

Usable Security and User Training

KAMI VANIEA

JANUARY 25

First, the news...

Tutorial this week: Elevation of Privilege card game

- In tutorial this week we will be playing a game invented at Microsoft Research that helps teams of software engineers and system administrators threat model their systems
- This game requires most of the topics we have covered thus far
 - Definition of security
 - Networking
 - Usable security – helping developers (users) do security
- Tutorial is up, but I do not expect you to have read it in advance of the tutorial

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

Phishing attacks and training

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?

From "Fletcher, Freya" <ffletcher@conejouisd.org> ☆

Subject **FW: ITS Administrative Support** 7:54 AM

To undisclosed-recipients; ☆ Other Actions ▾

From: Fletcher, Freya
Sent: Thursday, March 05, 2015 4:47 AM
Subject: ITS Administrative Support

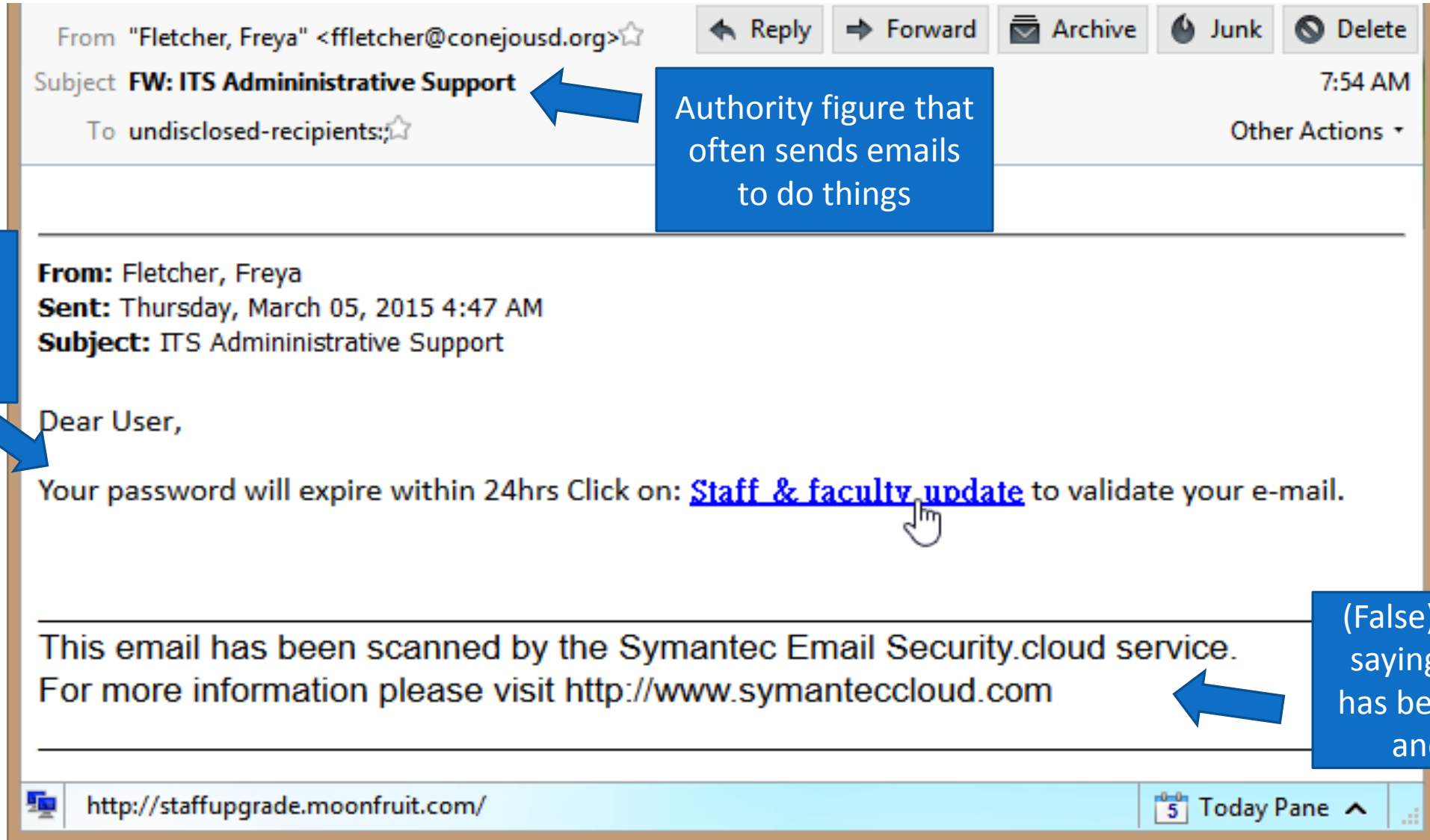
Dear User,

Your password will expire within 24hrs Click on: [Staff & faculty update](#) to validate your e-mail.

This email has been scanned by the Symantec Email Security.cloud service.
For more information please visit <http://www.symanteccloud.com>

<http://staffupgrade.moonfruit.com/> Today Pane ^

(Wrong) Trust indicators



Authority figure that often sends emails to do things

Clear threat to recipient's ability to log in


(False) statement saying the email has been scanned and is safe



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

Package Undeliverable May 16, 2012 10:25 AM

▼ From:

To:

 Express-Parcel-...ilure-Form..html (1.5 KB) [Download](#) | [Remove](#)


 External images are not displayed. [Display Images](#) - Always display images sent from [dhl.com](#) or [customer-care@dhl.com](#) 

Dear Damon,

Unfortunately we failed to deliver the postal package you have sent in time because the recipient's address is erroneous. Please fill out the attached form and bring it to our local office so that you can retrieve your package.

Thank you,
Customer Care

This is an automated email. Do not respond as the email address is not checked and you will not receive a response.

