

Usable Security and User Training

KAMI VANIEA

JANUARY 25

Equifax was serving up spyware

<https://krebsonsecurity.com/2017/10/equifax-credit-assistance-site-served-spyware/>

12 Equifax Credit Assistance Site Served Spyware

OCT 17

Big-three consumer credit bureau **Equifax** says it has removed third-party code from its credit report assistance Web site that prompted visitors to download spyware disguised as an update for **Adobe's Flash Player** software.

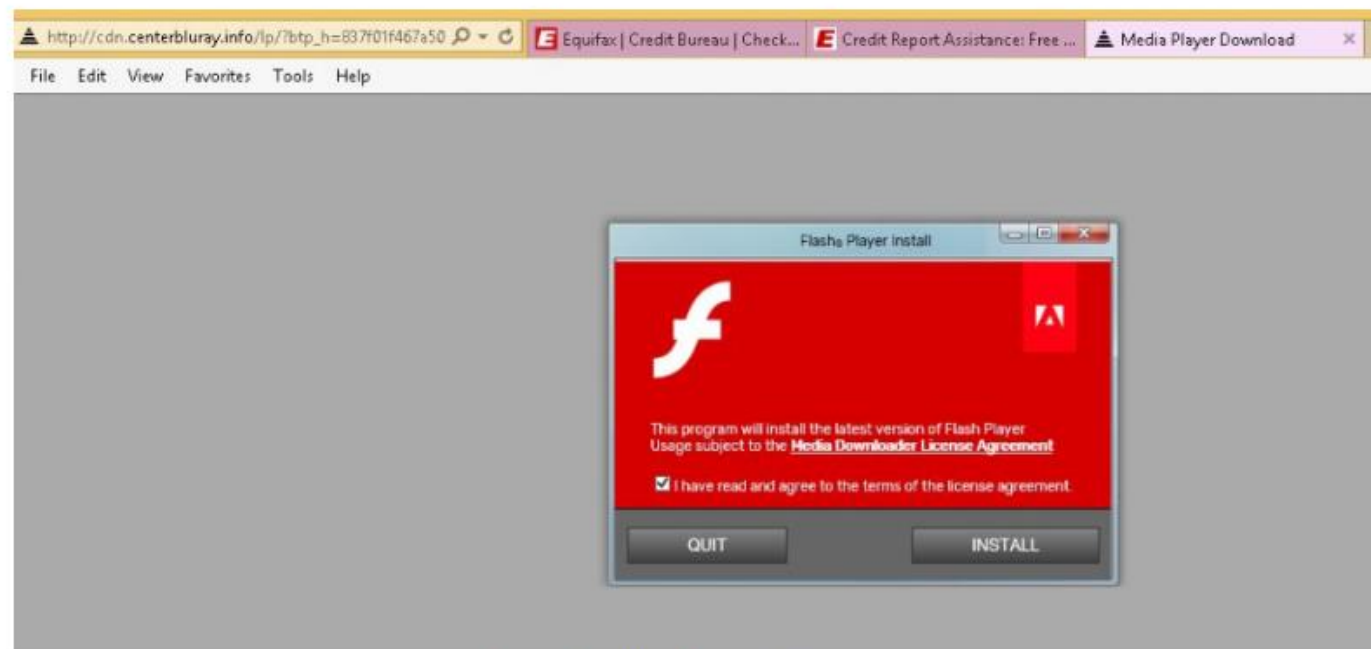


Image: Randy-abrams.blogspot.com

On Wednesday, security expert and blogger **Randy Abrams** **documented** how browsing a page at Equifax's **consumer information services portal** caused his browser to be served with a message urging him to download Adobe Flash Player.

“As I tried to find my credit report on the Equifax website I clicked on an Equifax link and was redirected to a malicious URL,” Abrahms wrote. “The URL brought up one of the ubiquitous fake Flash Player Update screens. ”

Equifax was serving up spyware

FILE UNDER WTF —

Equifax website borked again, this time to redirect to fake Flash update

Malware researcher encounters bogus download links during multiple visits.

DAN GOODIN - OCT 12, 2017 6:33 AM UTC

In a follow-up statement shared with KrebsOnSecurity this afternoon, however, Equifax said the problem stemmed from a “third-party vendor that Equifax uses to collect website performance data,” and that “the vendor’s code running on an Equifax Web site was serving malicious content.”

<https://krebsonsecurity.com/2017/10/equifax-credit-assistance-site-served-spyware/>

reached by **attackers who eventually made**
amount of other details for some 145.5
, and again early Thursday morning, the
ver fraudulent Adobe Flash updates,
dware that was detected by only three of



65 antivirus providers.



Randy Abrams, an independent security analyst by day, happened to visit the site Wednesday evening to check what he said was false information he had just found on his credit report. Eventually, his browser opened up a page on the domain `hxxp//:centerbluray.info` that looked like this:

What do they mean by “third party vendor”?

Websites are
made up of many
elements from
many sources



You can easily see this list on most browsers in the “Network” developer tool.

Check Your Credit Score | Equifax

https://www.equifax.co.uk

Search

Continue

EQUIFAX

Personal


Business

Public Sector

About

Login

10th Oct: Equifax cybersecurity incident: How it affects UK Consumers, Please [click here](#)



Check your Equifax Credit Report & Score now

✓ Easy to understand, no jargon

Inspector

Console

Debugger

Style Editor

Performance

Memory

Network

Storage

All

HTML

CSS

JS

XHR

Fonts

Images

Media

Flash

WS

Other

Disable cache

Filter URLs

Status	Method	File	Domain	Cause	Type	Transfer	Size	Time
200	GET	SaveGETEvents?d=ZGF0YT...	ws.sessionca...	JS img	gif	819 B	819 B	→ 719 ms
200	POST	SaveEvents?url=https://w...	ws.sessionca...	JS xhr	json	99 B	99 B	→ 1310 ms
200	GET	SaveGETEvents?d=ZGF0YT...	ws.sessionca...	JS img	gif	819 B	819 B	→ 1543 ms
200	POST	SaveEvents?url=https://w...	ws.sessionca...	JS xhr	json	99 B	99 B	→ 720 ms
200	GET	activityi;src=1361123;type...	1361123.fl.s.d...	JS subdocu...	html	177 B	194 B	→ 109 ms
200	POST	SaveEvents?url=https://w...	ws.sessionca...	JS xhr	json	99 B	99 B	→ 282 ms

