Usable Security and User Training

KAMI VANIEA

JANUARY 25

Think about it:

Is the Doodle link to the right secure?

Sign up for tutorial sessions

`http://doodle.com/poll/t7ia4mbv9vk8ekec`

Link is also available on the website, which is at:

`http://www.inf.ed.ac.uk/teaching/courses/cs/`

First, the news…

- And someone messes up SSL certs again…
  - http://arstechnica.co.uk/security/2016/09/firefox-ready-to-block-certificate-authority-that-threatened-web-security/
  - http://www.theregister.co.uk/2011/08/29/fraudulent_google_ssl_certificate/
  - http://arstechnica.com/security/2015/10/still-fuming-over-https-mishap-google-gives-symantec-an-offer-it-cant-refuse/
  - http://arstechnica.com/security/2015/02/lenovo-pcs-ship-with-man-in-the-middle-adware-that-breaks-https-connections/

Quick explanation of SSL

We will cover this in more detail later

Slides with this background are from a talk given at the Royal Society Frontiers of Science event on why encryption is not adopted at scale

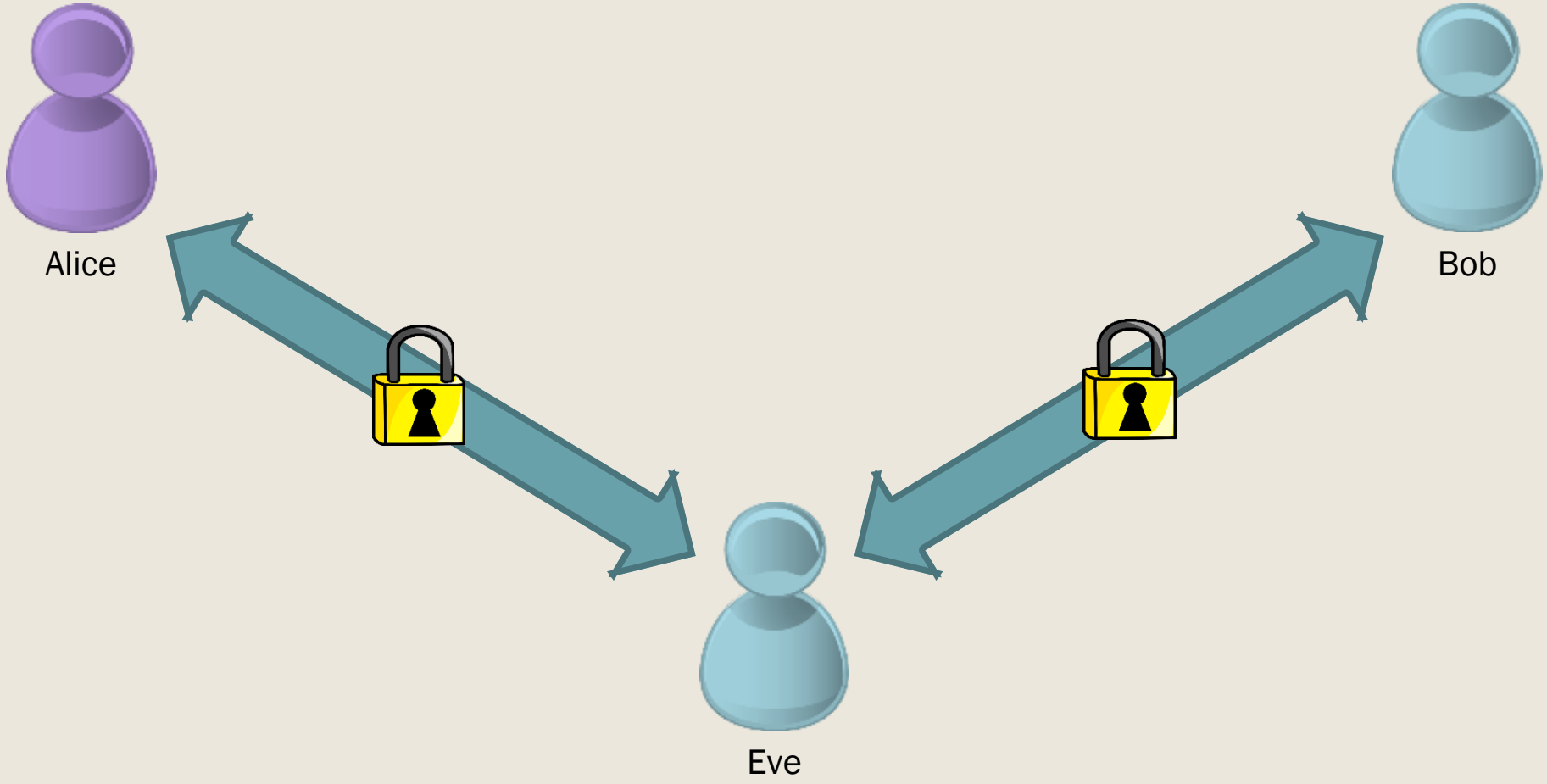
Encryption (in transit) properties we want:

1. The communication between you and the other party is **confidential** and has **not been changed**
   - *No one can read what you sent*
   - *No one can change what you sent*
2. **Knowing who** you are communicating with
   - *You are talking to who you think you are talking to and not someone else*

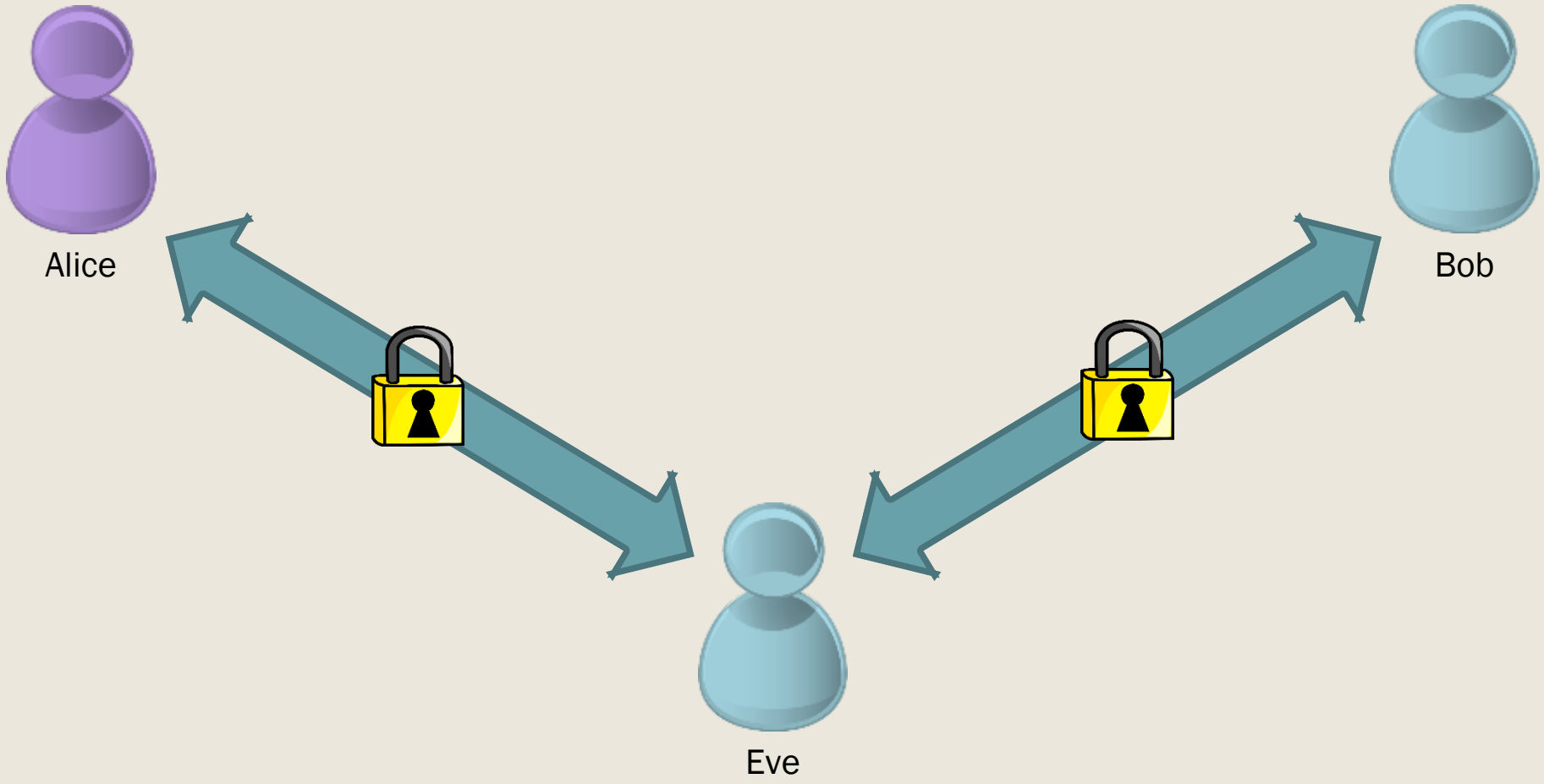
Alice wants to talk securely with Bob

She can encrypt the connection (1)

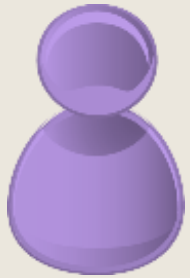
But how can Alice know she is talking to Bob and not talking to Eve? (2)



Man in the middle attack

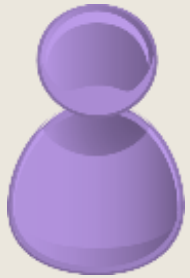


Alice goes to her favorite coffee shop and tries to visit BBC News



Alice

BBC NEWS



Alice

UK - BBC News

www.bbc.com/news/uk

Search

BBC | News | Sport | More | Search

NEWS

Home | Video | World | US & Canada | UK | Business | Tech | More

UK | England | N. Ireland | Scotland | Wales | Politics

Osborne unveils sugar tax on soft drinks

George Osborne unveils a tax on the makers of soft drinks - and warns of the risks of leaving the EU in his eighth Budget.