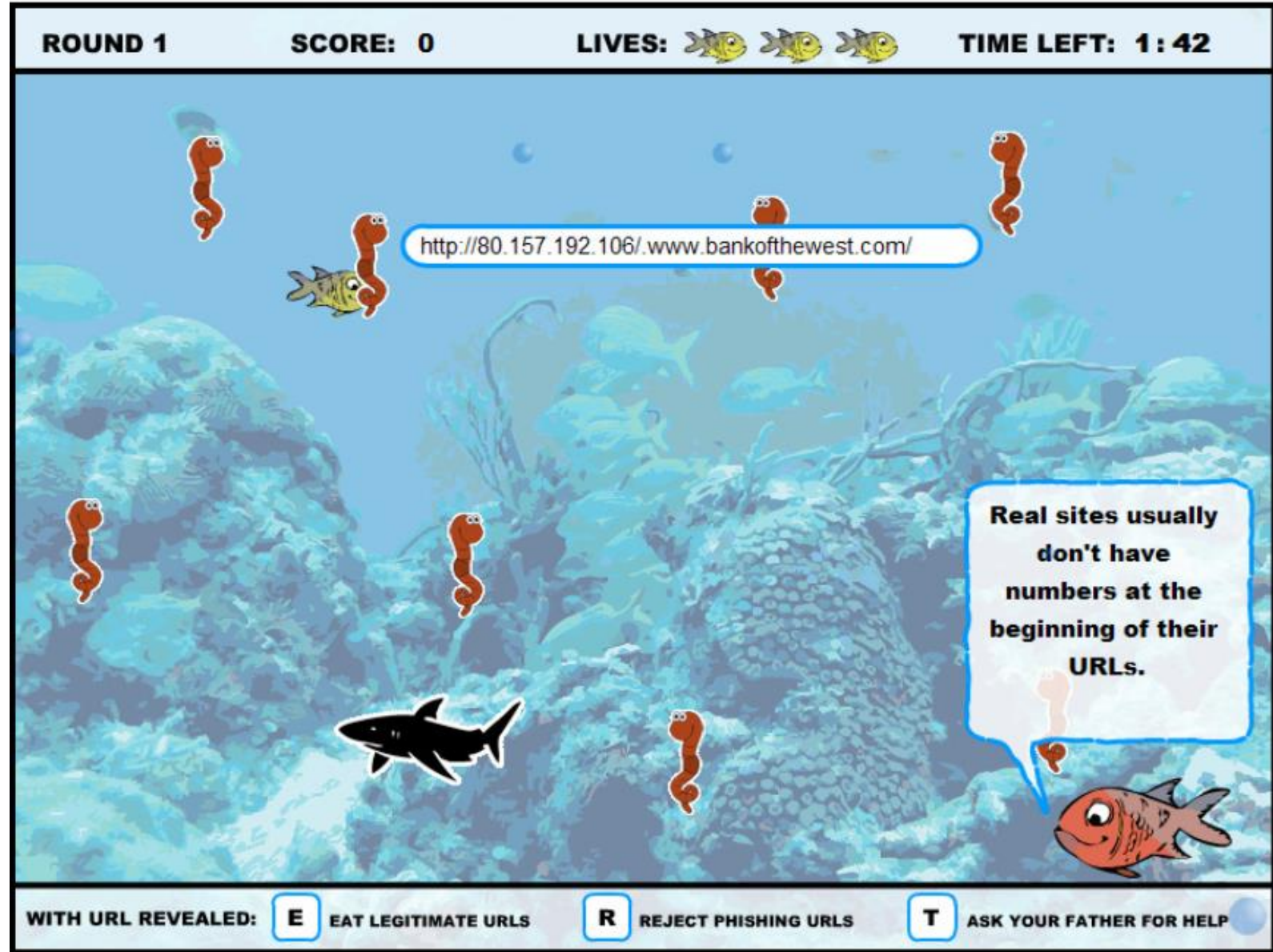


Problem: Users click on links and attachments

- 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

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

STOP!
Don't fall for this scam email.

Wombank
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.
<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.
[attach.pdf](#)

How phishers trick you

Here is how con artists try to steal your personal information.

I forged the address to look genuine.

I threatened the user with an urgent message.

I added a link that looks like it goes to Wombank - but it really sends people to my site so I can steal their information and money!

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

Thanks PhishGuru! Where can I learn more?

Visit phishguru.org

Give users options that make sense and work for them

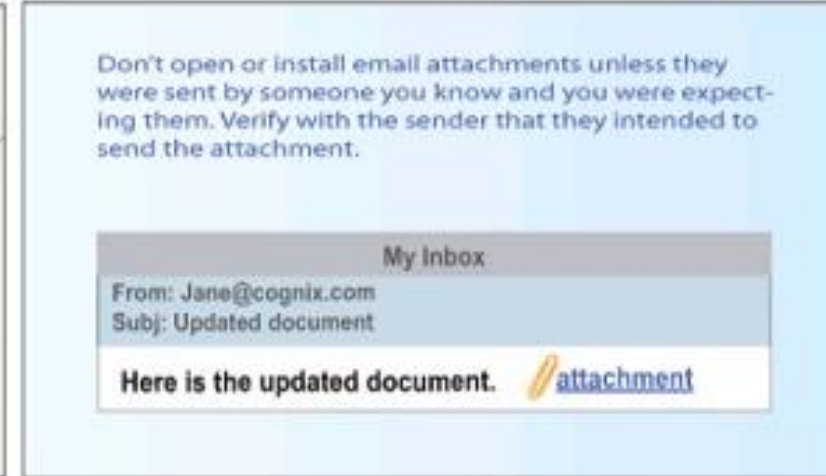
PhishGuru

- 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.



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

SSL and Malware Warnings

Quick explanation of SSL

We will cover this in more detail later

What is the difference?

Online Banking, CDs, Mon... x +

www.ally.com

ally Ally Bank Auto Financing About Ally

Savings CDs IRAs Checking Banking with Ally Open an

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

CDs

Maximize your earnings with our High Yield CDs.