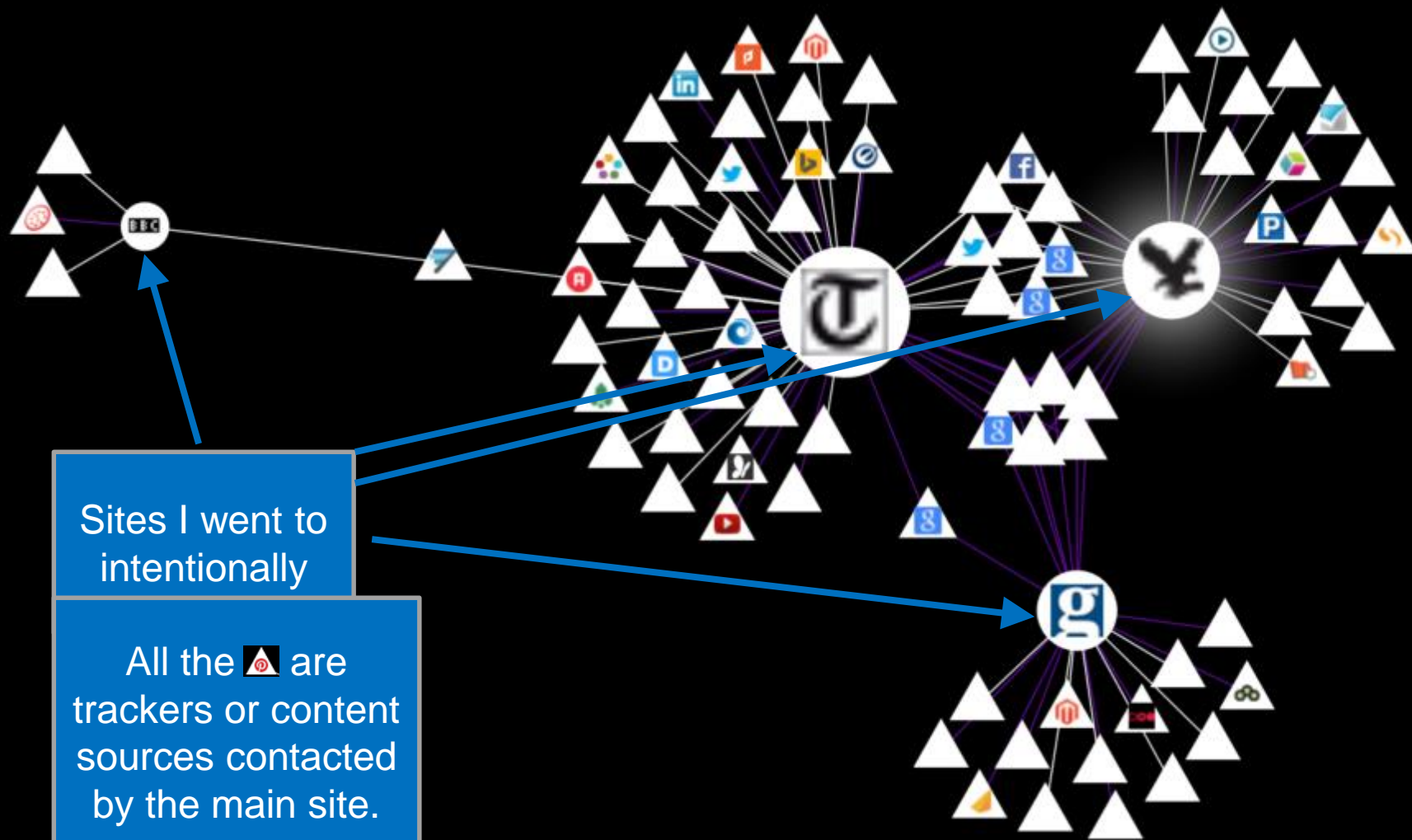
101 requests

1.58 MB / 1.16 MB transferred

Finish: 17.41 s

DOMContentLoaded: 2.07 s

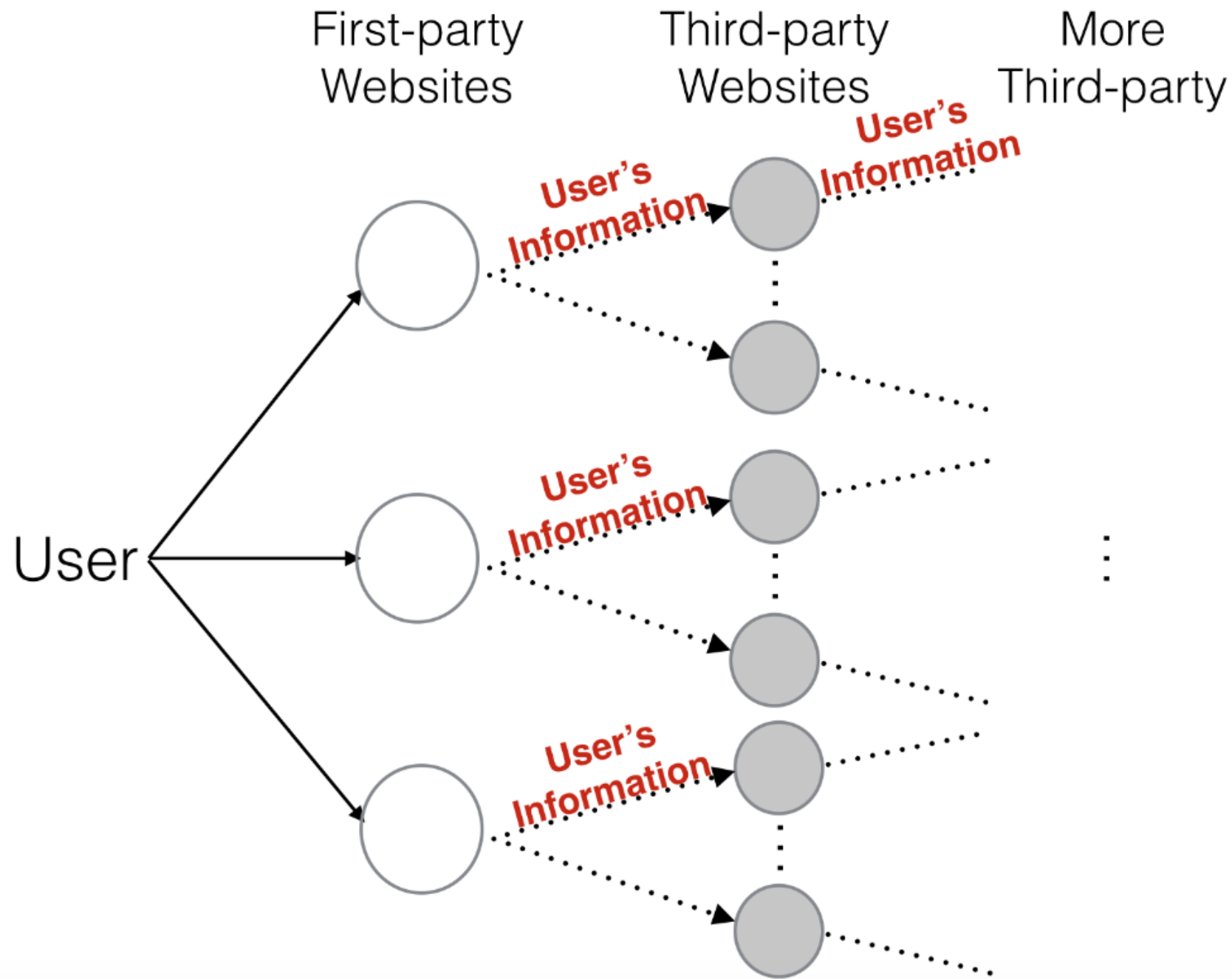
load: 3.87 s

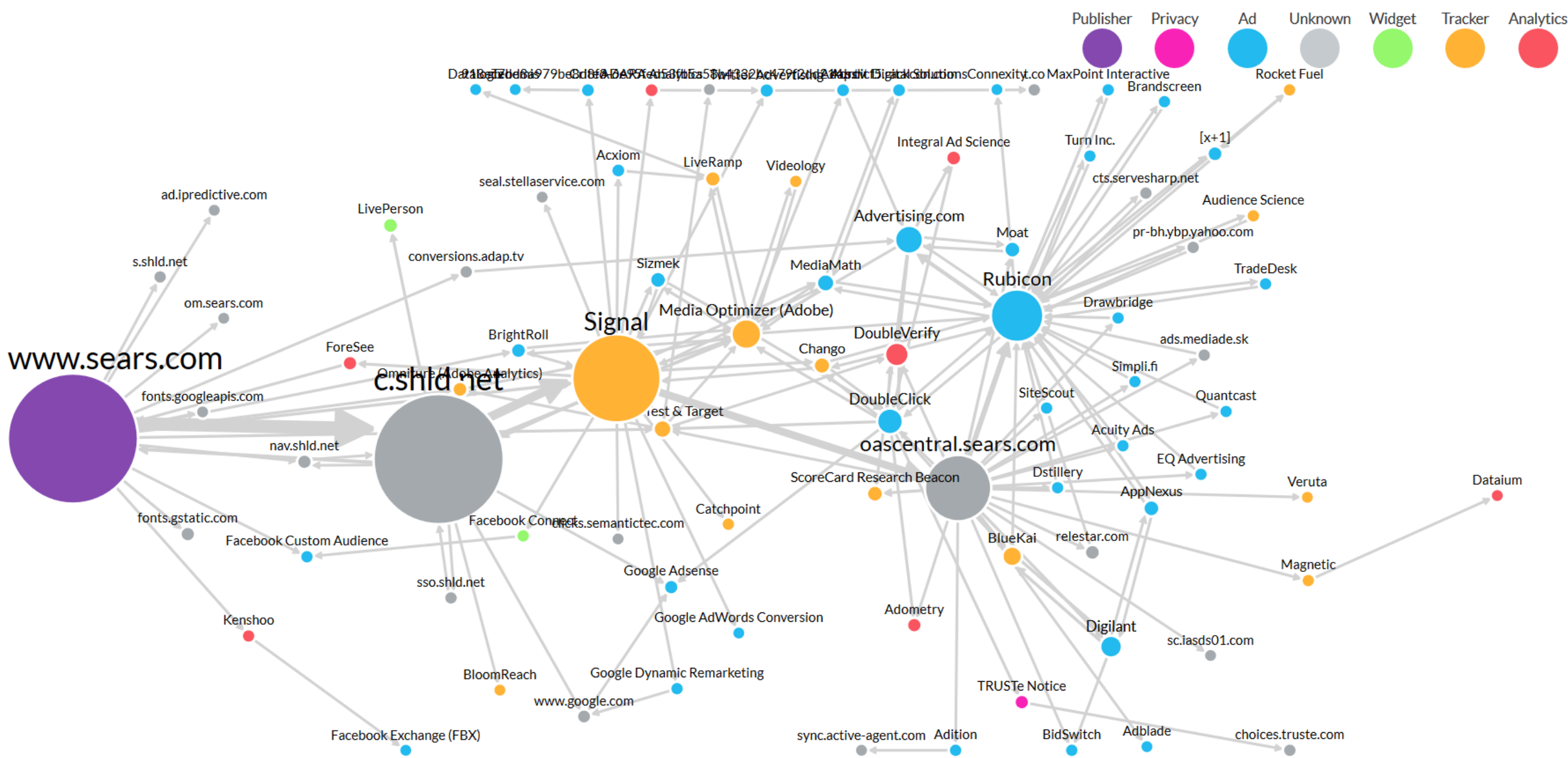


The user visits a “first party website” such as cnn.com or theguardian.com

That webpage then instructs your computer to fetch other websites to load content such as ads, images, calendars, Facebook, etc.

Those websites then in turn have more requests



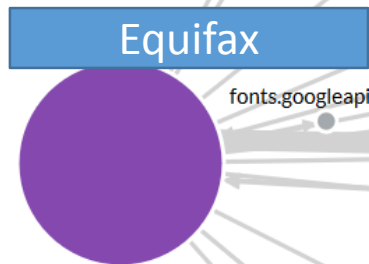


Fascinating, but what has all this got to do with Equifax serving Spyware?

Imagine that this node is a Javascript library that Equifax loads. Like jquery or Bootstrap.