20 minutes ago | UK Politics

LIVE Budget 2016 Live

Growth forecasts cut

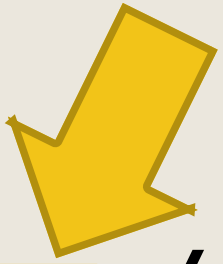
Budget key points: At-a-glance

'On course for a surplus'

BBC NEWS


STARBUCKS
Google
WIFI
GOOD MORNING
Google
WIFI
¡HOLA
Free Wi-Fi
From our friends at Google
Accept & Connect
I agree to the Terms of Service and have reviewed the Google Privacy Policy
Need help? 855-446-2374

Benign Main-in-the-Middle

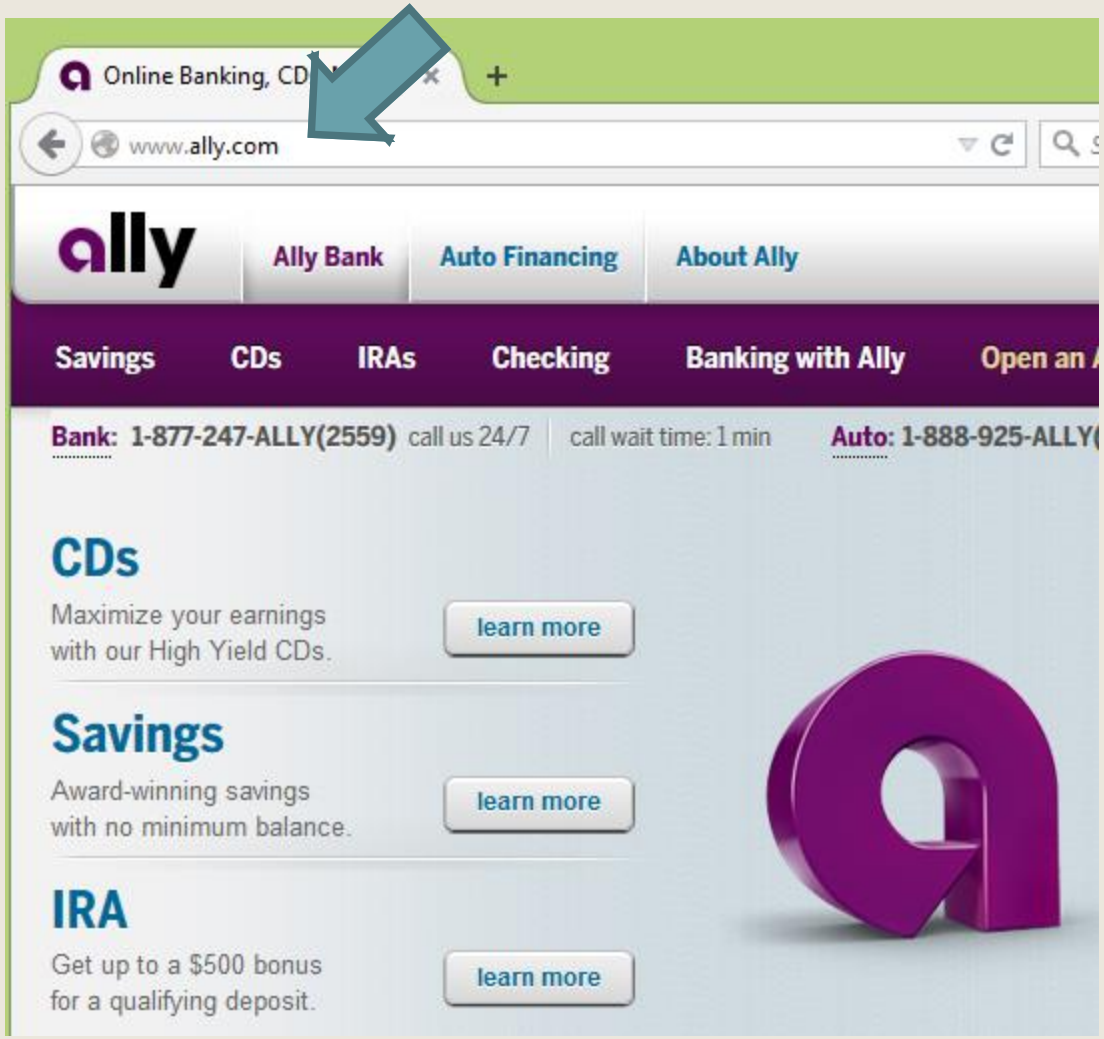


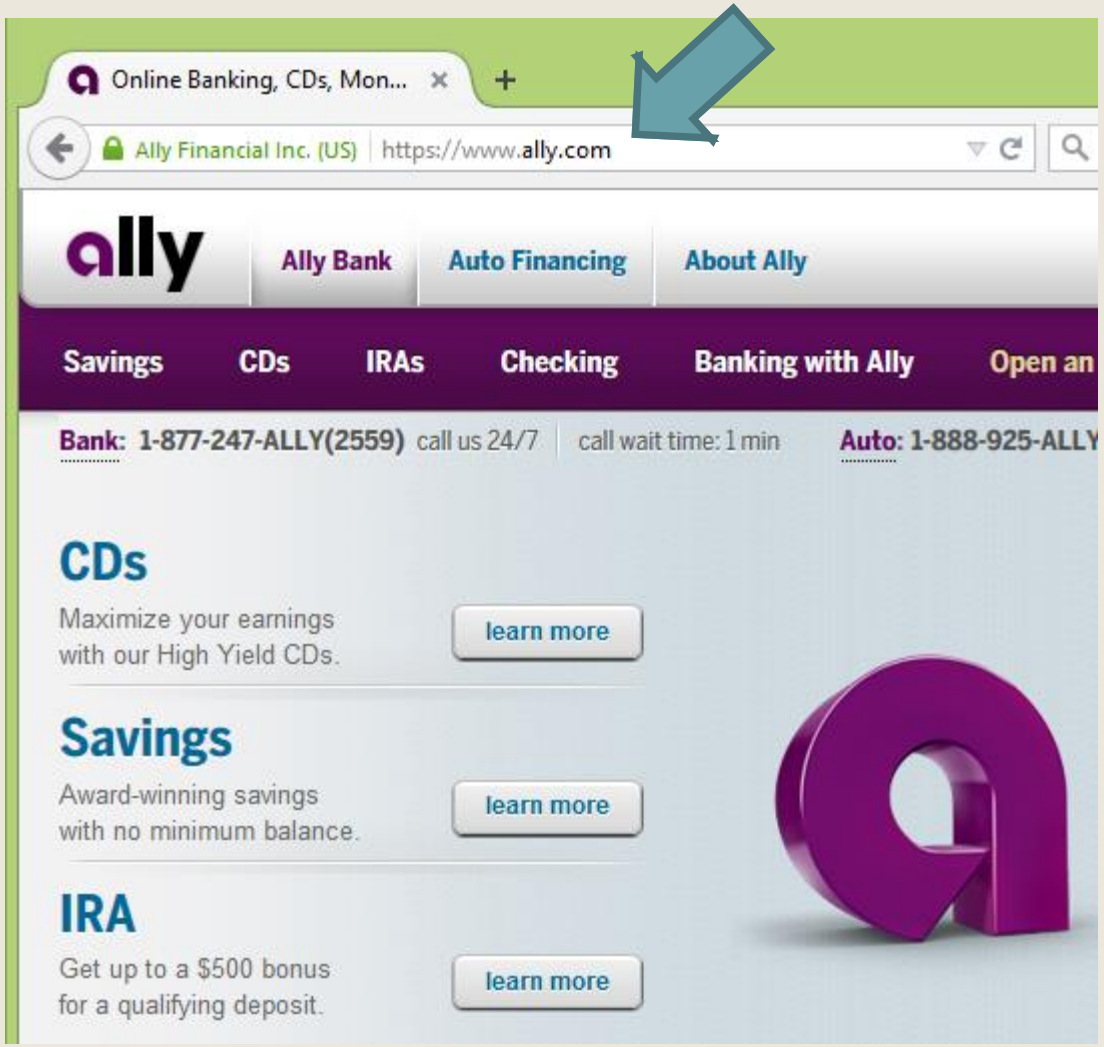
https://ally.com

versus

http://ally.com

http versus https





Encryption properties we want:

1. The communication between you and the other party is **confidential** and has **not been changed**
   - *No one can read what you sent*
   - *No one can change what you sent*
2. **Knowing who** you are communicating with
   - *You are talking to who you think you are talking to and not someone else*

Key management

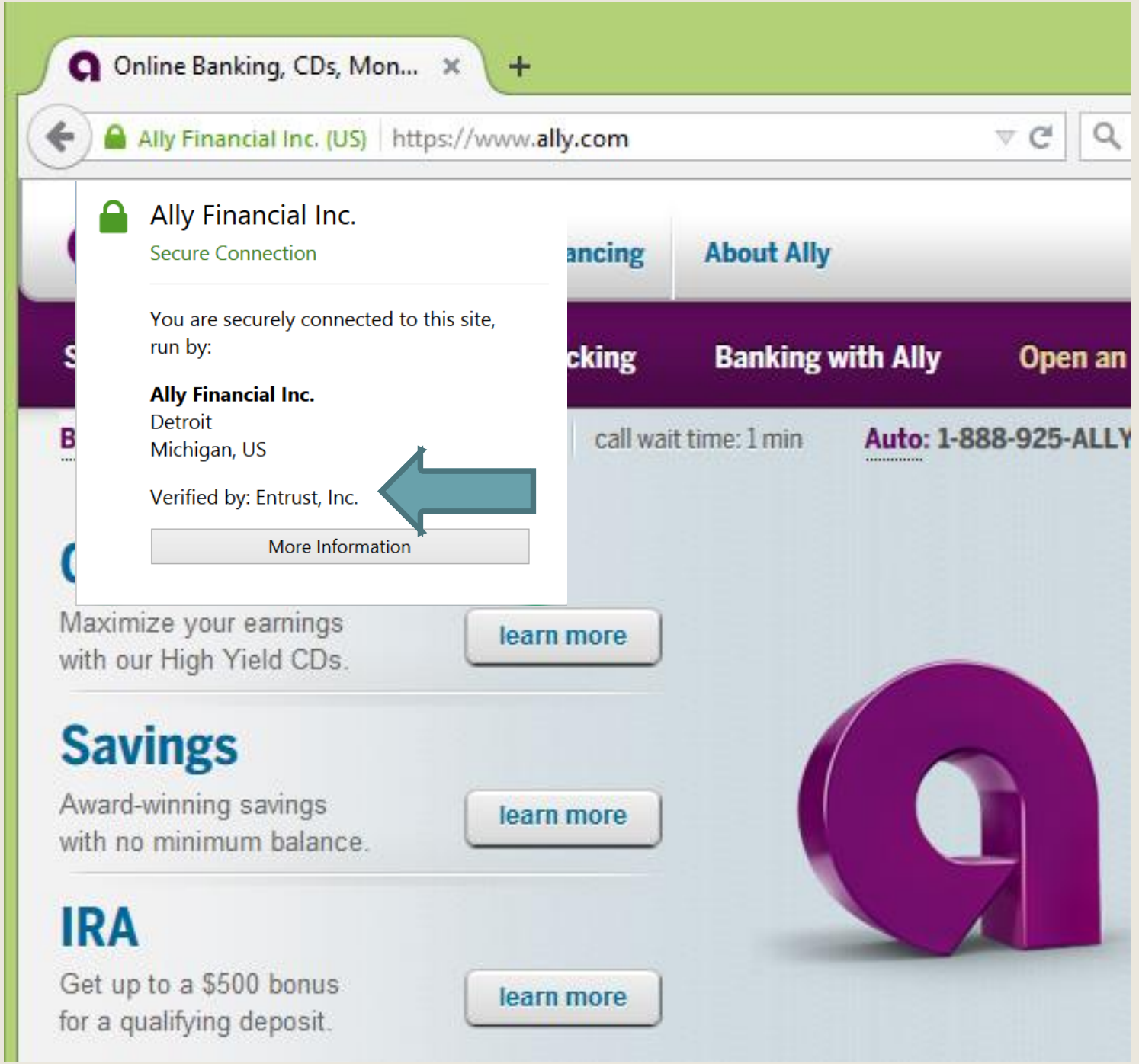
- Public/private key pairs
  - *Give public keys to other people*
  - *Keep private keys private*
  - *Verify other people's public keys*
- Keys are linked to identities
- A private key should NEVER be shared, so only one entity theoretically has access to it
- Possession of a private can be cryptographically proven when starting a communication IF you have the public key