[learn more](#)

Savings

Award-winning savings with no minimum balance.

[learn more](#)

IRA

Get up to a \$500 bonus for a qualifying deposit.

[learn more](#)



Online Banking, CDs, Mon... x +

Ally Financial Inc. (US) | https://www.ally.com

ally Ally Bank Auto Financing About Ally

Savings CDs IRAs Checking Banking with Ally Open an

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

CDs

Maximize your earnings with our High Yield CDs.

[learn more](#)

Savings


Award-winning savings with no minimum balance.


[learn more](#)

IRA

Get up to a \$500 bonus for a qualifying deposit.

[learn more](#)





https://ally.com

versus

http://ally.com

Correctly validated SSL means:

1. The communication between you and this website has been encrypted
 - No one can read what you sent
 - No one can change what you sent
 - Even the NSA has lots of trouble reading https
2. The communication is really from the website and not anyone else
 - If the url says “pnc.com” than it really is from PNC
 - If the url says “pmc.com” then it really is from PMC, which is not a real bank

The computer cannot verify that:

- You intended to go to this site
- The site is safe to visit
- The site has not been hacked
- If you went to pnnc.com the computer will tell you that the connection is safe when likely you shouldn't visit this page

Why would anyone want to see or change my web traffic?

Why would anyone want to see or change my web traffic?

- Marketing reasons
- Replace ads
- Collect information about you
- Impersonate you

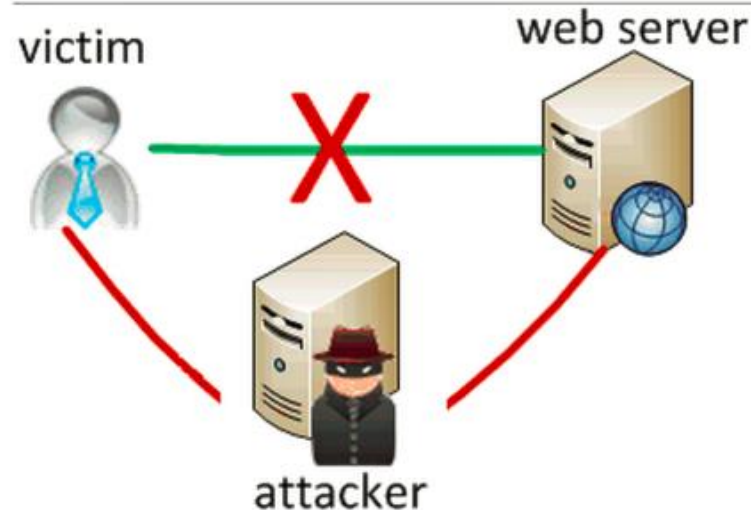
RISK ASSESSMENT / SECURITY & HACKTIVISM

Lenovo PCs ship with man-in-the-middle adware that breaks HTTPS connections [Updated]

Superfish may make it trivial for attackers to spoof any HTTPS website.