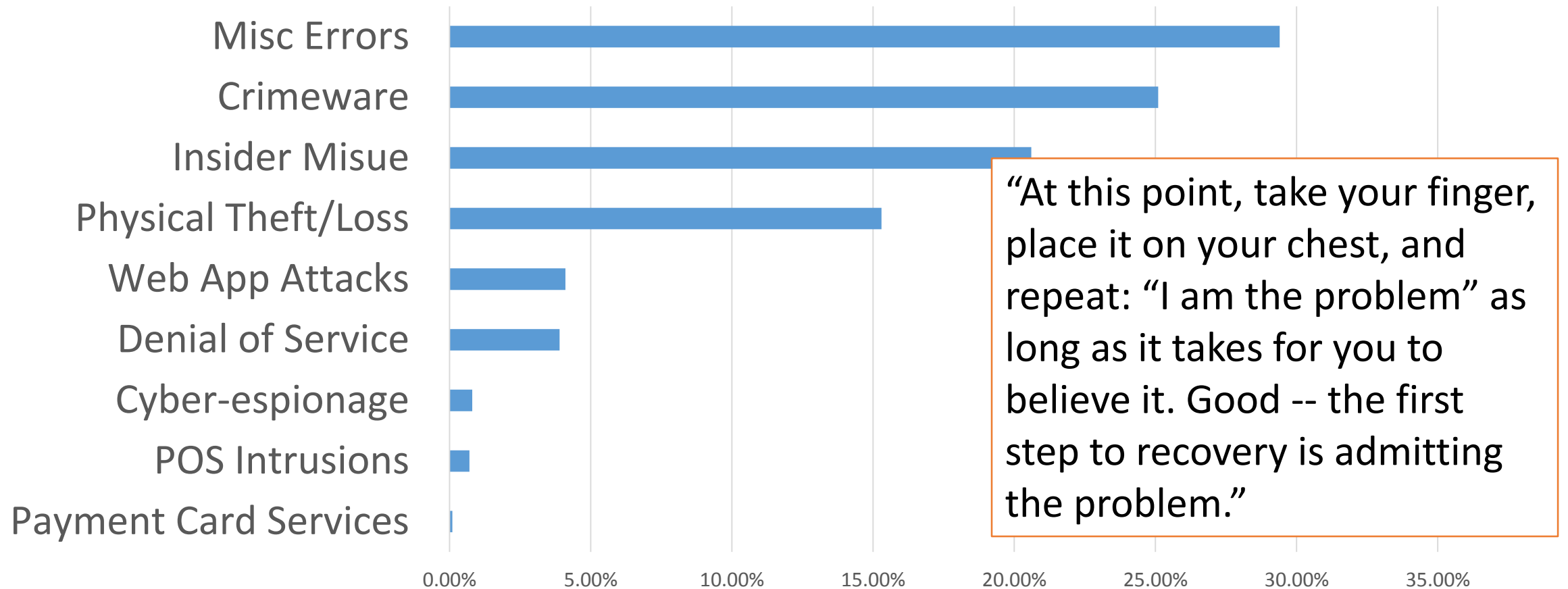
Except one day it goes out of business and no one notices because it is a very small company. And its domain registration lapses.

Then an ingenious malicious person registers the domain and starts serving spyware along with the old library.



Usable Security

People account for 90% of all security incidents



Users are not the enemy

- Malicious actors are the enemy
- Users are a partner in keeping the system secure
- Like any partner:
 - They have skills you don't have
 - They are missing skills you do have
- Think about what skills they have that you need
- Use the skills you have to make good decisions on users' behalf

Three reasons people don't use security or privacy technologies

1. They do not care about security and privacy
2. They do not know about security or privacy issues
3. They cannot use security and privacy technologies

Today and next lecture:


- How do I be safe online? Formulating good security advice
- Famous studies
- Passwords
- Phishing
- Warning and communications
- Trust. How it is built and supported

How do I be safe online?

The single most common question I get asked.

Opinion of
security
professionals
and normal
users.

They don't
match...

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

Common advice:

- Install an anti-virus scanner (Windows 8+ installed one for you)
- Keep your software updated
- Select a strong passcode for important things you use all the time
- Use a password manager for less important things that you use rarely
- If you have important things you use rarely, pick a strong password and write it down somewhere safe (this is ok)
- Install an ad blocker
- Remove software you don't use
- If you are not sure about a website Google for it

Software I use:

- **Ad-blockers** – they are not just about ads, they reduce the amount of content loading
- **Ghostery** and **Privacy Badger** – Will block trackers
- **Lightbeam** – visualizes the trackers, though it does not protect you from them very well
- **Password managers** – LastPass, OnePassword, and KeePass are the most recommended
- 2-Factor like **YubiKey** – Extra protection for accounts like Facebook
- If you are really serious, and do not mind major usability issues
 - UMatrix and NoScript - both block code from running off of third party sites

Famous studies

Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0 by Whitten and Tygar

- Asked 12 Carnegie Mellon Computer Scientists to correctly send an encrypted email using PGP 5.0
- Only 4 managed to accomplish this within 90 minutes
- Dangerous errors
 - Accidentally emailing without encrypting
 - Confusions around key system
 - Giving up



Fill in the blanks with:

Alice, Bob, Sign, Encrypt, Decrypt, Public, and Private

Bob would like to send Alice an encrypted email. So he first _____ the message with _____ key and then _____ the message with _____ key.

Alice gets a message supposedly from Bob. So she _____ the message using _____ key. She then verifies the _____ using _____ key.

- ✍️ Compose
- Inbox
- Drafts
- Sent
- Archive
- Spam
- Trash
- > Smart views
- ✓ Folders
- > Recent

To

Subject

CC/BCC



chrome-extension://kajibbejlbohfggdiogboambcijhkke/components/editor/editor.html?id=ba5baaef5c00a8bdb27...

Compose E-mail

frankchou1116@gmail.com ✕

Add recipient

Happy birthday !

Encrypt attachments

E-mail will be signed digitally

☒ Sign message with key: Qingyu Zhou <frankchou1116@yahoo.com> - 01C23B378BC3 ▾

Sign all messages with primary key

Options 📄

✍️ Sign Only

✕ Cancel

🔒 Encrypt

Send

Task 2: Write an encrypted email

	Webmail login	Composing email on	Opening Mailvelope popup	Sending encrypted email
T1	Success(hint)	Webmail editor	Failure	Failure
T2	Success(hint)	Webmail editor	Failure	Failure
T3	Success(hint)	Webmail editor	Failure	Failure
T4	Success(hint)	Webmail editor	Failure	Failure
T5	Success(hint)	Webmail editor	Failure	Failure
T6	Success	Webmail editor	Failure	Failure
T7	Success	Webmail editor	Failure	Failure
T8	Success	Webmail editor	Failure	Failure
T9	Success(hint)	Mailvelope popup	Success	Success
T10	Success	Webmail editor	Failure	Failure

Table 4.3: Completion details of Task 2 for each participant.

So why did they all fail?

Cognitive Walkthrough

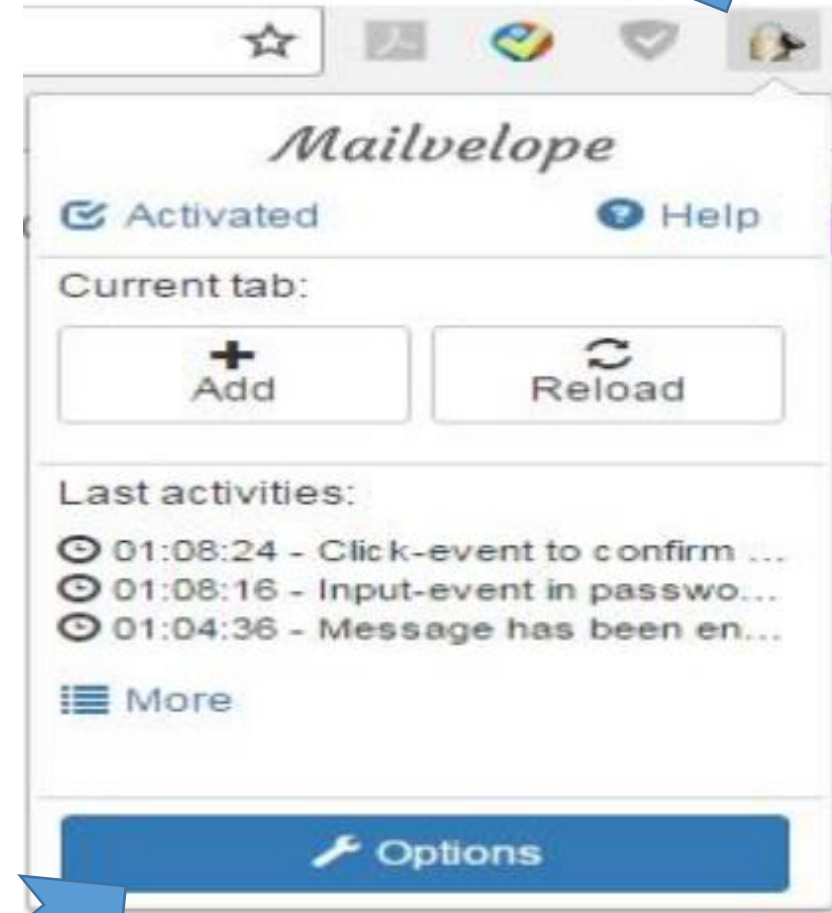
Step2: Click on the “Options” button.

Q1. Will users try to achieve the outcome of clicking on this button?

Q2. Will users see this button for the action?

Q3. Once users find this button, will users recognize that clicking on it will produce the effect they want?

Q4. After the action is performed, will users understand the feedback, so they can confidently continue on to the next action?



Security experts are not typically trained in usability.