My public key

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFHMcgABCAC9WrYDO6K2L3VHyi4eHN6suHLqMpJ+SO+IUTuLEVnUzIoXAUXH
KozHejfV/9XoG8j933ZtszXKCog3aMESe0E0z6fNGfolvaCe5B4jwqoJt8NHwb5L
B2dnq0CplgXcN2GJxfEHHUaf27C0SobCJxPMeshUh4ZHke+g6DatmiEtBpVp41Ot
1zgxdMQkgb2H2xw28RYfYkdDoueteIkOrFLrCy9ZF9KdMhA1eBH94KnwIQshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u2339hvH0
B/h+7xLM6FQb0UZQ9BD5w7IQHgYtXJVsUj0dABEBAAG0IkthbWkgVmFuaWVhIDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwEIACkFAlYKYvECGyMFCQImAYAHCwkI
BwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRCTdsxl9/HZffG+CACShuKxje3QAqew
GWh8K4gCdiY0xDqJwq3PHxmyhZmQeN/1a1KcOrljI2b+Q75/5t+EgXOHpR0PlxfG
lZ6zOEpf6A18iFXx3JgQZdwPD0jtBiWNpOyMeBGTglvEYG3so2VueQoeXcq3dbYp
5vstVxtD+TKHQ5CioIT75P2bzYq/XLT5aIbNQhQDPcTo0DgbRH+FvqsRXr7yeaef
JaPnxX0+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCDzQkJ7uQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZOaRxEa9Vf48jiWvrxuJ8YfHWS0hEScNOcYC2P8q20IJwwE26T
lpdtrwCqtB1LYW1pIFZhbmlIYSA8a2FtaUB2YW5pZWEuY29tPokBQgQTAQIALAIb
IwUJCWYBgAcLCQgHAwIBBhUIAgkKCwQWAgMBAh4BAheABQJWCmMeAhkBAAoJEJN2
zGX38dI9JJAIAIW0rxrIYsrmKS6CbW8MgTxxTD0XaCt1b7F0W0QZHskIUQhEcE+a
XBYib1A5uHaatLfyjeXaD3qMEoZnQHoYMGE0GKu00wWsbhfoQzHPgwzRLkD1i75M
BIbaww0KWoVB9e4AkMakXJCnF5BXeo6AHRL2v15V205DikVnICRXocKtu8b7LnkM
cLn7oLobr1de1uyKoNzbSnO/vpKDJp0/EY5yUeV9olypZy/6wFQBehg1sXye6znO
9wb9uUsu9+/P8pz4JILMDSevjfT7zSRSl/YP3f0fZ6N4bc+KOdwPM7u5lyoeu9zh
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhwEEwECAAYFAlTnSpEACgkQjyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4I7PpD1weJDf3a81Vhm7JyXE/Xy66ypfdt3w
XmFRUuIrwezY1NebWNCRQHzQvRv/VJwjbTUx+Q3HsjIkKlHbE7iCiQXXtTRk0Eny
2nudcjGI2v03C3B2JCucEw6esF1x79Pl/IPv2+6tgUBKmDfOpsB2vbtqrHnmAYKL
4IQBFH1YSJgnzwo2Jkh0hcHdF90Zem1eMeiDEeVkH63893N8Swk5fBKdTj+SKZ/L
rQElBBIpMR9BmeY6bPvWRuycVK0nIMR80G9iFABxjTpWBL8aGk6EeVK5EqYDGvkd
ZIarK84r+KU1KD5IfgOCN7nhwgy7VImE68caZHSRiPWZP1fVVMhydiRJv8WsoUs6
INfVU3nxH+ZYthPbY0T86leGSchBT5K/fBQvbjhrRTbTFwvjzSifb9efWyIDi994
nzP6cNorir3GIpsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLFwKBDsaHps2+1meFP0oJFvNetzp2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYZTSS05x1RdXHqpEbgap8dtuHhVvJw9QYDQBJr0K4aKyG9qqMD8cta
Pl/FAdyAqwH8Nw9efqAK+RQxSVUaue9BYEnbIRpsDK6MkP3YMFmu5ki5AQ0EUcxy
AAEIALyXYy8G2ZaTDJpdGcRhmIqO0SUlzPV7/5E5BbYKBNu4KU3nX+JLVcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TTXSIUKAt3T1oGBtXmGvqbGBq8ljSGl1UTwdF
5yu50JyRSf2fqRND6P/2eHNXejDUtdvhUXlUt8h9MuUO/ipD0DnwIvMnAATJHA+R
Zqw6oNpyjRGzvr3iuWUwe4PtyJDI3ELAFkbp/NAc5TIuVHRHNOWNplcIJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgJPOdbCZf
2Tozd7h9MXtGJDlPKJ8eLG8ogcMAEQEAAYkBJQQYAQIADwUCUcxyAAIbDAUJCWYB
gAAKCRCTdsxl9/HZfS+hB/9BJqSmIgcoHFXnb1PVIKxekzL8+WVm5Pk/EgMQSLZ2
HX4p3iaI5PEPcYgUw9YnaG4i00dwJGw5/daTWRrTzcnKd8YqoP+DU0t96HZDSu3m
mCzE9NVAQYboFbVmGOx0eo627UBSvFqaXvAxBDYkoR8B0TnKhrQFwXkZVb30hKwD
TgAFjOGlZiE6uAdST231tFaq0bizYfe5AVXRqro20xBqNbaJNqs3SW0D831Syvdv
lIOBx83/R0gg7hUkI6F2vzXicWmUwFSXRrggCSbLosHsP6isBWwvlHeRmna/aQab
YKG3gbV9iyczAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
=x5FK
-----END PGP PUBLIC KEY BLOCK-----

Idea: Certificate Authorities can do the verification instead of users



ars technica

MAIN MENU | MY STORIES: 2 | FORUMS | SUBSCRIBE | JOBS | ARS CONSORTIUM

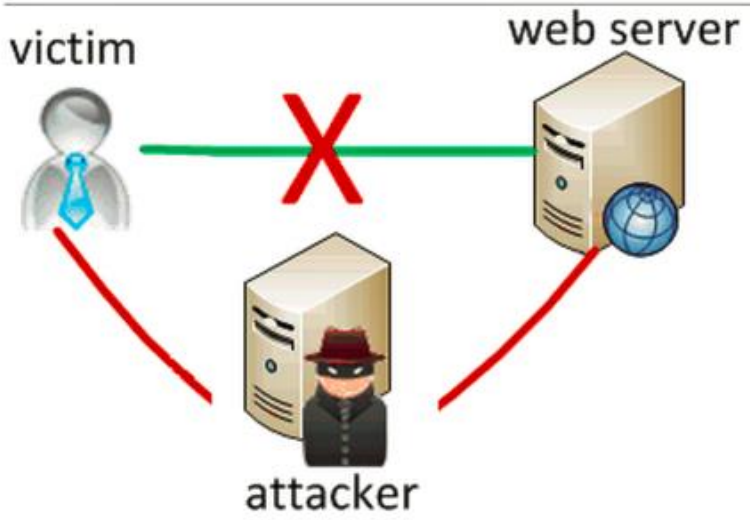
RISK ASSESSMENT / SECURITY & HACKTIVISM

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

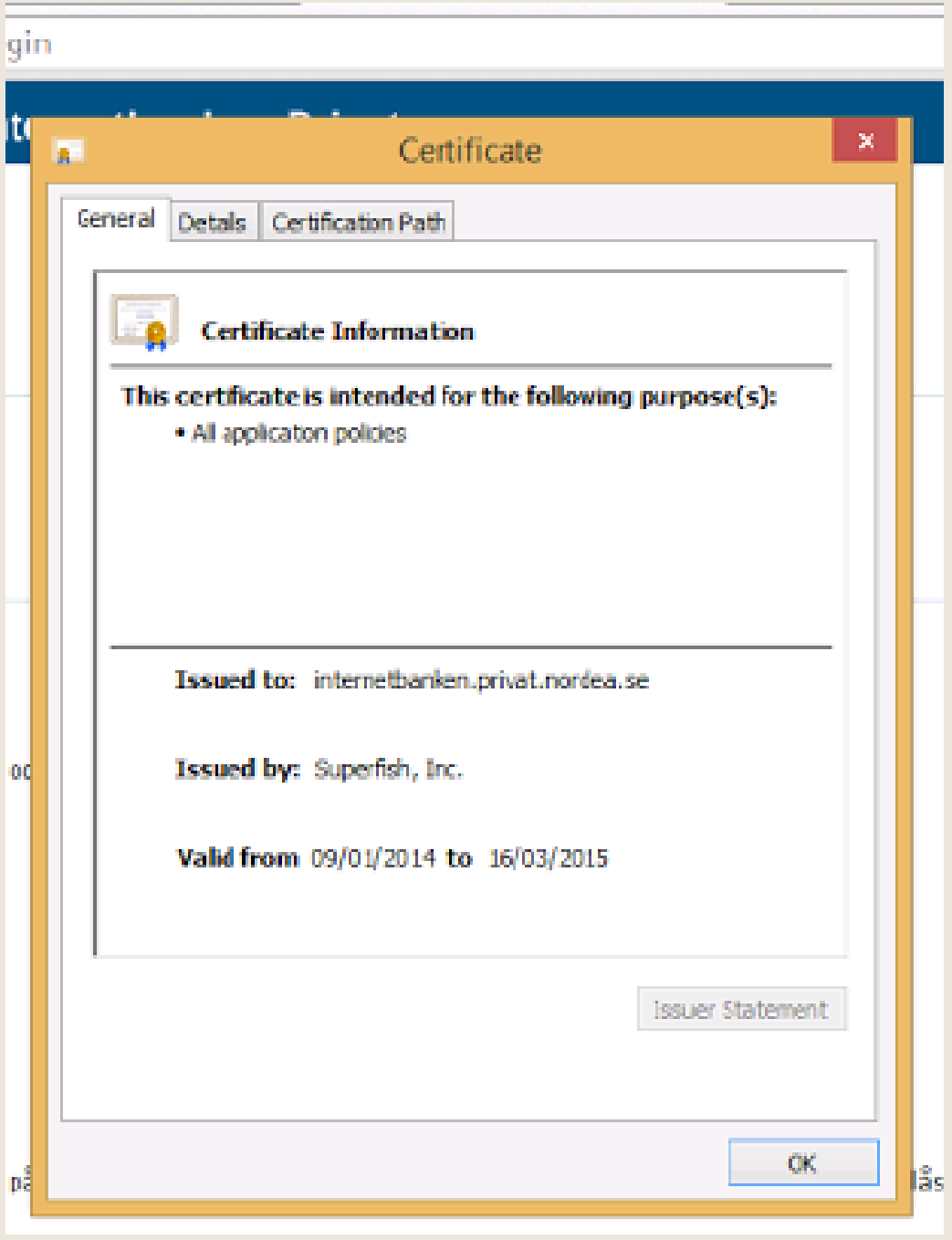
Superfish may make it trivial for attackers to spoof any HTTPS website.