by Dan Goodin - Feb 19, 2015 11:36am EST

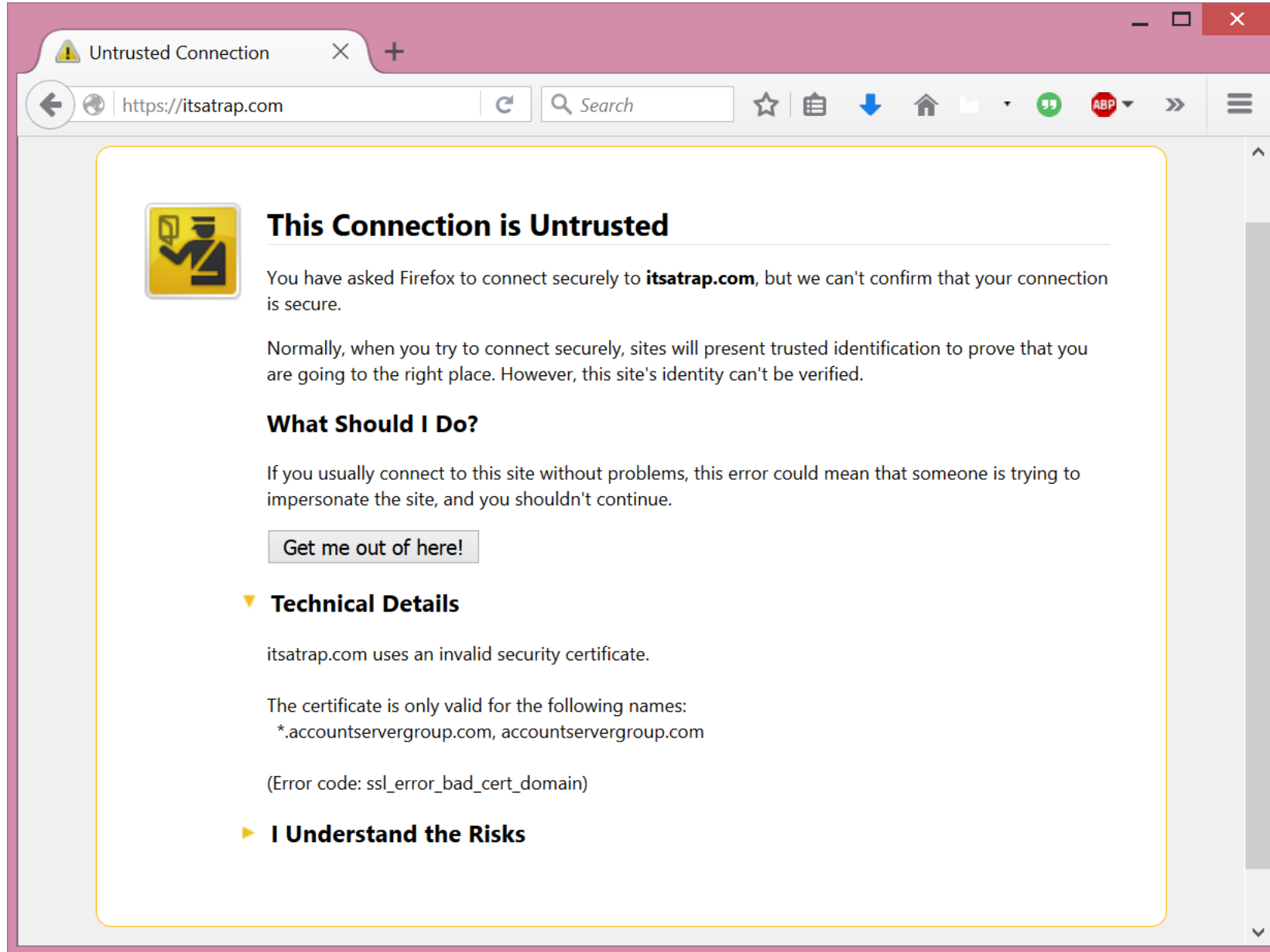
Share Tweet 333



Back to discussing warnings

Firefox SSL warning

- This site is using the wrong SSL certificate. I went to itsatrap.com but the certificate is for accountservergroup.com
- This could be malicious



Untrusted Connection

https://itsatrap.com

This Connection is Untrusted

You have asked Firefox to connect securely to **itsatrap.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

Technical Details

itsatrap.com uses an invalid security certificate.

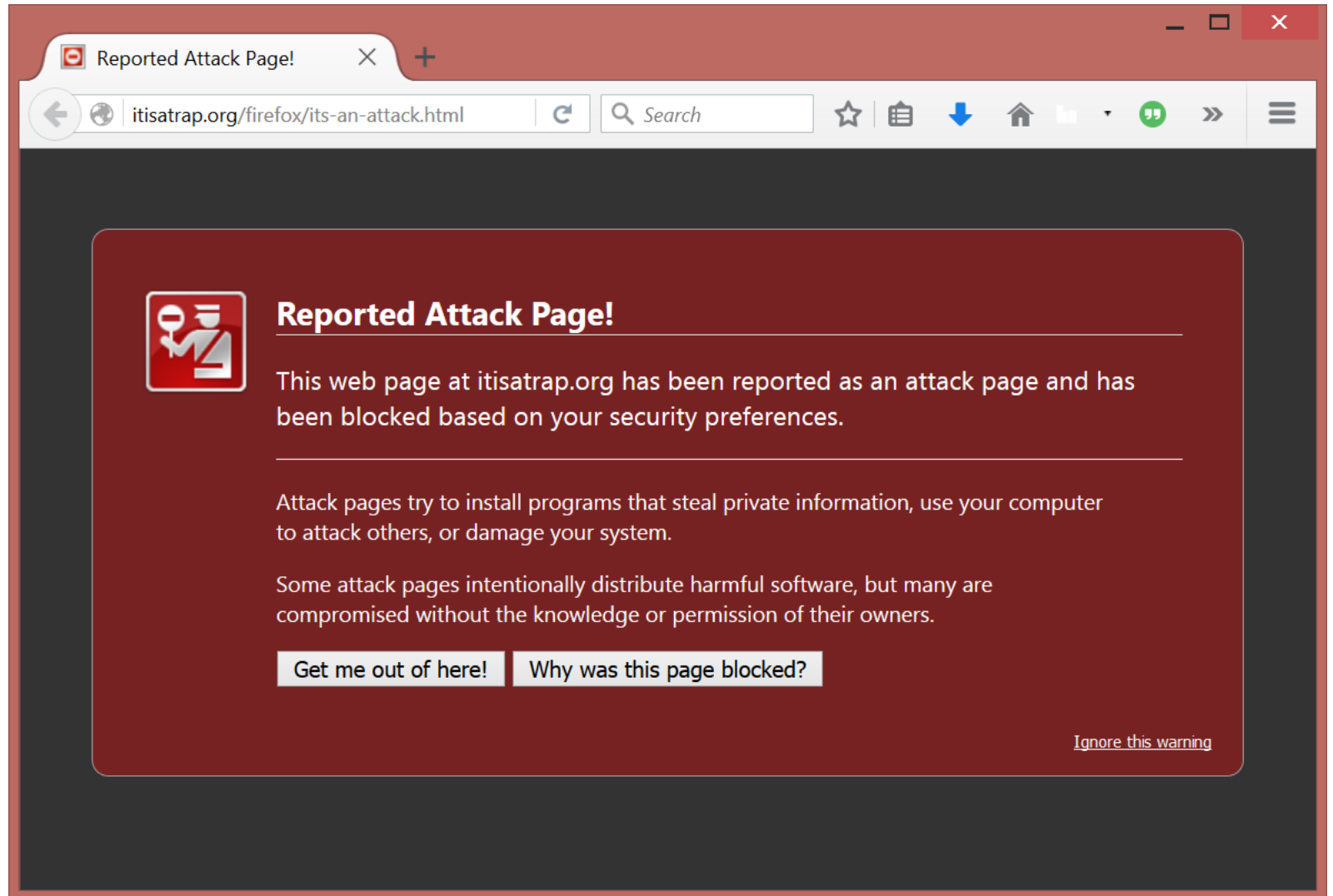
The certificate is only valid for the following names:
*.accountservergroup.com, accountservergroup.com

(Error code: ssl_error_bad_cert_domain)