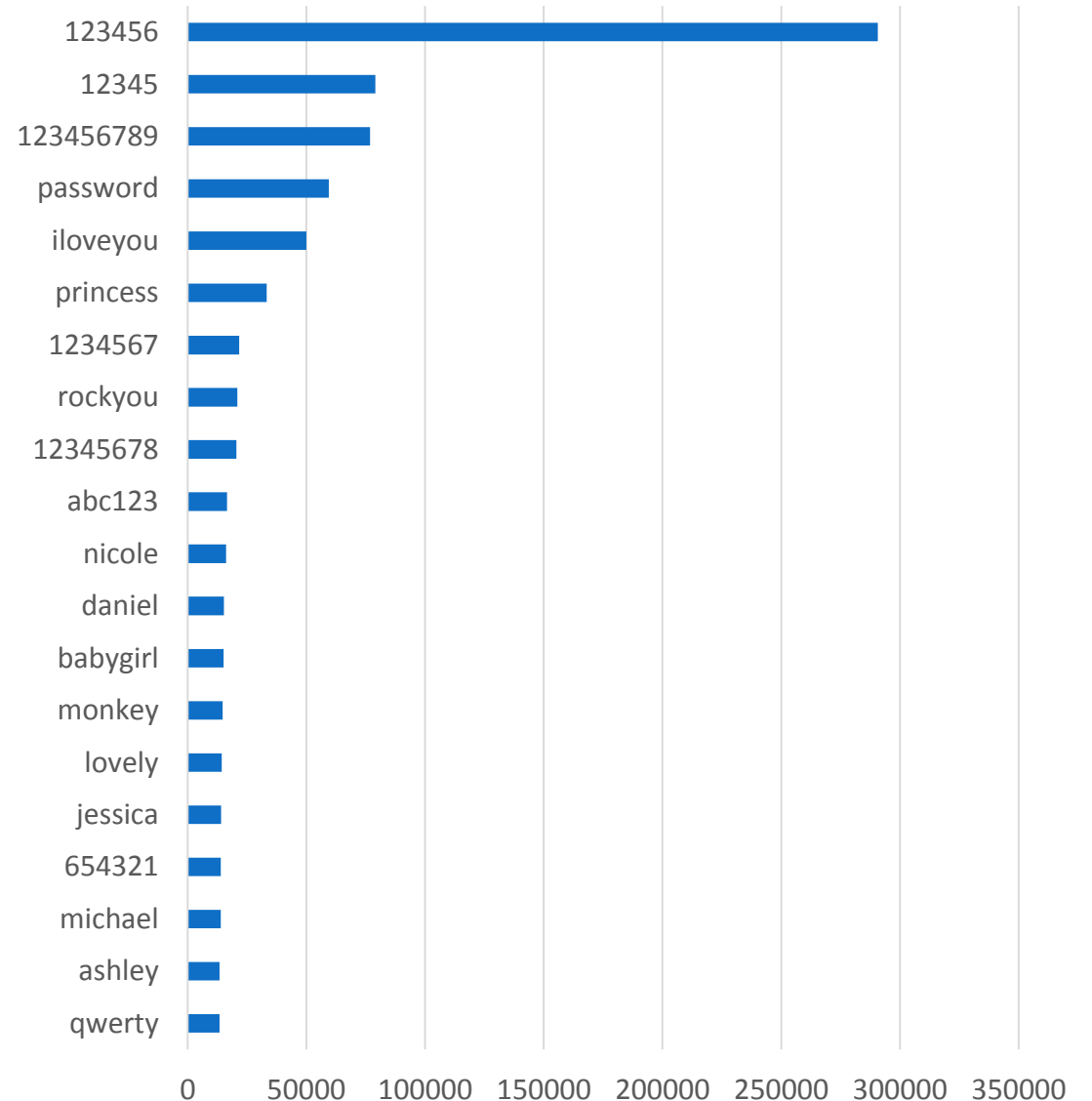
Usability experts tend to leave out very important security steps (like key verification).

Passwords

Passwords

- Most popular method of authentication
 - A character string (password) is agreed upon between the user and the system
 - User proves their identity by providing the password
- Convenient system design
 - Easy to store encrypted
 - Easy to enter on many systems
 - No special equipment needed
 - Scales well
- Problem: people choose easy to guess passwords
 - Low entropy, so easy to guess
 - Hard to remember

Most common passwords in RockYou data



Rockyou

Count	Password
290729	123456
79076	12345
76789	123456789
59462	password
49952	iloveyou
33291	princess
21725	1234567
20901	rockyou
20553	12345678
16648	abc123
16227	nicole
15308	daniel

Phpbb

Count	Password
2650	123456
1244	password
708	phpbb
562	qwerty
418	12345
371	12345678
343	letmein
313	111111
273	1234
253	123456789
224	abc123
223	test

Myspace

Count	Password
75	password1
56	abc123
34	fuckyou
29	monkey1
28	iloveyou1
24	myspace1
24	fuckyou1
18	number1
18	football1
17	nicole1
17	123456
16	iloveyou2

Standard password guidance

What does a **good** password look like?

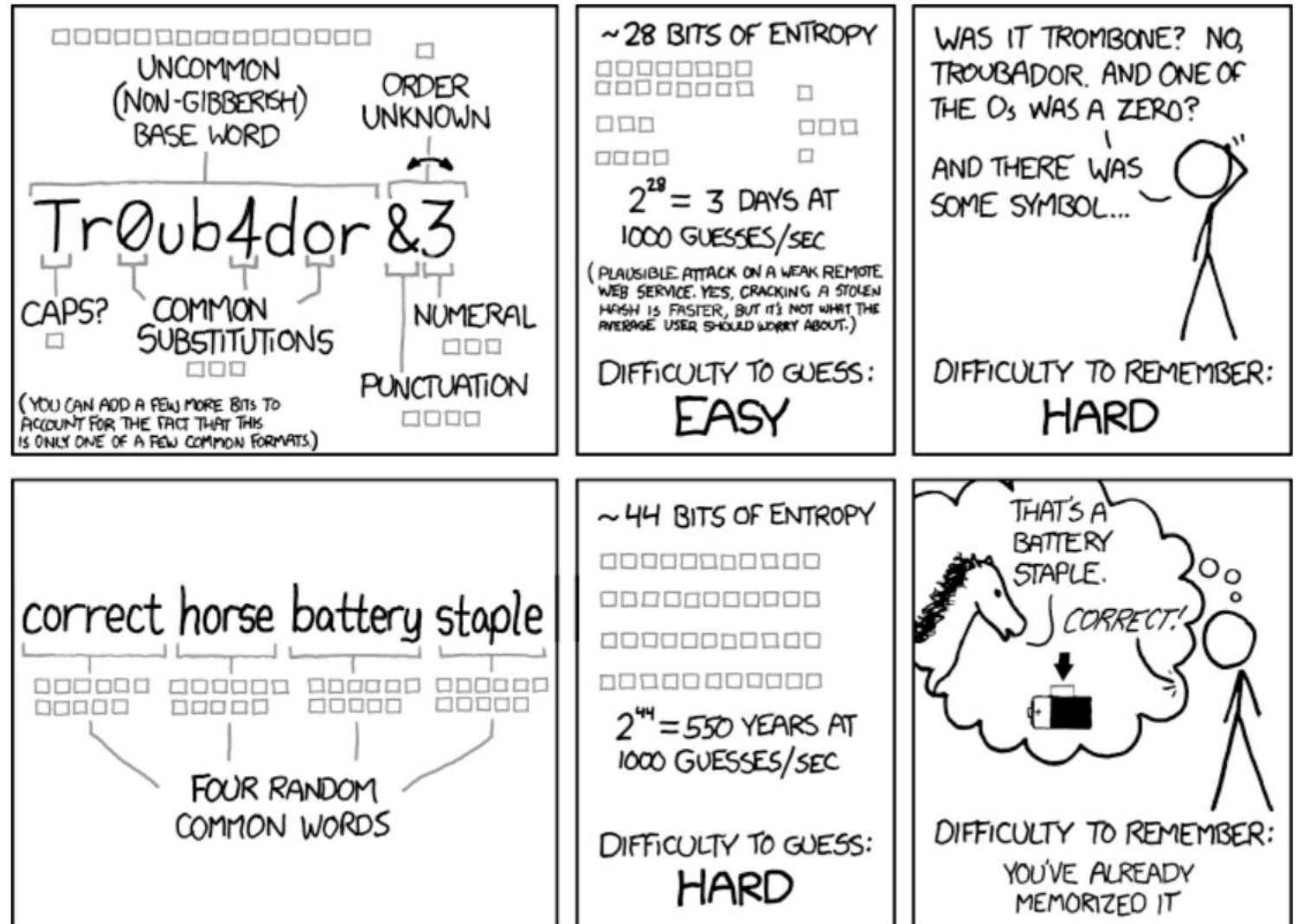
- At least 8 characters, longer better
- No words (any language, especially English)
- Avoid common patterns
 - Upper case letter as first letter
 - Putting the number at the end
 - Putting the special character at the end
- High entropy
 - Lowercase letters
 - Upper case letters
 - Numbers
 - Special characters

What does a **bad** password look like?