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

Share Tweet 333



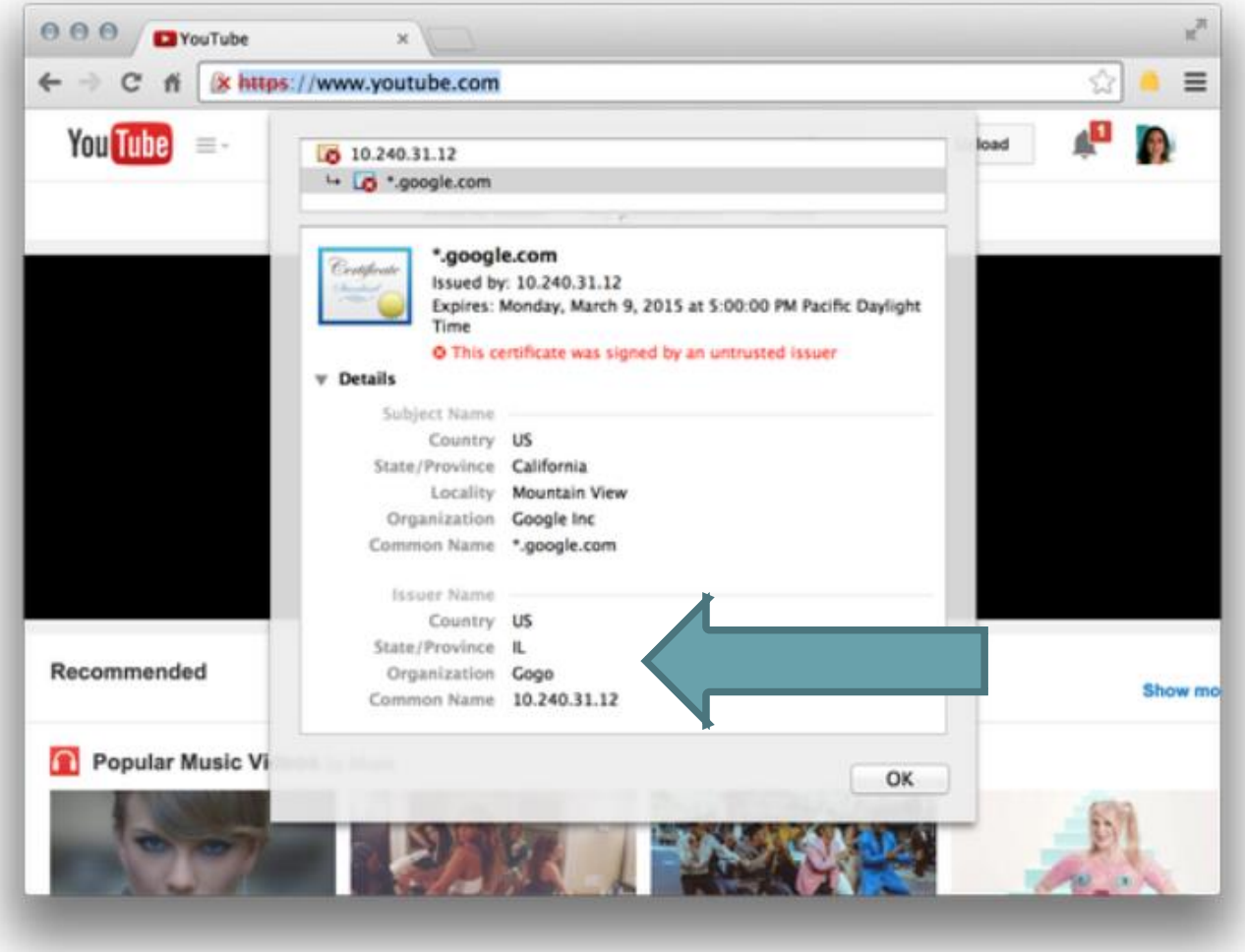
Web Programming Step by Step, 2nd Edition



Adrienne Porter Felt
@__apf__

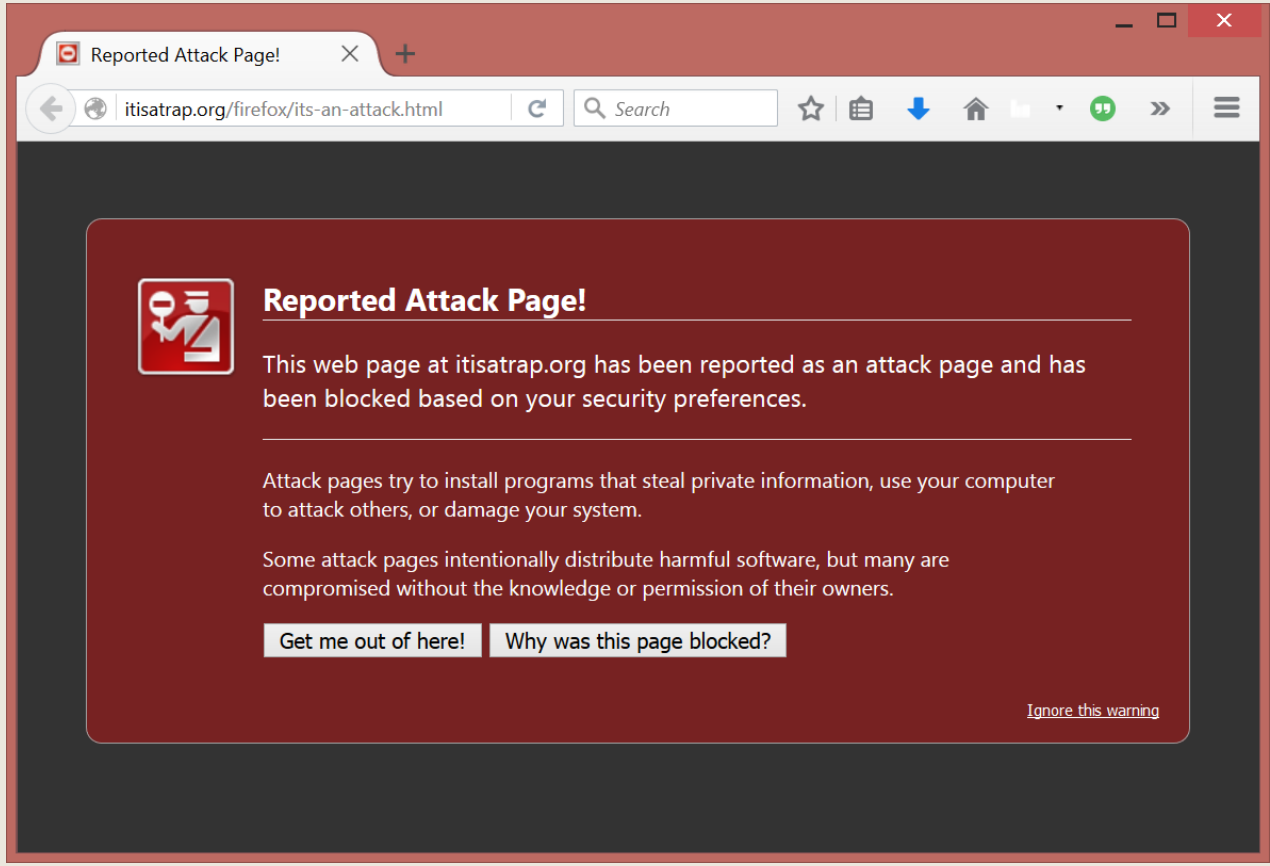
Following

hey @Gogo, why are you issuing *.google.com certificates on your planes?



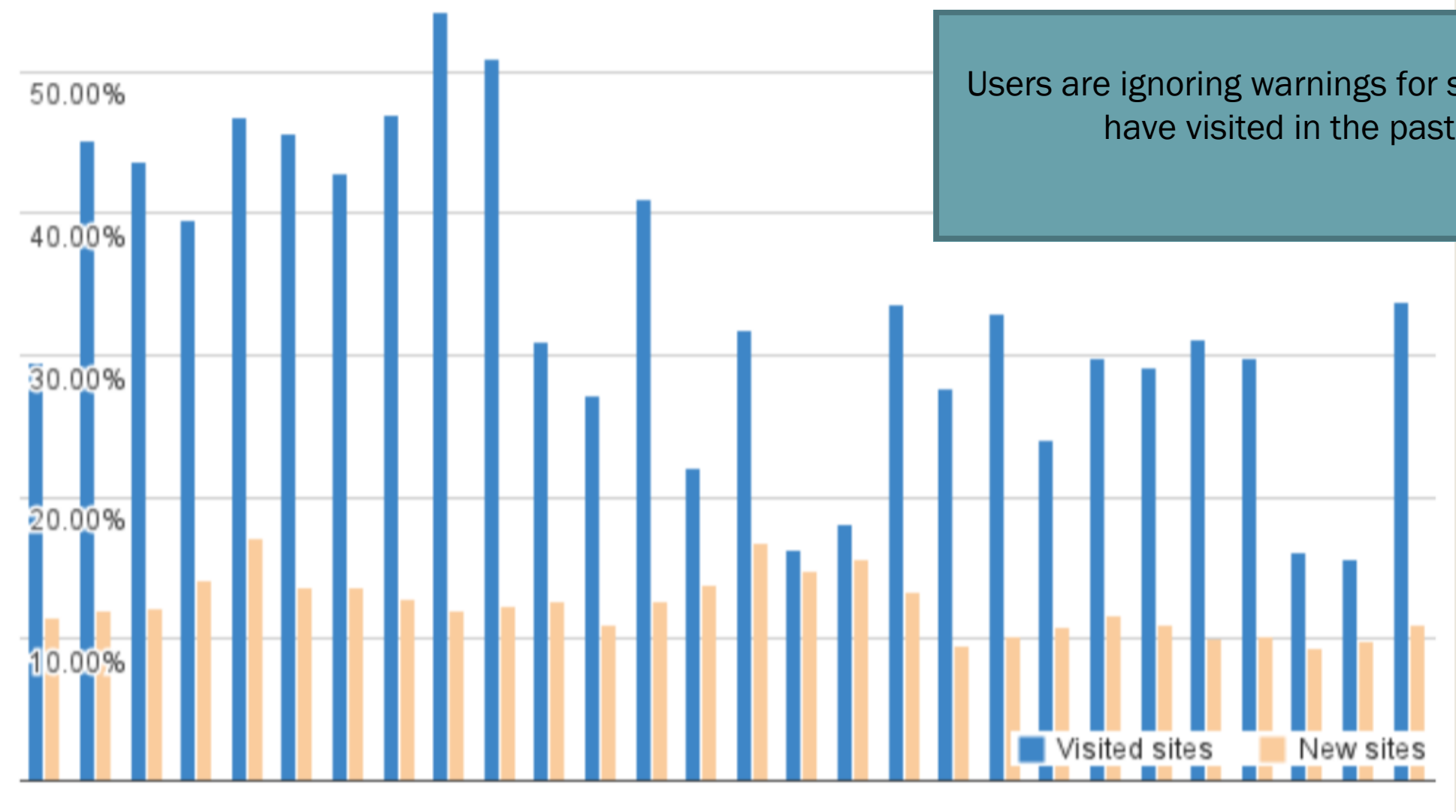
Real world click-through rates

- 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%*



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

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



Users are ignoring warnings for sites they have visited 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.