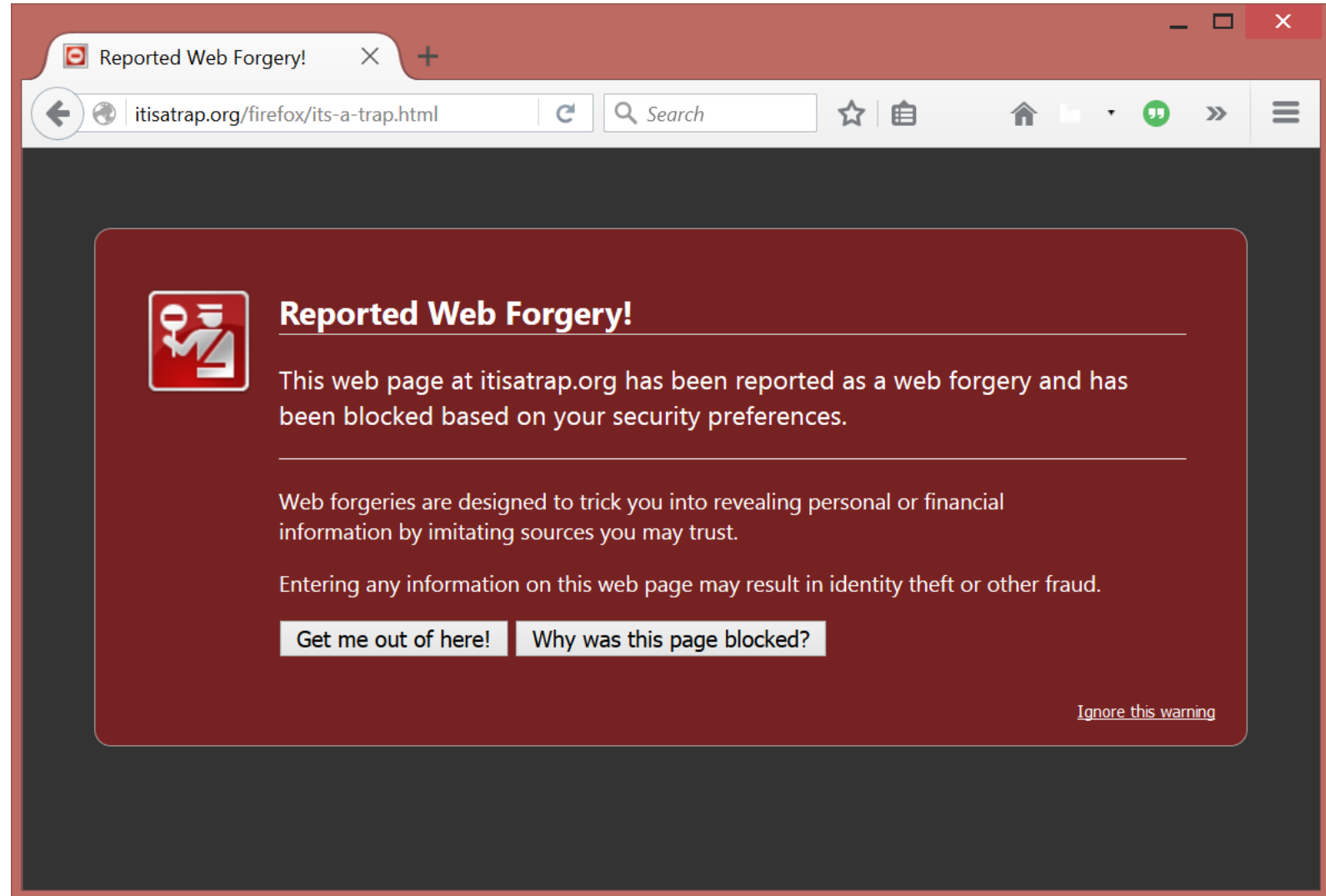
I Understand the Risks

Firefox malware warning

- This page was reported as an attack page
- <http://itsatrap.org> is Firefox's test page for warnings



Firefox phishing warning



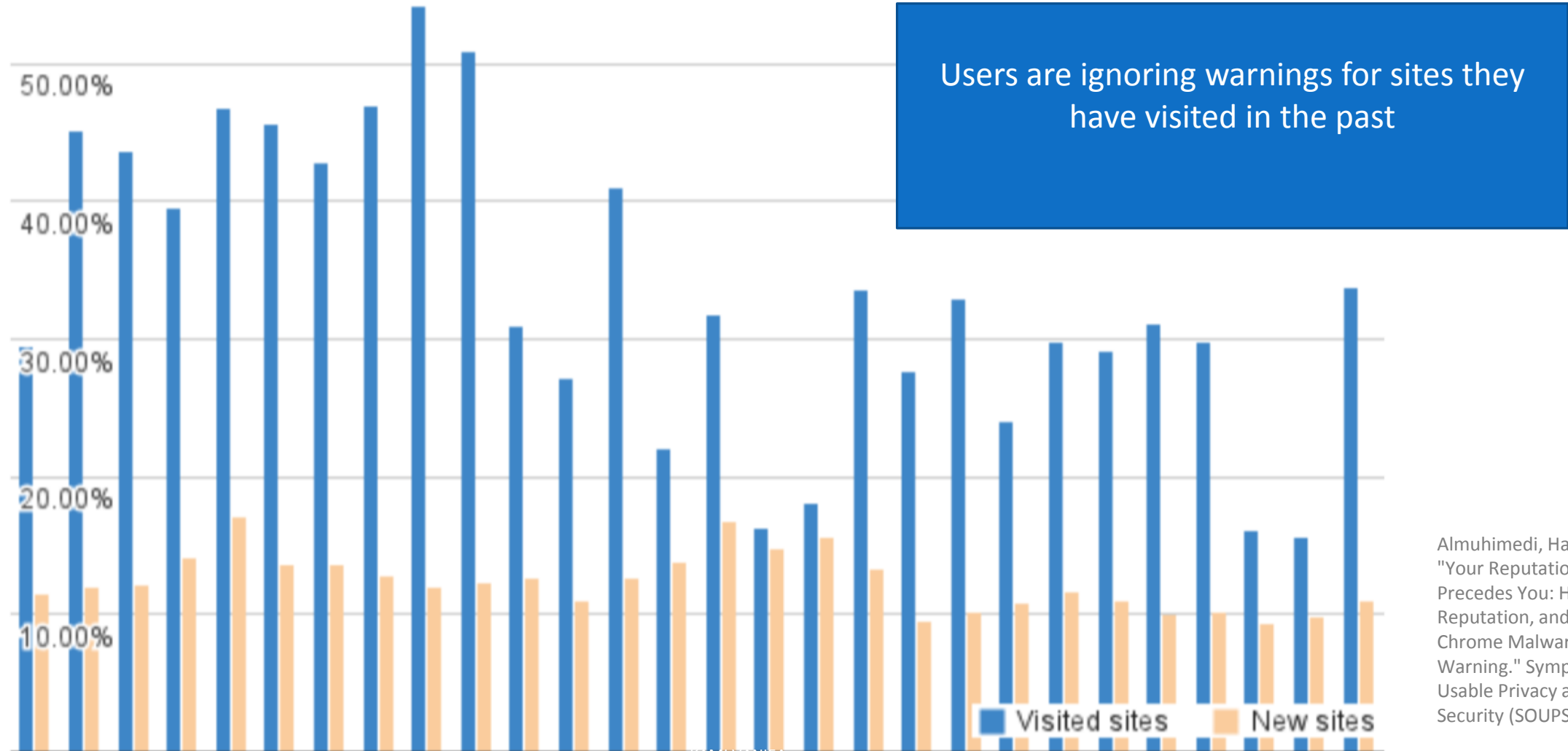
Why show warnings at all?