- Short
- Easy to guess (significant other attack)
- Uses common patterns
- Low entropy
 - Word (in any language)
 - Same combination other people use

Password entropy

- A good password should be drawn randomly from a large set of possible passwords
- A bad password is drawn from either a small set or not randomly



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

UK guidance on simplifying passwords

1. Change all default passwords
2. Help users cope with password overload
3. Understand the limitations of user-generated passwords
4. Understand the limitations of machine generated passwords
5. Prioritize administrator and remote user accounts
6. Use account lockout and protective monitoring
7. Don't store passwords as plain text

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf

Common (possibly wrong) wisdom

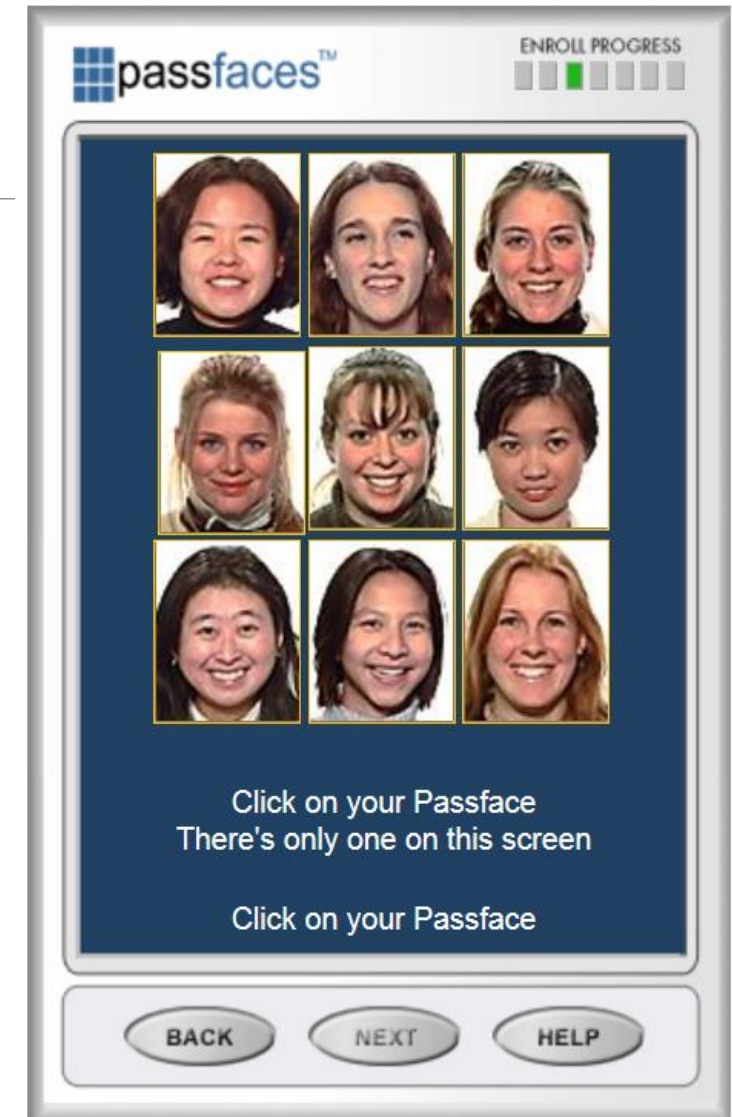
- Reset passwords every 30 days
- Use long passwords
- Use a different password for every site
- Don't ever give out your password
- Don't use easy to guess passwords

User generated passwords

- People are somewhat ok at generating passwords they can remember
- People are bad at generating passwords that are hard to guess
- User-generated passwords:
 - Low entropy
 - Tend to have facts about themselves such as their pet's name
 - Guessable by someone who knows them
 - Easy to lookup in a password dictionary

PassFaces

- Humans are better at recognizing things than they are at recalling information.
- High feature information, like faces, are easier to recognize
- Idea: Use high feature information as the pin, so humans can recognize their password
- Problem: People select faces that mean something to them. If you know basic characteristics about someone you can easily guess their PassFace.



PassFaces

- Password length = 4
- Each password selected from a set of 9 faces like what is shown on the right
- Theoretical password space = 6561
- What is the best way to break someone's password?
 - If the person is a white male, you can guess the correct password in about two guesses by selecting all the pretty white females.



Machine generated passwords

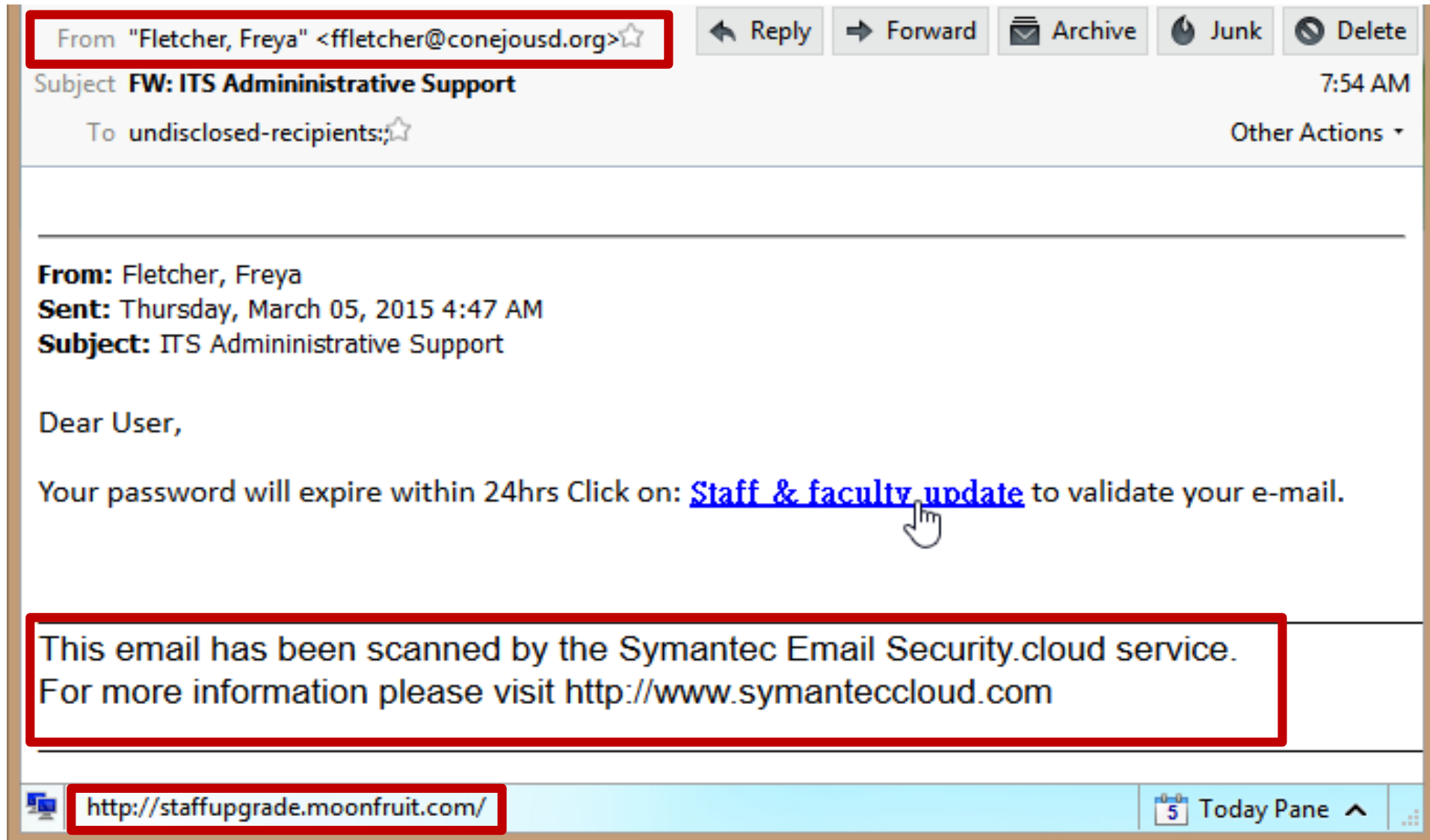
- Computers are better at selecting passwords that are challenging for other computers to guess
- Computers are less good at selecting passwords that are easy to remember
- Tactics:
 - Some algorithms produce passwords which are pronounceable, or are made up of words (correct battery horse staple)
 - Let users choose from a small number of passwords