Why do people click through the warnings?

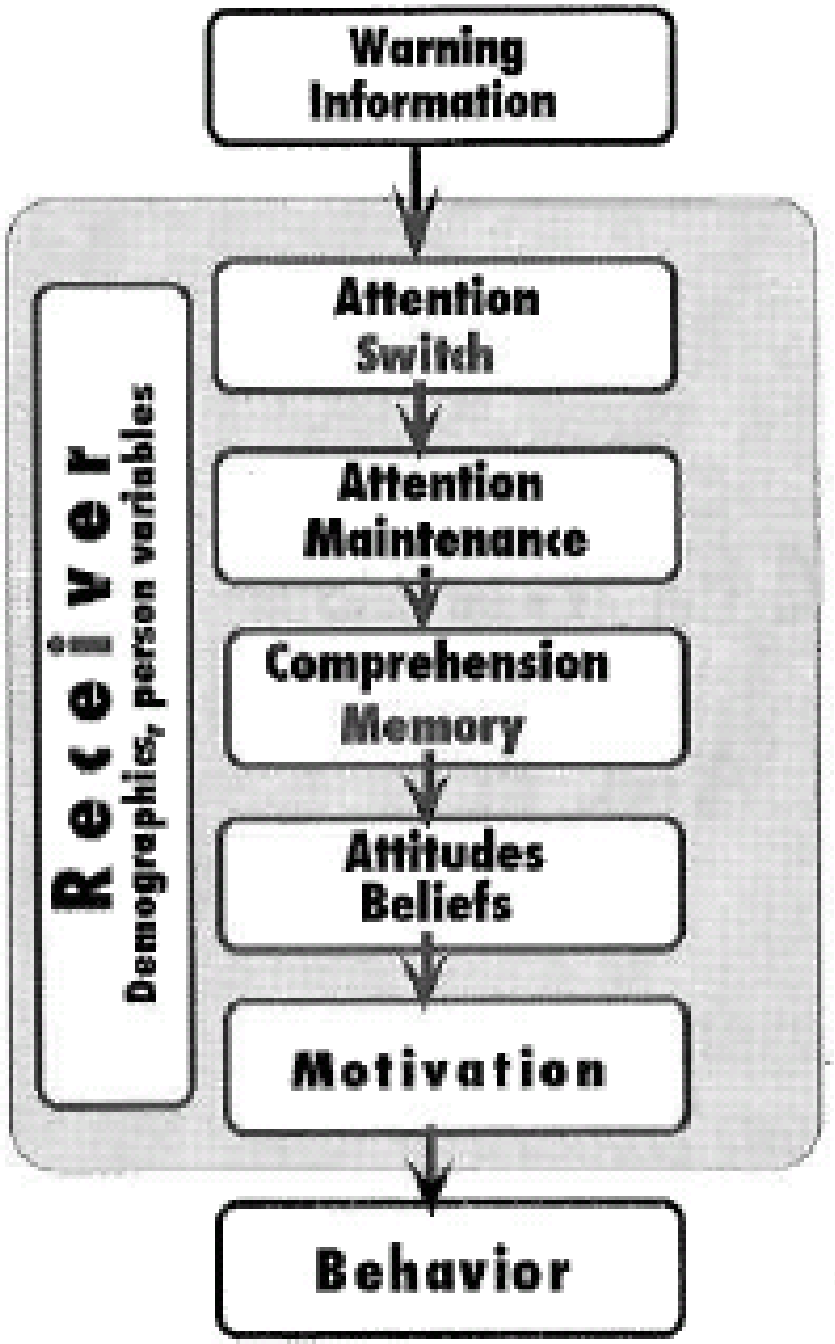
- The site is used often and trusted
  - *“YouTube is a well known website. I’d assume that the malware block is in error.”*
- The person who posted the link is trusted
  - *“I find it harder to believe [the warning] when my facebook friend just posted it and had no problems.”*
- The site where the link 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”*

Why people don’t use privacy protections

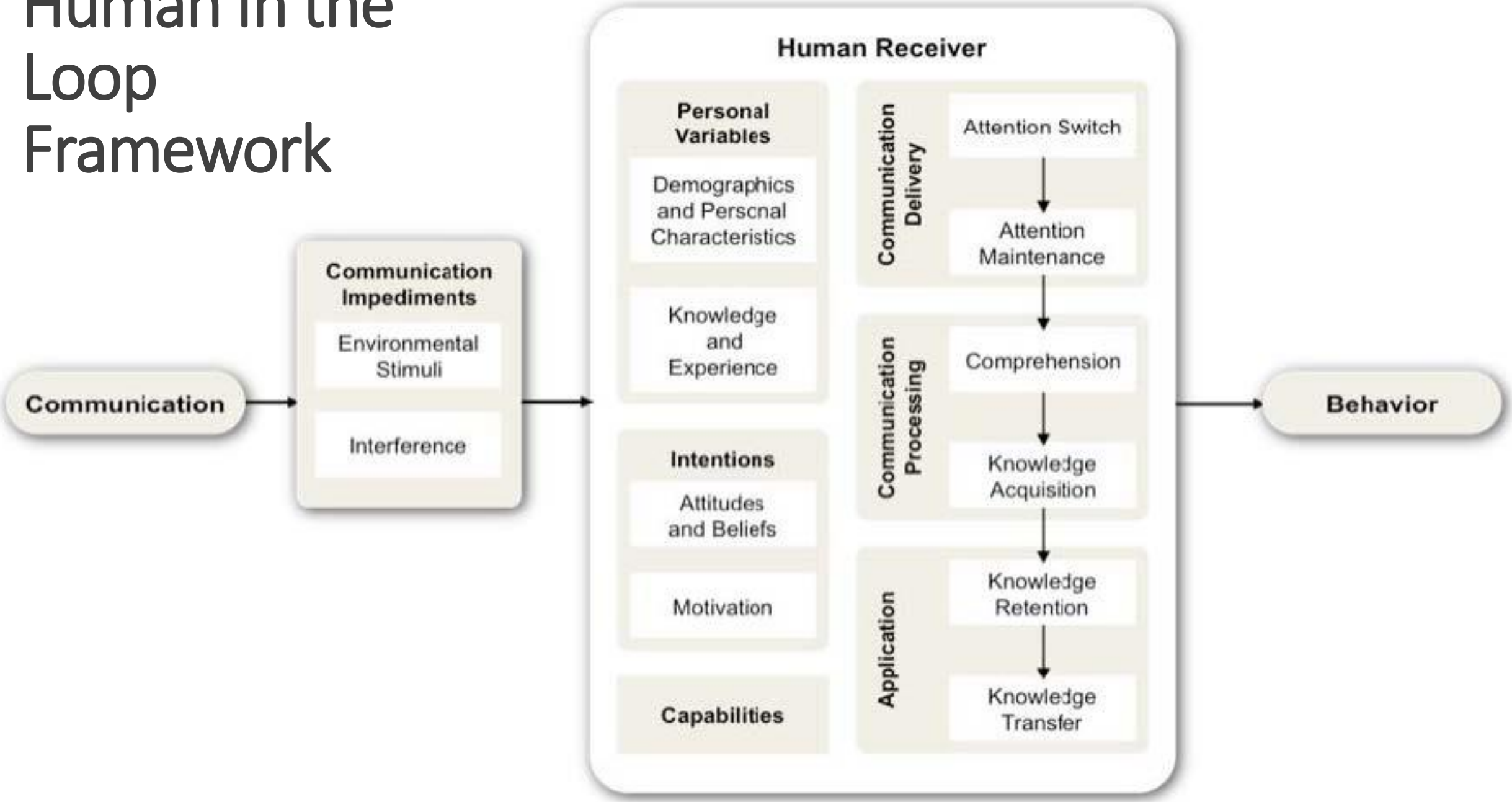
1. People don’t really care about privacy
2. People are not aware of the privacy issues
3. People are not aware of how to protect themselves
4. People are aware, but are unable to use the privacy protections

Communication-Human Information Processing Model (C-HIP)

- Developed to model why people do or don't understand road signs
- We adapted it to computer security