- 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.

Real world analysis

- Studied the click-through rate for malware and HTTPS warnings
- Malware
 - Firefox 7.2%
 - Chrome 23.2%
- Phishing
 - Firefox 9.1%
 - Chrome 18.0%
- HTTPS
 - Firefox 33.0%
 - Chrome 70.2%

Click through rates based on if the user had visited the site in the past



Almuhimedi, Hazim, et al. "Your Reputation Precedes You: History, Reputation, and the Chrome Malware Warning." Symposium on Usable Privacy and Security (SOUPS). 2014.

Chrome malware warning

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



 chrome

Danger: Malware Ahead!

Google Chrome has blocked access to this page on www.huffingtonpost.com.

Content from images.buddytv.com, a known malware distributor, has been inserted into this web page. Visiting this page now is very likely to infect your Mac with malware.

Malware is malicious software that causes things like identity theft, financial loss, and permanent file deletion. [Learn more](#)

[Advanced](#)

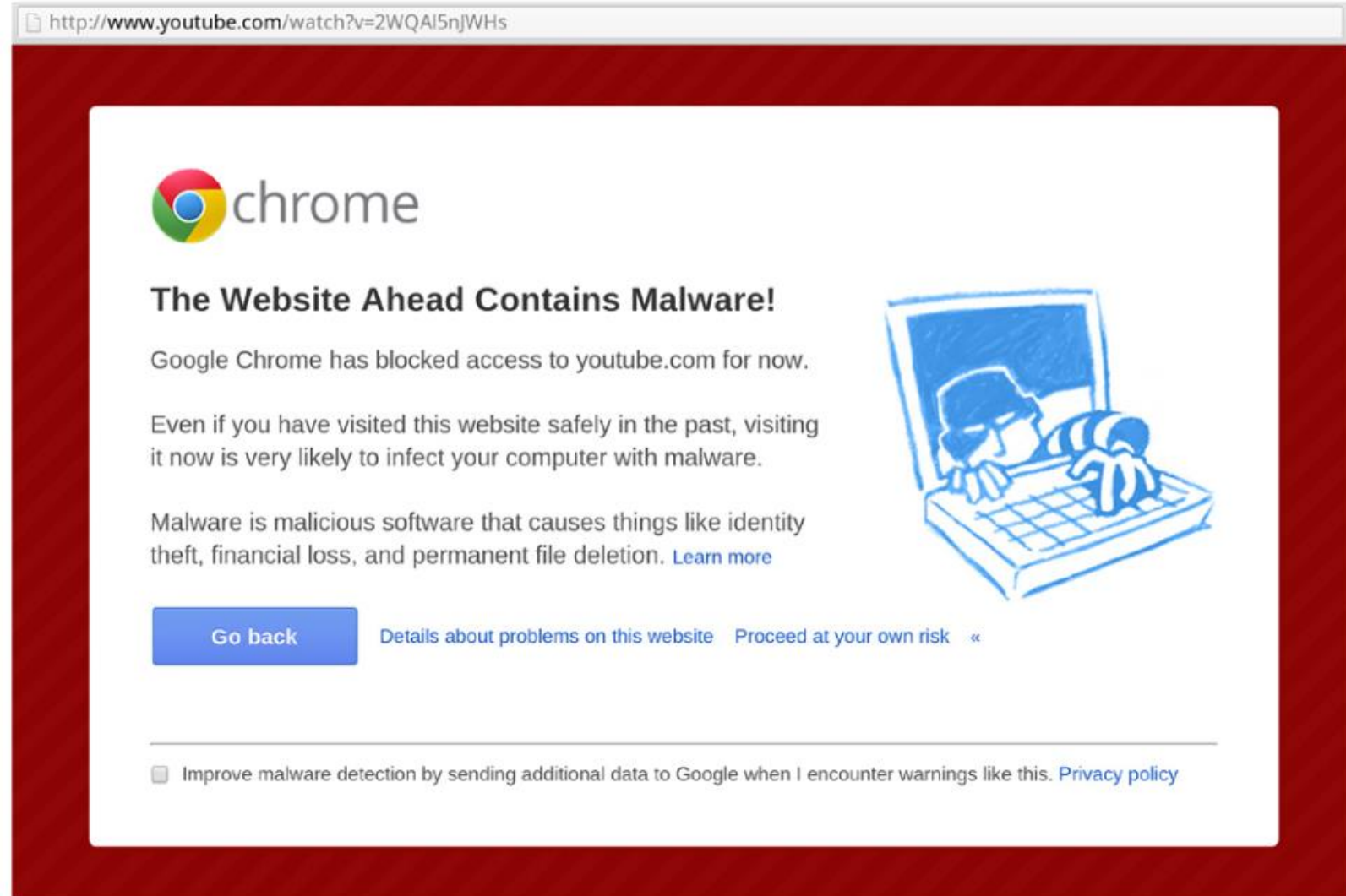
Improve malware detection by sending additional data to Google when I encounter warnings like this. [Privacy policy](#)