Phishing

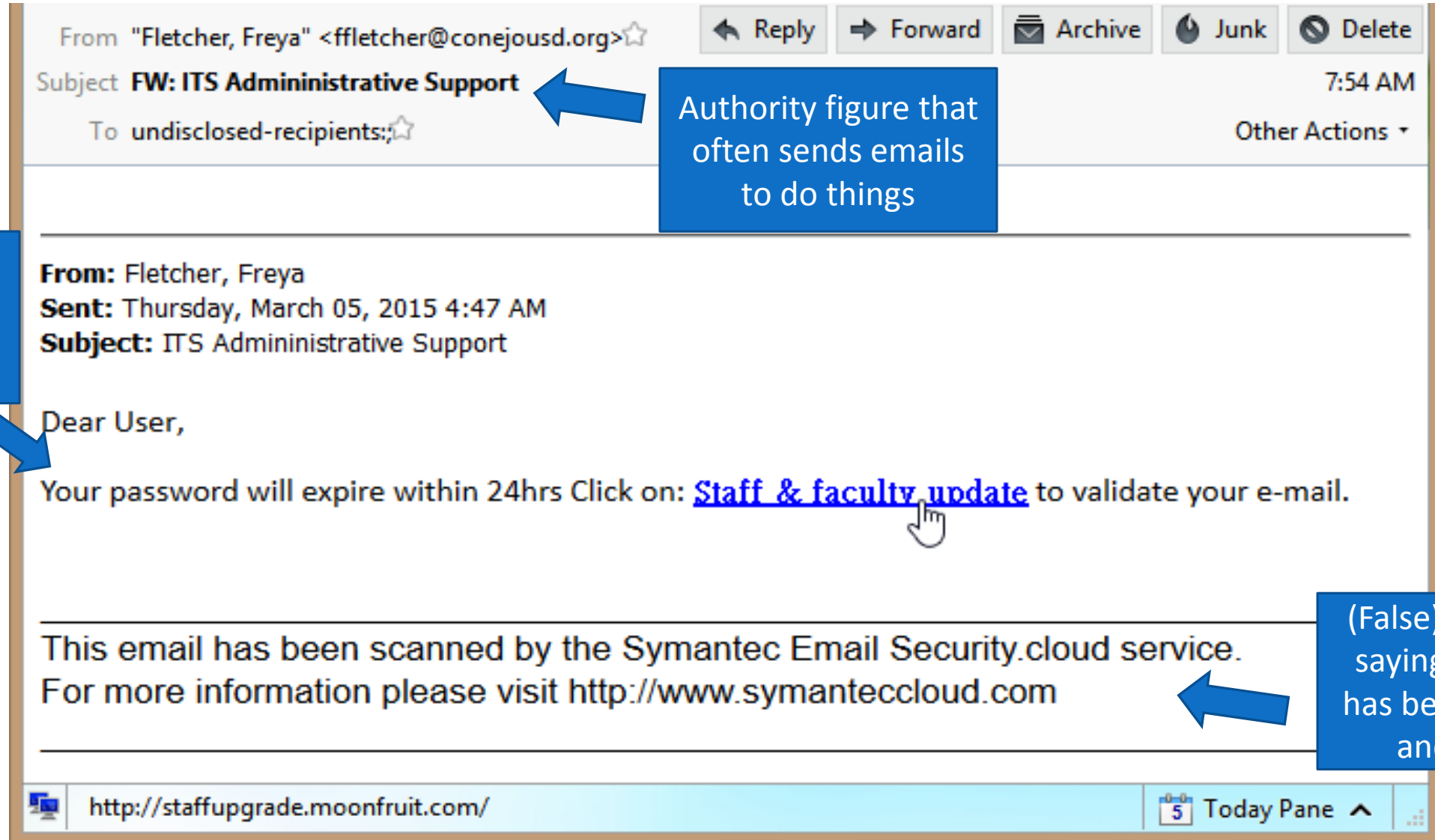
Phishing

- Phishing – Attempting to trick someone into taking the “bait” and interacting in a way they should not.
 - Typically involves the impersonator pretending to be someone else that the person trusts
 - Interactions: Clicking a link, opening a file, replying with information, transferring money, ect.
- Spear phishing – Phishing, but with a small number of targets and each email is crafted for that individual
- Whaling – Phishing for people with a lot of money, i.e. CEO
- QRishing – Phishing attacks through QR codes

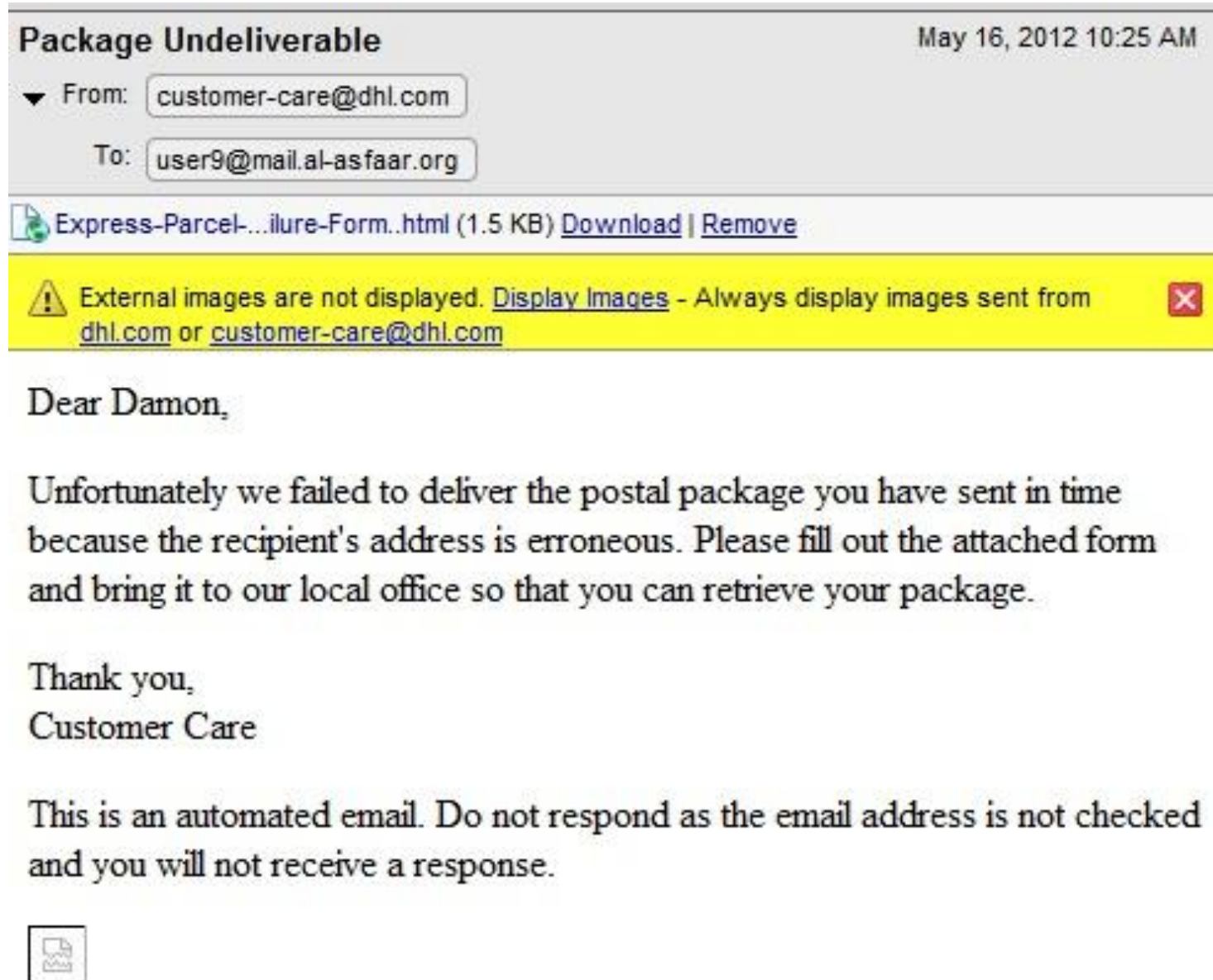
What on this email can be trusted?



(Wrong) Trust indicators



Sneaky email
to get the
recipient to
open the
attachment,
which is an
html document