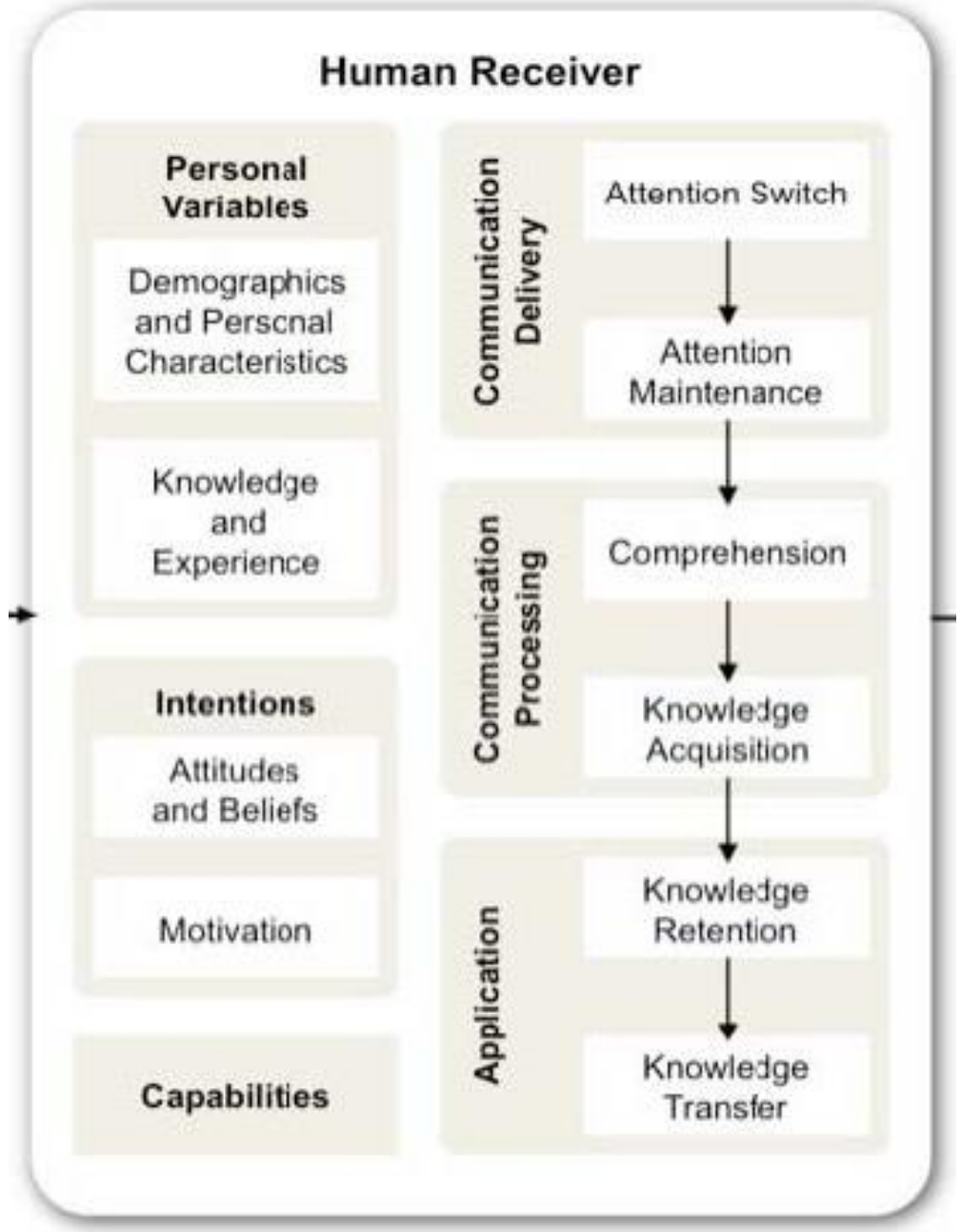


Human In the Loop Framework

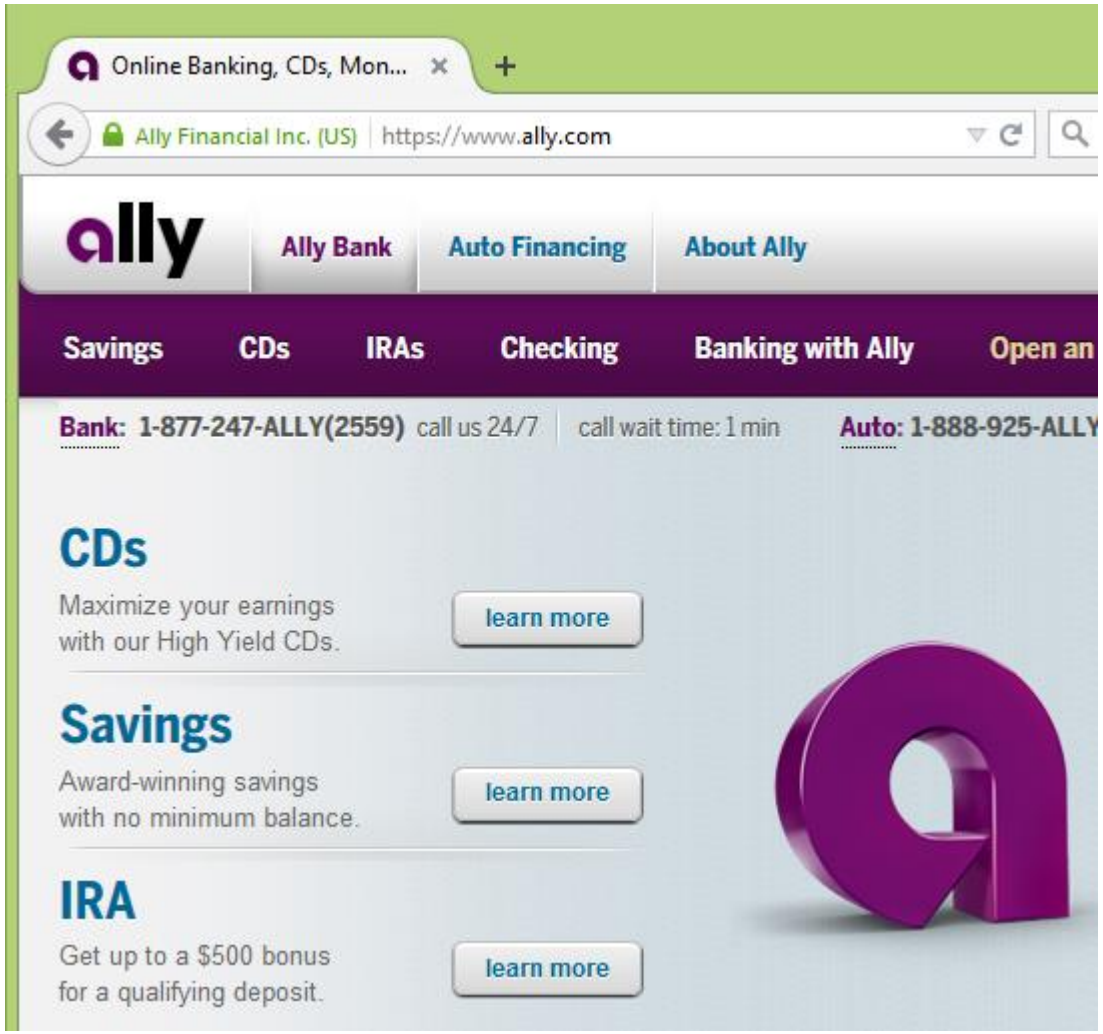


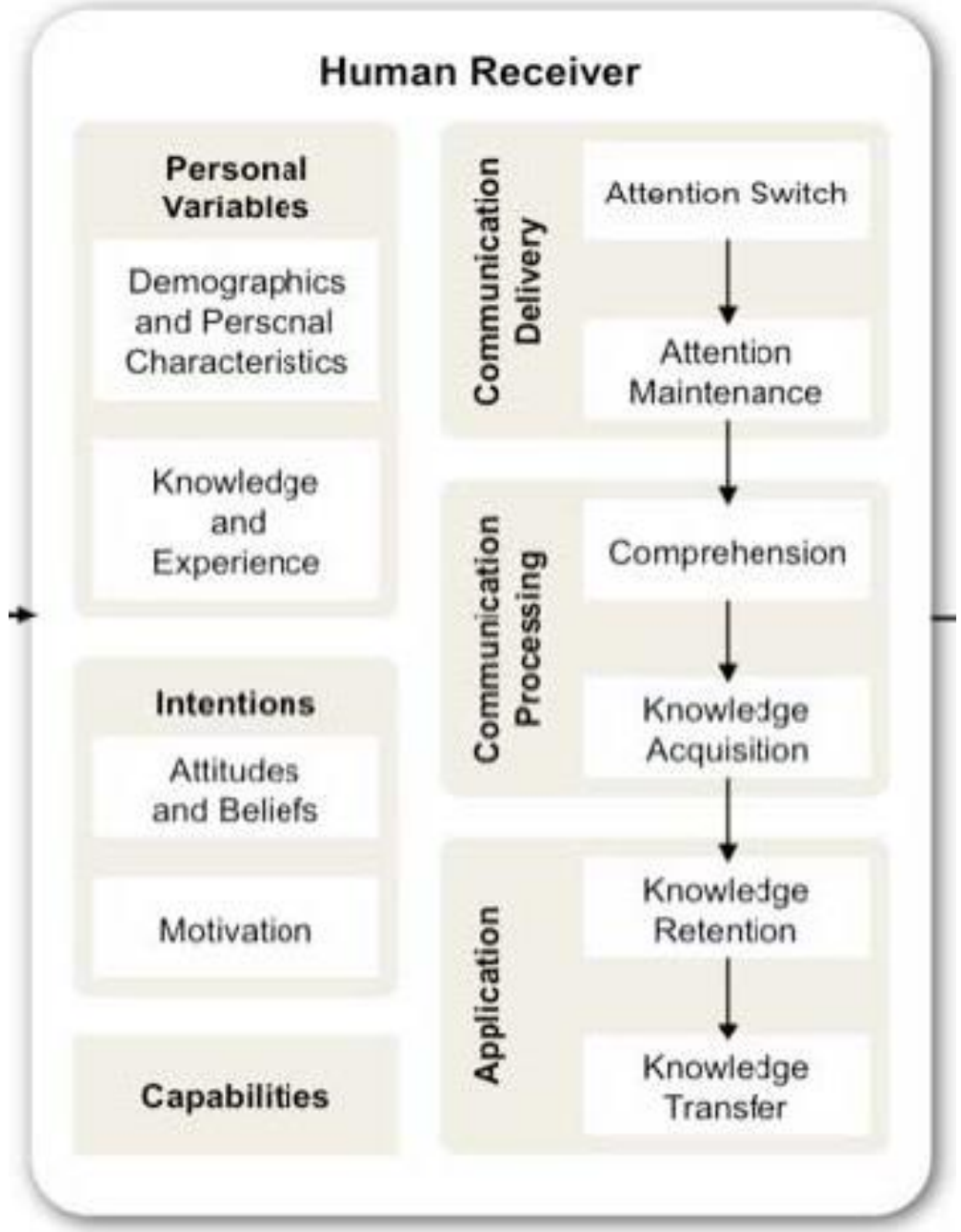
We are now going to use the framework to figure out why people are ignoring SSL warnings…

What level of the framework does this fail at?

