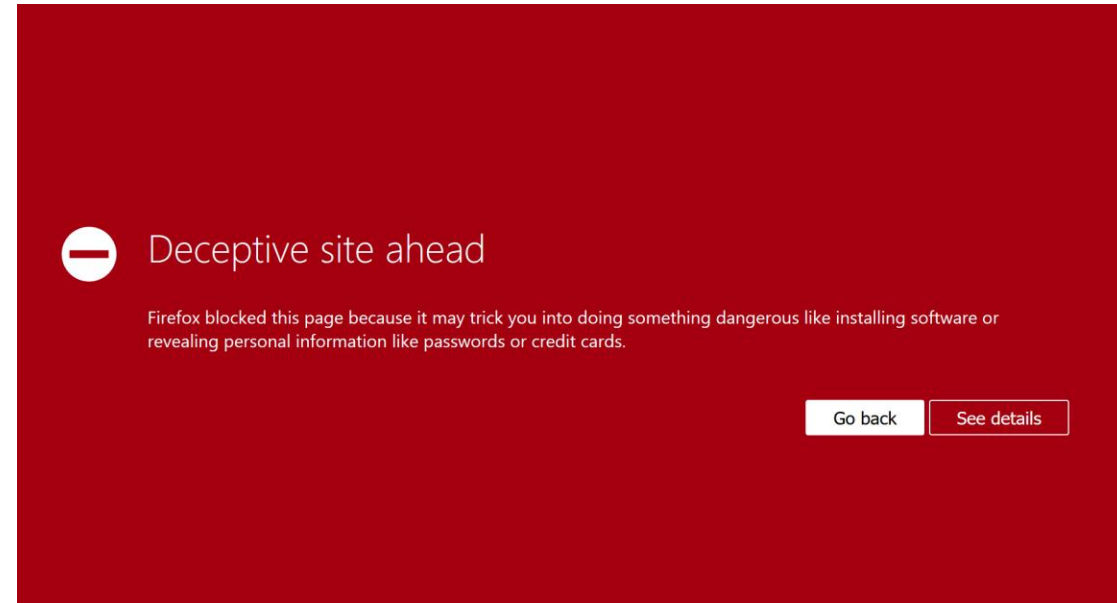


- Toll Violation Notification
- [EXTERNAL]: Your Unclaimed Property
- Updated Building Evacuation Plan
(also among the highest failure rates in 2017)
- Invoice Payment Required
- February 2018 – Updated Org Chart
- Urgent Attention (a notification requesting an email password change)

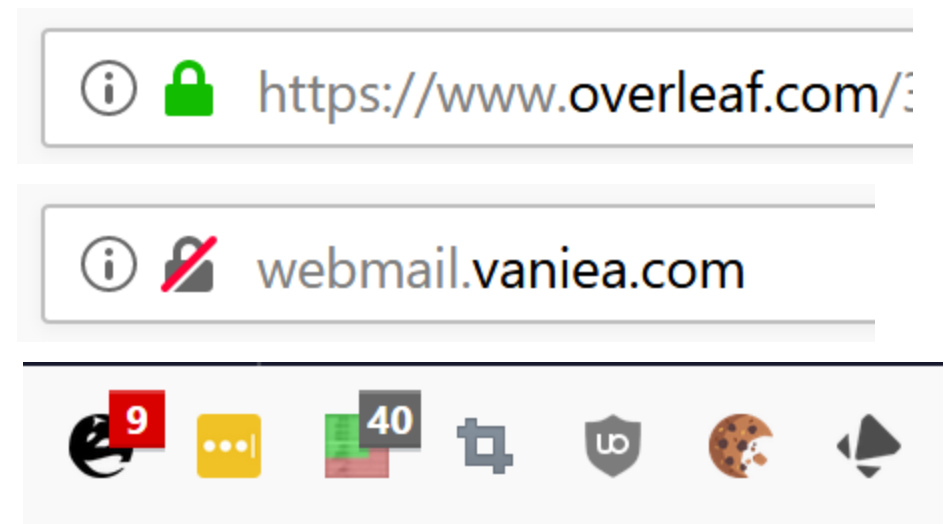
Managing phishing

- 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 Joint Program of the APWG and Carnegie Mellon CUPS

Developers and admins are users too.

Provide help for those who are trying to counter phishing at their organizations.