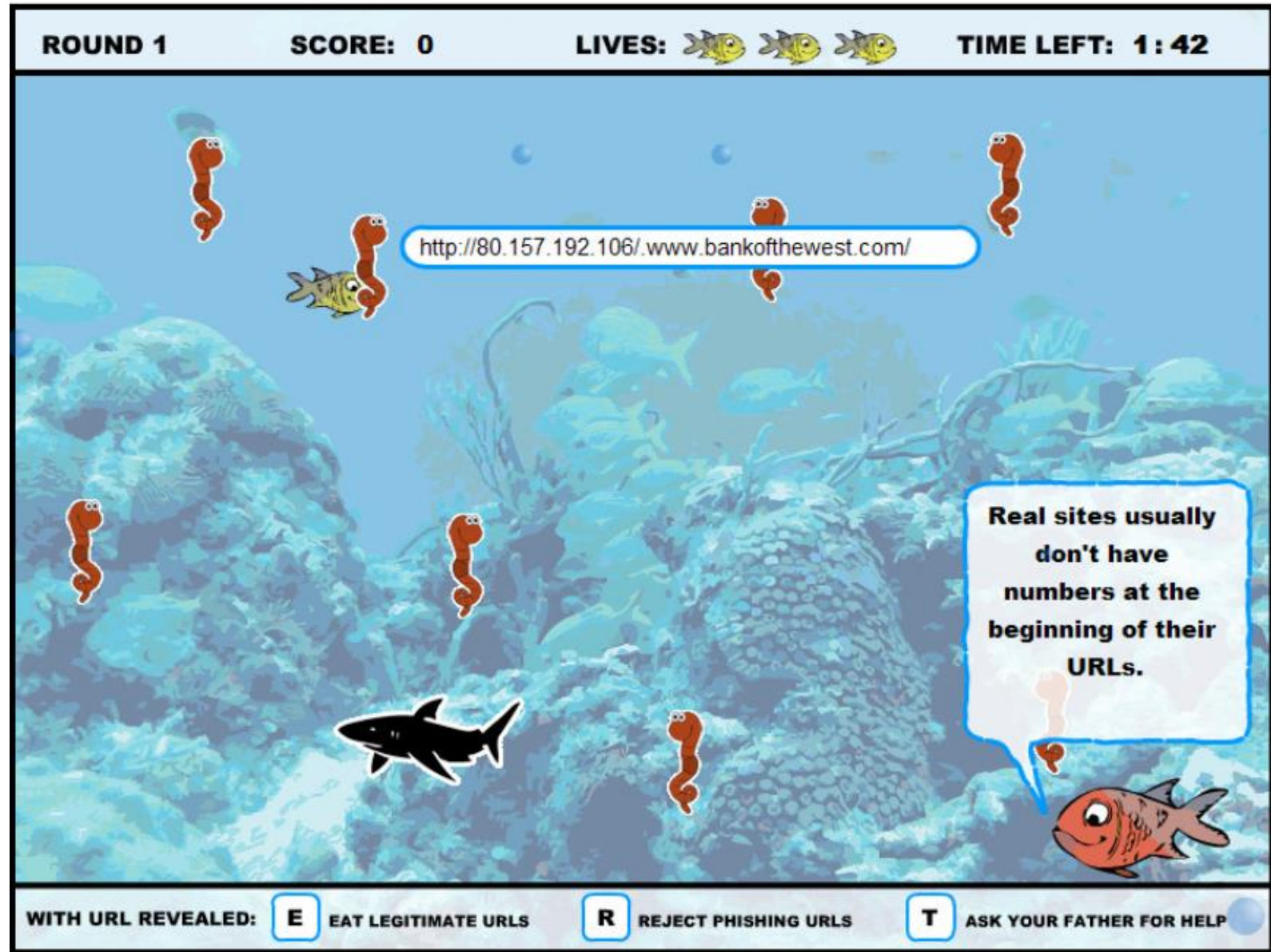


Problem: Users click on links and attachments

- Scan all incoming attachments and links for blacklisted content
- Teach users
 - Only click if you are expecting the email
 - Do not open attachments unless you are expecting them
 - If you are not sure, contact the person or company separately and ask if they sent the email
 - If you are not sure, contact the IT department
 - Banks and credit card companies will never contact you this way

Anti-Phishing Phill

- Serious game to help people learn to spot dangerous URLs
- Training sometimes works
- But it takes time
- And people forget



PhishGuru

- Comic to train people to spot phishing attacks
- Best time to train is after a users has already fallen for an attack
- Send out fake attacks and train those who click on them

Carnegie Mellon The PhishGuru Protect yourself from Phishing Scams



WARNING!

Clicking on links like the one in the email you've just read puts you at risk for identity theft. A phishing scam uses fraudulent email and web pages to steal bank account information, passwords, and other confidential information.

How you were tricked



How to help protect yourself

- 1 Don't trust links in an email.
<http://www.wombank.com/update>
- 2 Never give out personal information upon email request.
Name: Jane Smith
SSN: 123 456 789
- 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-xxxx

- 6 Don't open unexpected email attachments or instant message download links.

My Inbox

Here is the updated document.

[attachement](#)

How phishers trick you



Thanks PhishGuru!
Where can I learn more?

Visit
phishguru.org

Give users options that make sense and work for them

PhishGuru

- Users know what they are expecting
- Users know who the email looks like it is from
- Users can do an out-of-band contact (phone call)
- Users do not want to ignore a serious issue



WARNING

Clicking on links in emails puts you at risk for identity theft and financial loss. This tutorial was developed by Wombat Security Technologies to teach you how to protect yourself from phishing scams.



Don't open or install email attachments unless they were sent by someone you know and you were expecting them. Verify with the sender that they intended to send the attachment.



I forged the address to look genuine.
I threatened the user with an urgent message.
I added an attachment to collect sensitive information.



To learn more about protecting yourself from phishing scams visit <http://www.phishguru.org>

In Summary...

- Academics say in-the-moment training works
- Chief Security Officers (CSOs) have mixed opinions
- Everybody thinks that users clicking on links and attachments is a big problem

Warnings and communication

Why show warnings at all?

- Determined users might disable Safe Browsing. Which would prevent future warnings.
- User could also open the website in another browser that is less safe and does not block the website.
 - America Online users used to go to a friend's house to open malicious sites because the ISP blocked malicious sites.
 - Different browsers block different sets of sites, we don't want to teach users to use less safe browsers.

Chrome malware warning

- Huffington post was blocked because a content provider images.buddytv.com had malware

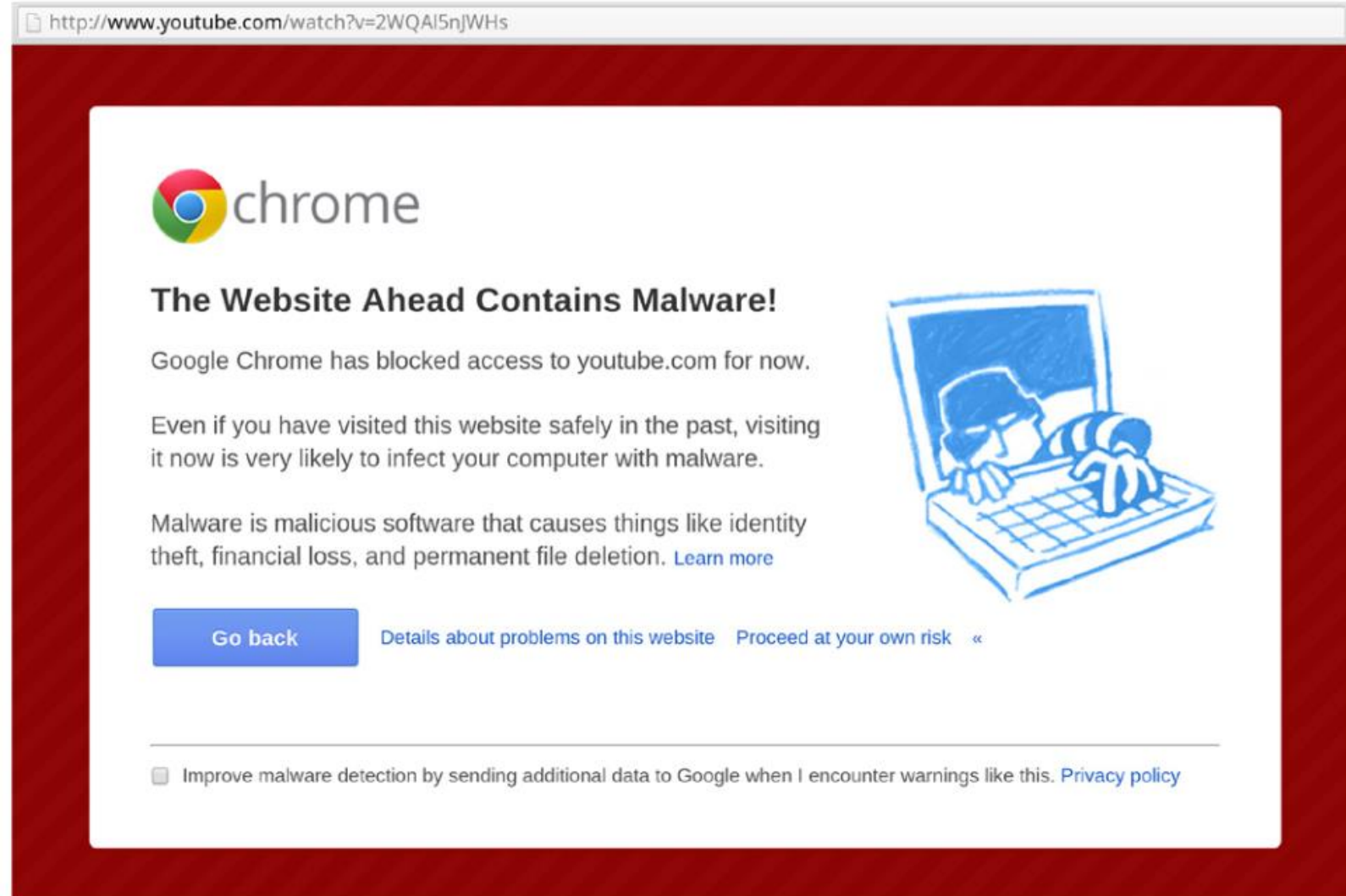


Why do people click through the warnings?

- The site is used often and trusted
 - “YouTube is a well known website. I’d assume that the malware block is in error.”
- The person who posted the link is trusted
 - “I find it harder to believe [the warning] when my facebook friend just posted it and had no problems.”
- The site where the link is assumed to have good security
 - “I presume that visiting youtube from a facebook link would be safe.”
- They think they are safe
 - “I use Linux I’m not afraid of anything.”
 - “I have an anti virus”

Improved warning

- Added “for now”
- Added “even if ... visited safely in the past”
- Consider special warning for common websites