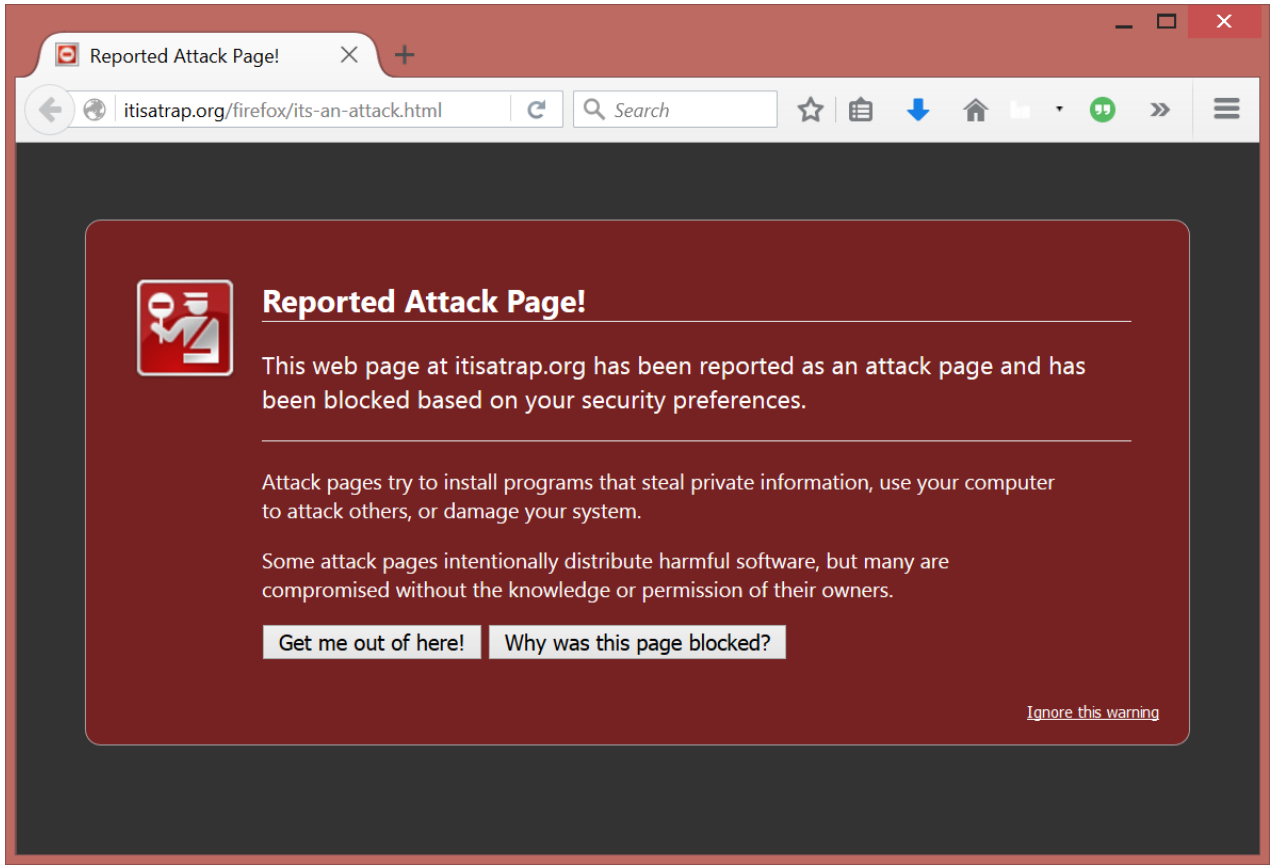


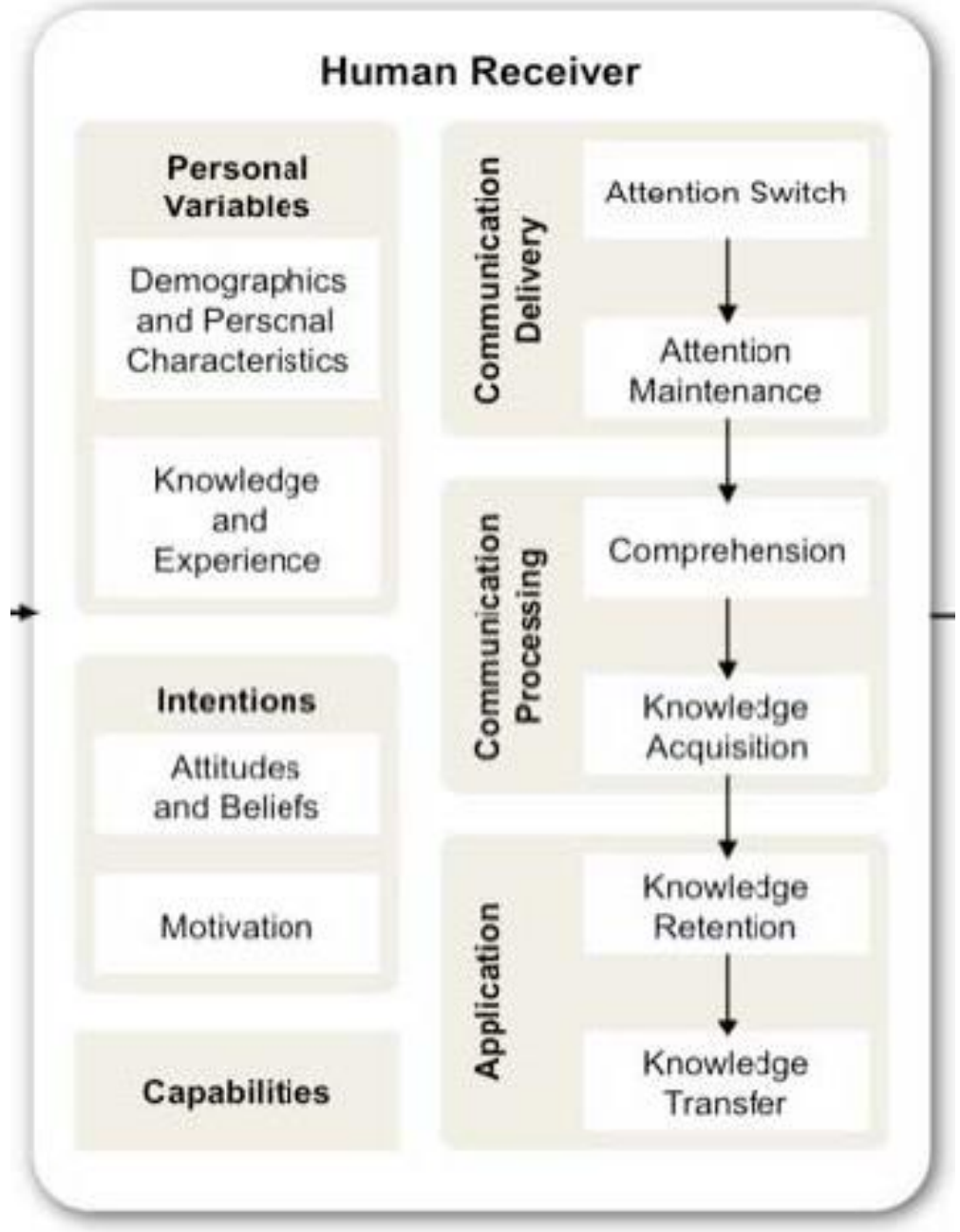
And this one?


Online Banking, CDs, Mon...
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

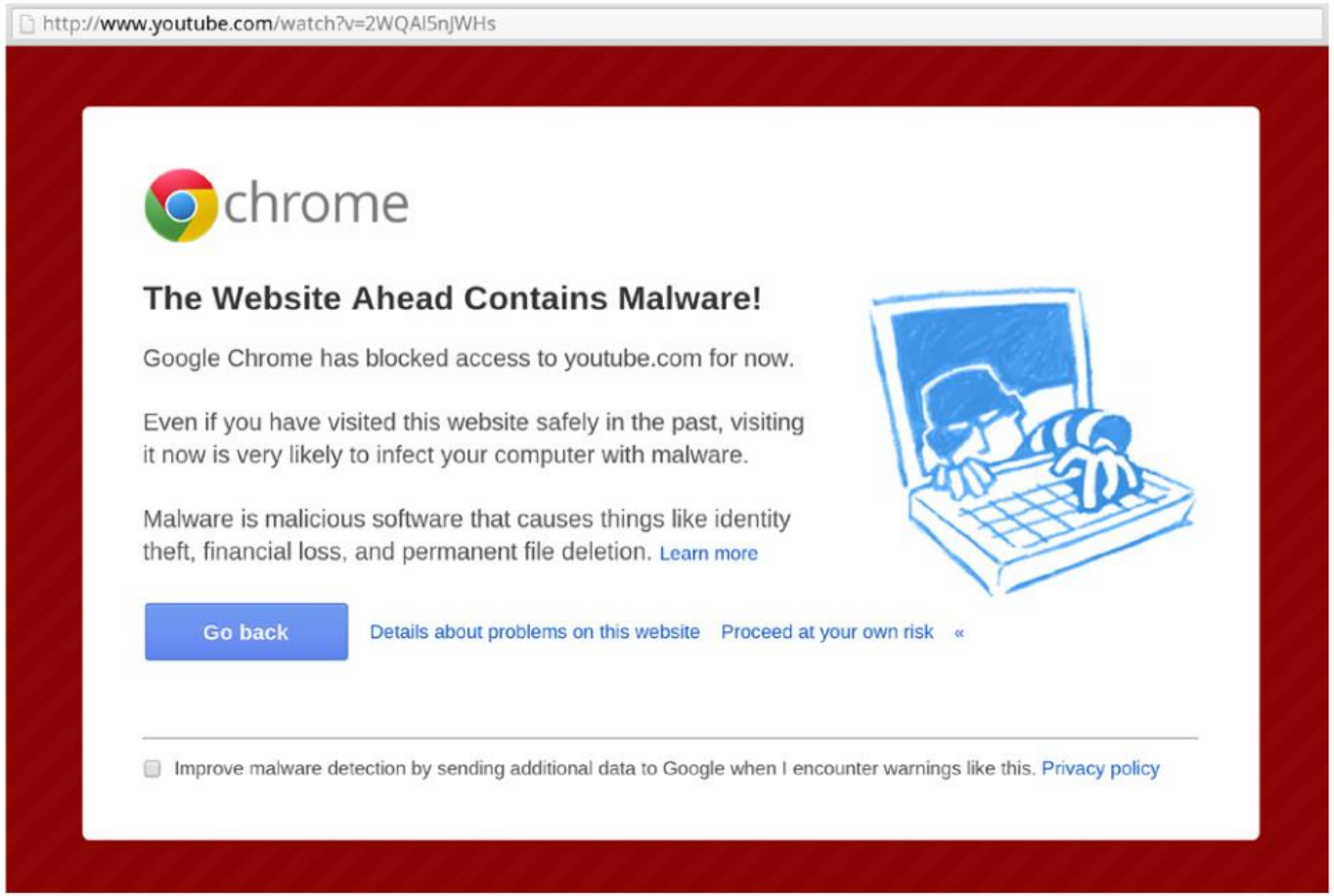

Human Receiver
Personal Variables
Demographics and Perscnal Characteristics
Knowledge and Experience
Intentions
Attitudes and Beliefs
Motivation
Capabilities
Communication Delivery
Attention Switch
Attention Maintenance
Communication Processing
Comprehension
Knowledge Acquisition
Application
Knowledge Retention
Knowledge Transfer

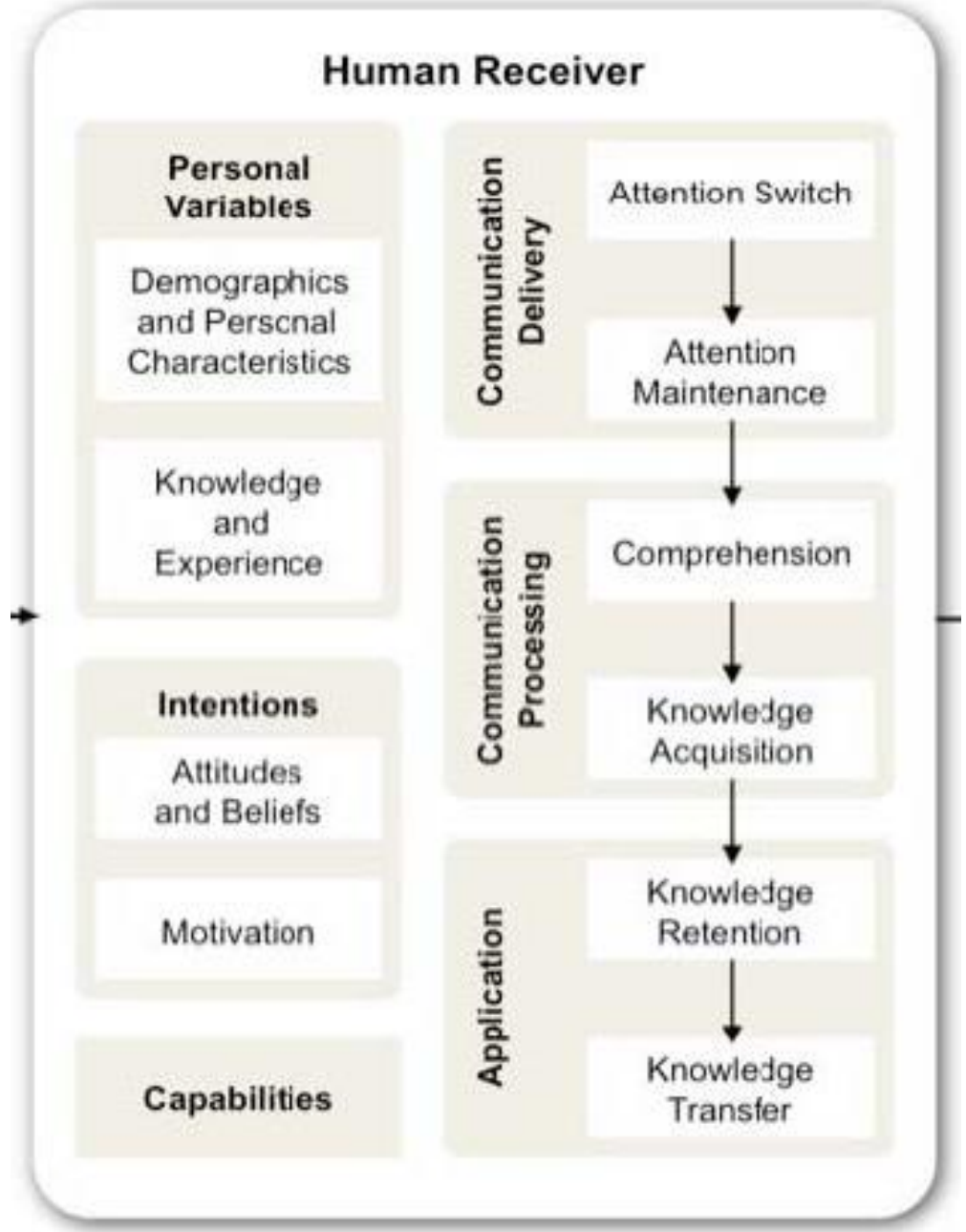
And this one?