How to Redirect a Phishing Site Web Page to the APWG.ORG Phishing Education Page

Important note to program participants: To verify any communication about the APWG/CMU Phishing Education Landing Page Program, please open a new browser – do not click on any links in email or instant message - to go to the homepage of the APWG and click on the link for the redirect education initiative. This way you can be sure that the redirect you are creating is going to a legitimate APWG web page.

The APWG and Carnegie Mellon Cylab Usable Privacy and Security Laboratory (CUPS) are working to educate consumers on the perils of phishing and how to avoid them. As part of this initiative, we are requesting that instead of disabling phish sites, ISP, registrars, and other infrastructure entities put an HTTP redirect in place of the phishing page at the phishing URL. The redirect would send a user who has been tricked into visiting a phish site to go to the **Phishing Education Landing Page** at the “most teachable moment”.

In addition, by including a parameter that is the URL of the website that was taken down, you will also help the APWG and CMU’s Cylab Usable Privacy and Security Laboratory to track the success rates of the various phishing education campaigns. This is invaluable information and we appreciate your cooperation in including this parameter in the redirect URL. Your efforts can help educate consumers and enterprise computing users so that they can better protect themselves from electronic crime.

This page has information on how to implement a redirect to the education page.

Implementing a redirect in Apache

There are several ways to implement a redirect in Apache, but the following method is one of the simplest.



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

APWG

Unifying the
Global Response
to Cybercrime

CyLab

Carnegie Mellon
Supporting Trust Decisions Project
cps.cs.cmu.edu/trust



WARNING!

The web page you tried to visit might have been trying to steal your personal information. That page was removed after being identified as a "phishing" web page. A phishing web page tricks people out of bank account information, passwords and other confidential information.

How You Were Tricked

This email is from my bank. It asks me to update my information. I better click on the link and update it.

STOP!
Don't fall for scam email.

My Inbox
From: service@Wombank.com
Dear Jane, Your account will be suspended if you do not update your information.
<http://www.Wombank.com/update>

How to Help Protect Yourself

- 1 Don't trust links in an email.
DANGER! <http://www.amazon.com/update>
- 2 Never give out personal information upon email request.
DANGER! Name: Jane Smith
Credit Card: 1234 5678 9101 1213
- 3 Look carefully at the web address.
<http://www.amazon.com>
- 4 Type in the real website address into a web browser.
<http://www.amazon.com>
- 5 Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.
Credit Card Statement
For Customer Service call: 1-800 xxx-xxx
- 6 Don't open unexpected email attachments or instant message download links.
My Inbox
Here is the updated document.
[attachment](#)

How Phishers Trick You Into Giving Out Personal Information

My Inbox
From: service@Wombank.com
Dear Jane, Your account will be suspended if you do not update your information.
<http://www.Wombank.com/update>

- He forges email addresses to look genuine
- He provokes the computer user with an urgent request
- He adds links that appear to connect to a real bank but bring users to the phisher's counterfeit site - to take their information and money

How You Can Help

Should I report this suspicious email?

This one was already reported. You are safe. But please tell your friends what you learned here.

For additional information, please visit APWG's resources page at <https://apwg.org/resources/>

Legal Disclaimer

PLEASE NOTE: The APWG, Carnegie Mellon University, and any cooperating service providers have provided this message as a public service, based upon information that the URL you were seeking has been involved in a phishing or malware exploit. There is no guarantee that you have not been phished or exposed to malware from this URL you were seeking, or previously. This is not a complete list of steps that may be taken to avoid harm from phishing, and we offer no warranty as to the completeness, accuracy or pertinence of this advisory with respect to the page you attempted to access. Please see <https://www.apwg.org> for more information. The FishGuru goldfish character is a trademark of Wombat Security Technologies, Inc.



Content on this web page is licensed by APWG, Carnegie Mellon University, and Wombat Security Technologies, Inc. under a Creative Commons Attribution-No Derivative Works 3.0 Unported License

APWG Home

CMU STDP Home

Consumer Advice

Membership

Contact Us

About

Common phishing elements

- Automated – Typically directed against many people.
- Impersonation – Communication claims to be from someone trusted or that they are not. For example, from a bank.
- Direction to a website – Links that look like they go somewhere legitimate but in fact go somewhere controlled by the attacker.
- Contain an attachment – Attachment asks for information to be sent back or contains malicious code.
- Authentication info requested – The communication aims to get authentication information.

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