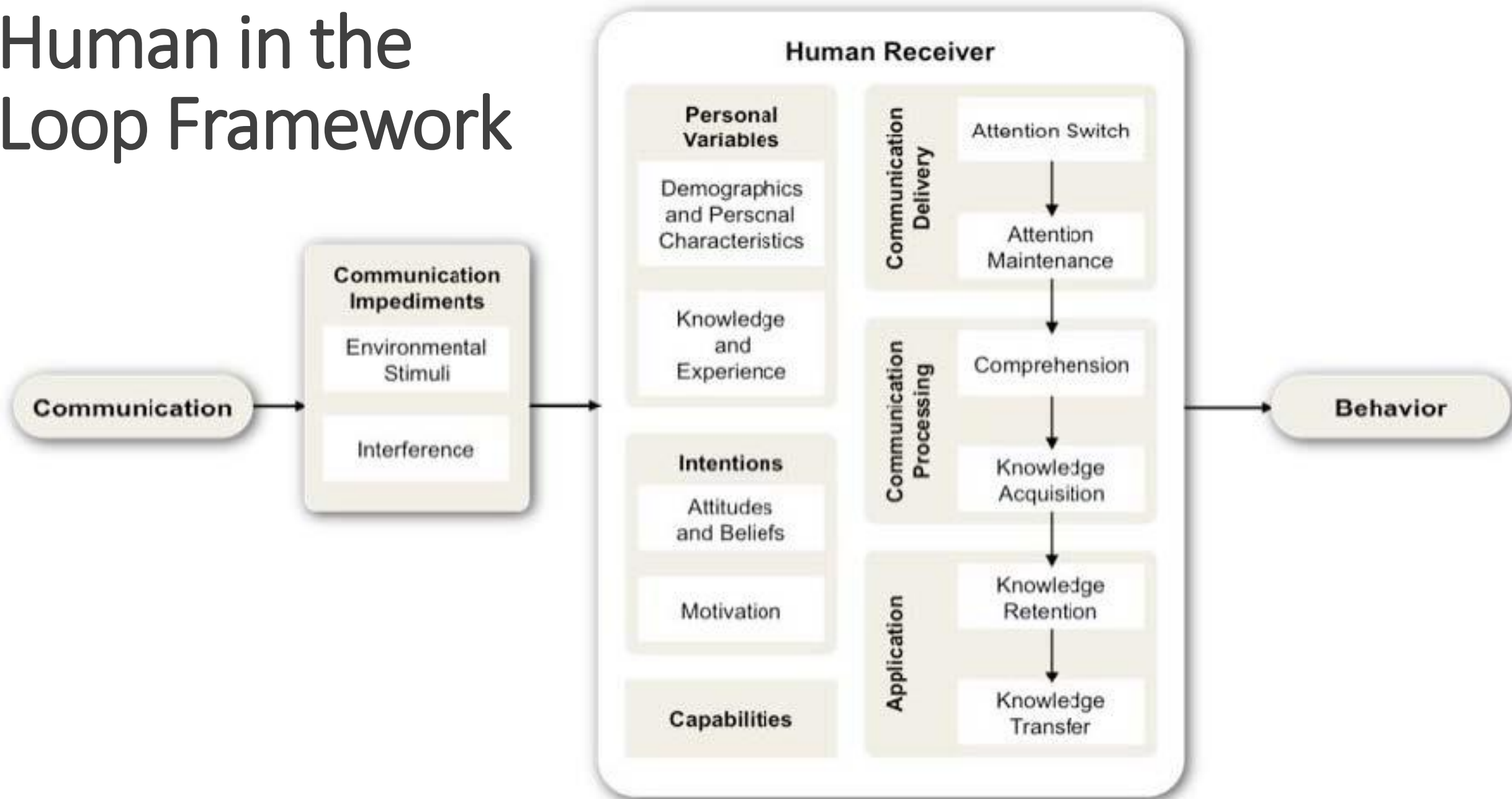


Are users correct to ignore the warnings?

- Studied TLS activity of more than 300,000 users
 - Collected certificates passively at egress points of 10 network sites
 - Over 9 month period
 - Validated certificate chains using local browser logic
 - 98.46% of the filtered connections validate correctly, implying a false warning rate of 1.54%
- In a scenario with a hypothetical Man-In-The-Middle chance of 1 in 1,000,000
 - 1,000,000 connections would produce 15.401 warnings
 - Out of which 15.4 would be false warnings

Devdatta Akhawe, Bernhard Amann, Matthias Vallentin, and Robin Sommer; Here's My Cert, So Trust Me, Maybe?
Understanding TLS Errors on the Web, 2013

Human in the Loop Framework



Account activity for September 2016 - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Get Messages Write Chat Address Book Tag

From squinney@inf.ed.ac.uk

Subject **Account activity for September 2016** 11:04 AM

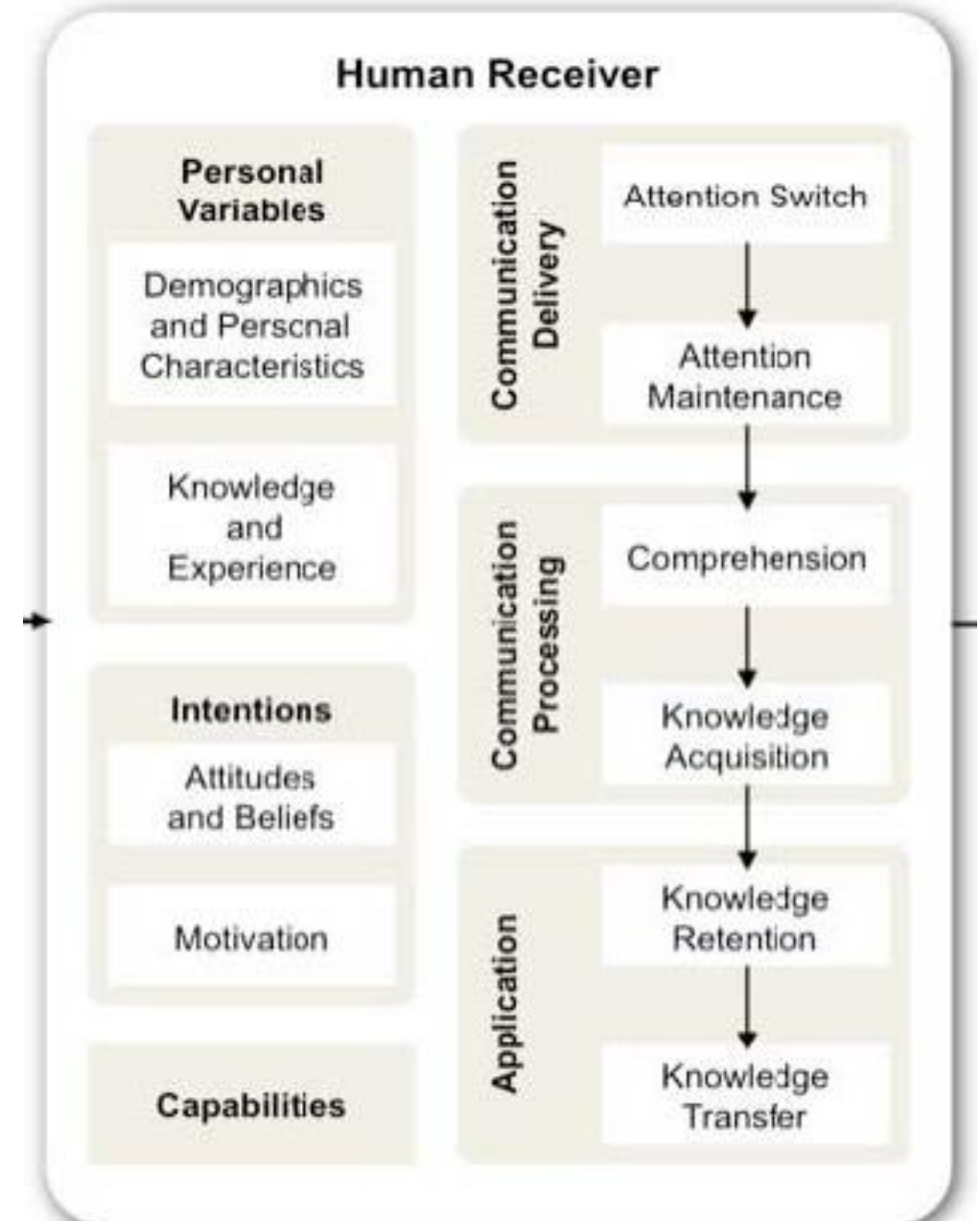
To Me <Kami.Vaniae@ed.ac.uk>

This is a regular monthly email from the School of Informatics Computing Team which summarises your recent account activity. For the month of September 2016 your account 'kvaniea' was used to access Informatics computing resources from remote locations on 84 occasions.

Please review all these hosts listed below and check for any activity which appears to be unusual (i.e. logins from locations you do not recognise).

- 5ac68545.bb.sky.com (Cosign: 11, SSH: 21)
- 5ac8e505.bb.sky.com (Cosign: 13, SSH: 16)
- 172.20.107.180 {EdLAN} (SSH: 4)
- 172.20.105.173 {EdLAN} (Cosign: 3)
- 172.20.107.42 {EdLAN} (SSH: 2)
- 94.197.120.234.threembb.co.uk (Cosign: 2)
- 172.20.104.174 {EdLAN} (Cosign: 2)
- 172.20.104.182 {EdLAN} (SSH: 1)
- 94.197.120.37.threembb.co.uk (SSH: 1)
- 172.20.104.14 {EdLAN} (Cosign: 1)
- 172.20.105.217 {EdLAN} (Cosign: 1)
- 172.20.106.190 {EdLAN} (SSH: 1)
- 172.20.106.229 {EdLAN} (Cosign: 1)
- 172.20.106.255 {EdLAN} (Cosign: 1)
- 172.20.110.7 {EdLAN} (SSH: 1)
- 172.20.105.98 {EdLAN} (Cosign: 1)
- 172.20.104.83 {EdLAN} (SSH: 1)

For a more detailed view you can access the logs of all authentication



NEAT and SPRUCE

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

NEAT

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

Explained- Does your user experience present all the information the user needs to make this decision? (See SPRUCE)

Actionable – Have you determined a set of steps the user will realistically be able to take to make the decision correctly?

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

SPRUCE

Source – State who or what is asking the user to make a decision

Process – Give the user actionable steps to follow to make a good decision

Risk – Explain what bad thing could happen if they user makes the wrong decision

Unique knowledge the user has – Tell the user what information they bring to the decision

Choices – List available options and clearly recommend one

Evidence – Highlight information the user should factor in or exclude in making a decision

Questions