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



The screenshot shows a Chrome browser window with the address bar displaying `http://www.youtube.com/watch?v=2WQAI5njWHs`. The main content area has a dark red background and contains the following elements:

- chrome** logo and text.
- The Website Ahead Contains Malware!** (Section Header)
- Text: "Google Chrome has blocked access to youtube.com for now."
- Text: "Even if you have visited this website safely in the past, visiting it now is very likely to infect your computer with malware."
- Text: "Malware is malicious software that causes things like identity theft, financial loss, and permanent file deletion. [Learn more](#)"
- Illustration of a person wearing a mask and sunglasses sitting at a laptop, representing malware.
- Buttons: "Go back", "Details about problems on this website", "Proceed at your own risk" (with a left arrow).
- Footer: A checkbox labeled "Improve malware detection by sending additional data to Google when I encounter warnings like this." followed by a "Privacy policy" link.

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

Writing usable warnings

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

Updating software

a.k.a.

Non-security things that confusingly
impact security

Most attacked software

(Microsoft Security Essentials)

1. HTML / Javascript
2. Java
3. Operating Systems
4. Documents (Adobe Reader, MS Word, etc.)
5. Adobe Flash

Security only impacts security software...wrong!

- ALL software impacts security
- Challenging for a user to understand how display-oriented software impacts security
- Easy to understand how browsers and anti-virus impact security

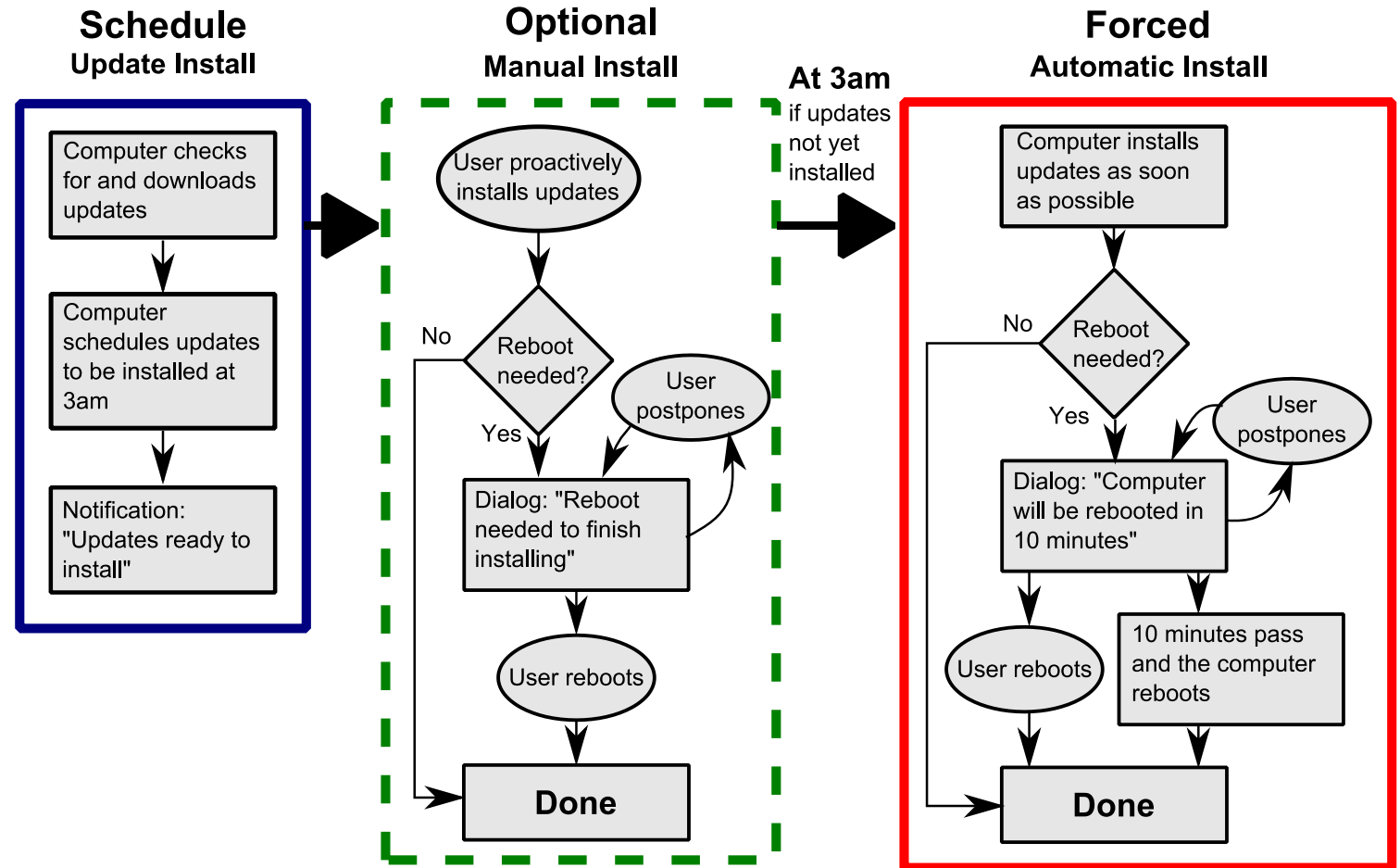
Updating Adobe Reader

“I feel like if I’m really used to the software I’m using and I think it’s meeting my needs I won’t upgrade the software.”

“I just don’t see what an update to [AdobeReader] can do. I mean it’s PDF files. Its viewing them...”

Windows 7 Update flow

- Windows 7 had three update stages with an optional installation in the middle
- Silent security gives users less chance to learn about it making it harder to make good decisions about it



Updates can contain viruses

“I honestly could not tell if it was trustworthy. I did not know if I should accept or not. I chose not and it was a wise choice as a friend told me later it was a virus.”

Users confuse unwanted software with viruses and learn that updates contain viruses

The screenshot shows an update window for Adobe Flash Player. The main content area is divided into three sections. The left section displays the Adobe Flash Player logo and version information. The middle section contains an 'Optional offer' for McAfee Security Scan Plus, which is highlighted with a red border. The right section contains 'Terms & conditions' and an 'Update now' button.

Adobe Flash Player

Version 18.0.0.160
System requirements

Your system:
Windows, English

Are you an IT manager or OEM?

Optional offer:

Yes, install the free **McAfee Security Scan Plus** utility to check the status of my PC security. It will not modify existing antivirus program or PC settings.

McAfee® | Security Scan Plus

[Learn more](#)

Terms & conditions:

By clicking the "Update now" button, you acknowledge that you have read and agree to the [Adobe Software Licensing Agreement](#) and the [McAfee Security Scan Plus License Agreement](#).

Note: Your antivirus software must allow you to install software.

Update now

Total size: 18.38 MB

Developers are also
users

Which line has the fatal flaw? (Trick question)

```
curl_setopt($curlHandle, CURLOPT_SSL_VERIFYPEER, true);  
curl_setopt($curlHandle, CURLOPT_SSL_VERIFYHOST, true);  
...  
// Execute the request  
$response = curl_exec($curlHandle);
```

Which line has the fatal flaw? (Trick question)

```
curl_setopt($curlHandle, CURLOPT_SSL_VERIFYPEER, true);  
curl_setopt($curlHandle, CURLOPT_SSL_VERIFYHOST, true);
```

...

```
// Execute the request  
$response = curl_exec($curlHandle);
```

- CURLOPT_SSL_VERIFYHOST is an Enum (Integer) not a Boolean.
- PHP is not strongly typed so it just casts the Boolean to a Integer.
- True => 1 => Off (1)
- Correct setting is On (2)

Novice developer:

“This app was one of our first mobile apps and when we noticed that there were problems with the SSL certificate, we just implemented the first working solution we found on the internet.”

Intermediate developer:

“We used self-signed certificates for testing purposes and the easiest way to make them working is to remove certificate validation. Somehow we must have forgotten to remove that code again when we released our app.”

Expert developer (kind of):

“[...] When I used Wireshark to look at the traffic, Wireshark said that this is a proper SSL protected data stream and I could not see any cleartext information when I manually inspected the packets. So I really cannot see what the problem is here.”

No.	Time	Source	Destination	Protocol	Length	Info
55	16.352652	127.0.0.1	127.0.0.1	TCP	42836 > 10443	[ACK] Seq=10443
56	16.534849	127.0.0.1	127.0.0.1	SSLv3	Application Data	
57	16.534869	127.0.0.1	127.0.0.1	TCP	10443 > 42836	[ACK] Seq=42836
58	16.537346	127.0.0.1	127.0.0.1	SSLv3	Application Data	Application Data, Appl
59	16.537674	127.0.0.1	127.0.0.1	TCP	42836 > 10443	[ACK] Seq=10443
81	31.540448	127.0.0.1	127.0.0.1	SSLv3	Encrypted Alert	
82	31.540486	127.0.0.1	127.0.0.1	TCP	42836 > 10443	[ACK] Seq=10443
83	31.541069	127.0.0.1	127.0.0.1	TCP	10443 > 42836	[FIN, ACK] Seq=42836
84	31.572562	127.0.0.1	127.0.0.1	TCP	42836 > 10443	[ACK] Seq=10443
91	36.540157	127.0.0.1	127.0.0.1	TCP	42836 > 10443	[FIN, ACK] Seq=10443
92	36.540206	127.0.0.1	127.0.0.1	TCP	10443 > 42836	[ACK] Seq=42836

Transmission Control Protocol, Src Port: 42836 (42836), Dst Port: 10443 (10443), Seq: 806, A

Secure Socket Layer

- SSLv3 Record Layer: Application Data Protocol: http
 - Content Type: Application Data (23)
 - Version: SSL 3.0 (0x0300)
 - Length: 400

Encrypted Application Data: e5e4820b5bac7a02e0950d68ae61e430f7051bab74457210...

Offset	Hex	ASCII
0040	1f dc 17 03 00 01 90 e5 e4 82 0b 5b ac 7a 02 e0 [.z..
0050	95 0d 68 ae 61 e4 30 f7 05 1b ab 74 45 72 10 11	..h.a.0. ...tEr..
0060	10 be f4 00 6a 56 43 dc 50 5f a8 75 5c 83 48 9a	...jVC. P_u.H.
0070	ef 7a 91 66 ba f7 88 bb f8 87 7c 5b b4 f4 a4 dc	.z.f.... [...]
0080	35 8c 90 f7 98 c9 b1 56 44 92 b8 3b d7 3d 75 d0	5.....V D.;=u.
0090	78 c7 1e fd 61 16 2b 68 d6 b7 ae 1e 0f 13 af 0b	x...a+th

Neilson's 10 usability heuristics

Neilson's 10 usability heuristics

- Visibility of system status
- Match between system and the real world
- User control and freedom
- Consistency and standards
- Error prevention
- Recognition rather than recall
- Flexibility and efficiency of use
- Aesthetic and minimalist design
- Help users recognize, diagnose, and recover from errors
- Help and documentation

Questions