Reported Attack Page!
itisatrap.org/firefox/its-an-attack.html
Search
Reported Attack Page!
This web page at itisatrap.org has been reported as an attack page and has been blocked based on your security preferences.
Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.
Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.
Get me out of here!
Why was this page blocked?
Ignore this warning


Human Receiver
Personal Variables
Demographics and Perscnal Characteristics
Knowledge and Experience
Intentions
Attitudes and Beliefs
Motivation
Capabilities
Communication Delivery
Attention Switch
Attention Maintenance
Communication Processing
Comprehension
Knowledge Acquisition
Application
Knowledge Retention
Knowledge Transfer

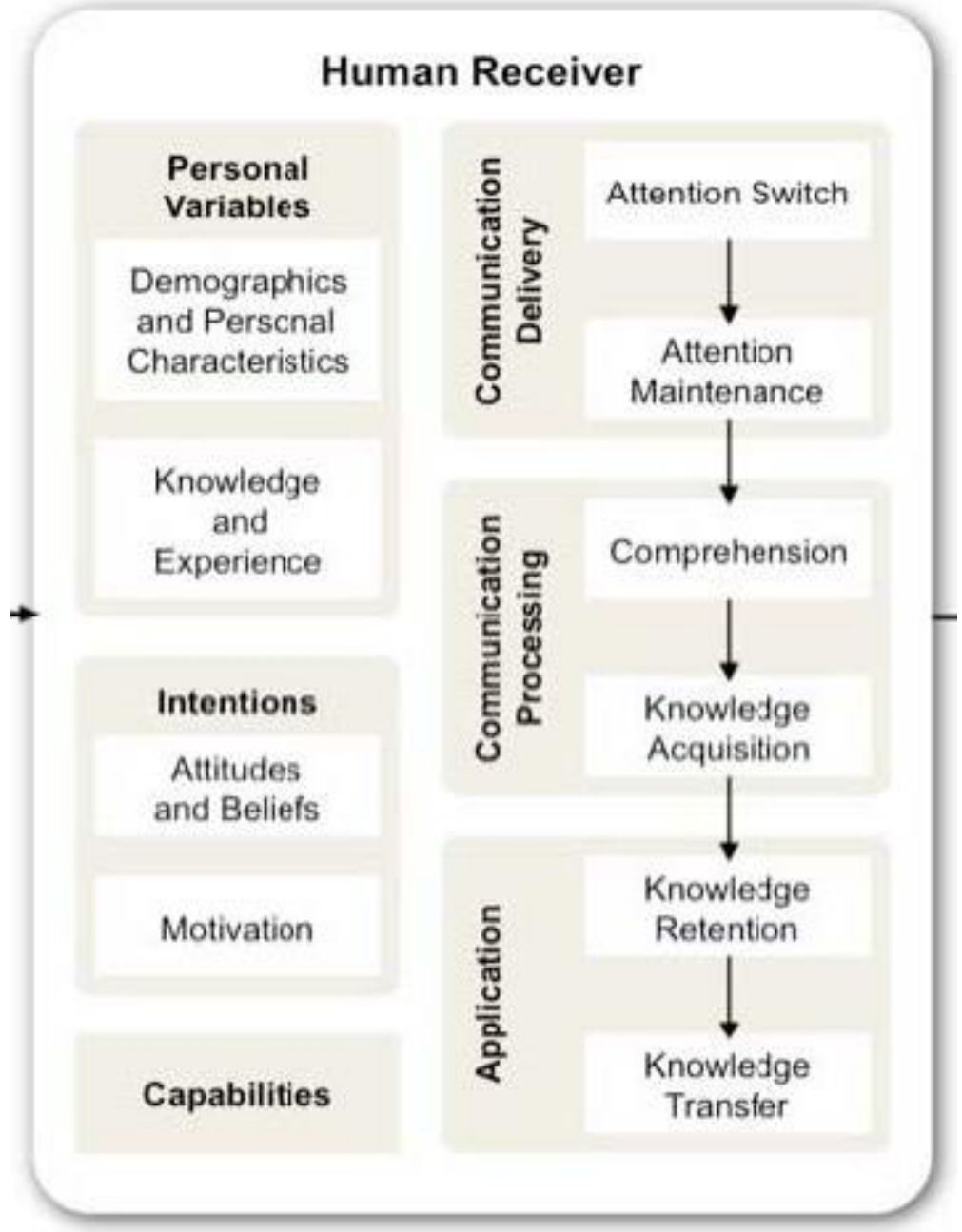
Any better?


http://www.youtube.com/watch?v=2WQAI5nJWHs
chrome
The Website Ahead Contains Malware!
Google Chrome has blocked access to youtube.com for now.
Even if you have visited this website safely in the past, visiting it now is very likely to infect your computer with malware.
Malware is malicious software that causes things like identity theft, financial loss, and permanent file deletion. Learn more
Go back
Details about problems on this website
Proceed at your own risk «
Improve malware detection by sending additional data to Google when I encounter warnings like this. Privacy policy


Human Receiver
Personal Variables
Demographics and Perscnal Characteristics
Knowledge and Experience
Intentions
Attitudes and Beliefs
Motivation
Capabilities
Communication Delivery
Attention Switch
Attention Maintenance
Communication Processing
Comprehension
Knowledge Acquisition
Application
Knowledge Retention
Knowledge Transfer

And this one?

- 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”



Users

Users are not the enemy

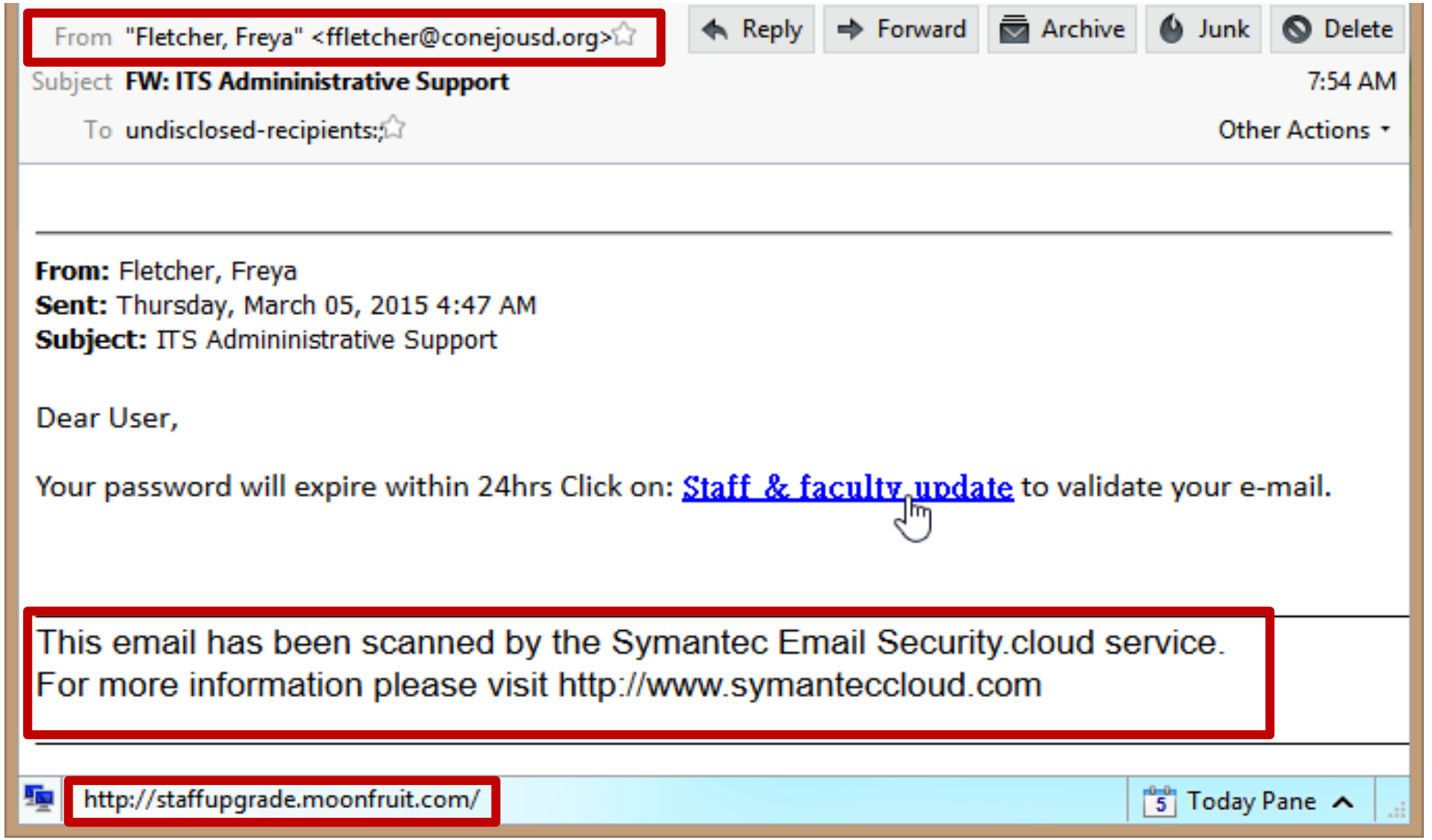
- Malicious actors are the enemy
- Users are a partner in keeping the system secure
- Like any partner:
  - They have skills you don’t have
  - They are missing skills you do have
- Think about what skills they have that you need
- Use the skills you have to make good decisions on users’ behalf

Phishing attacks and training

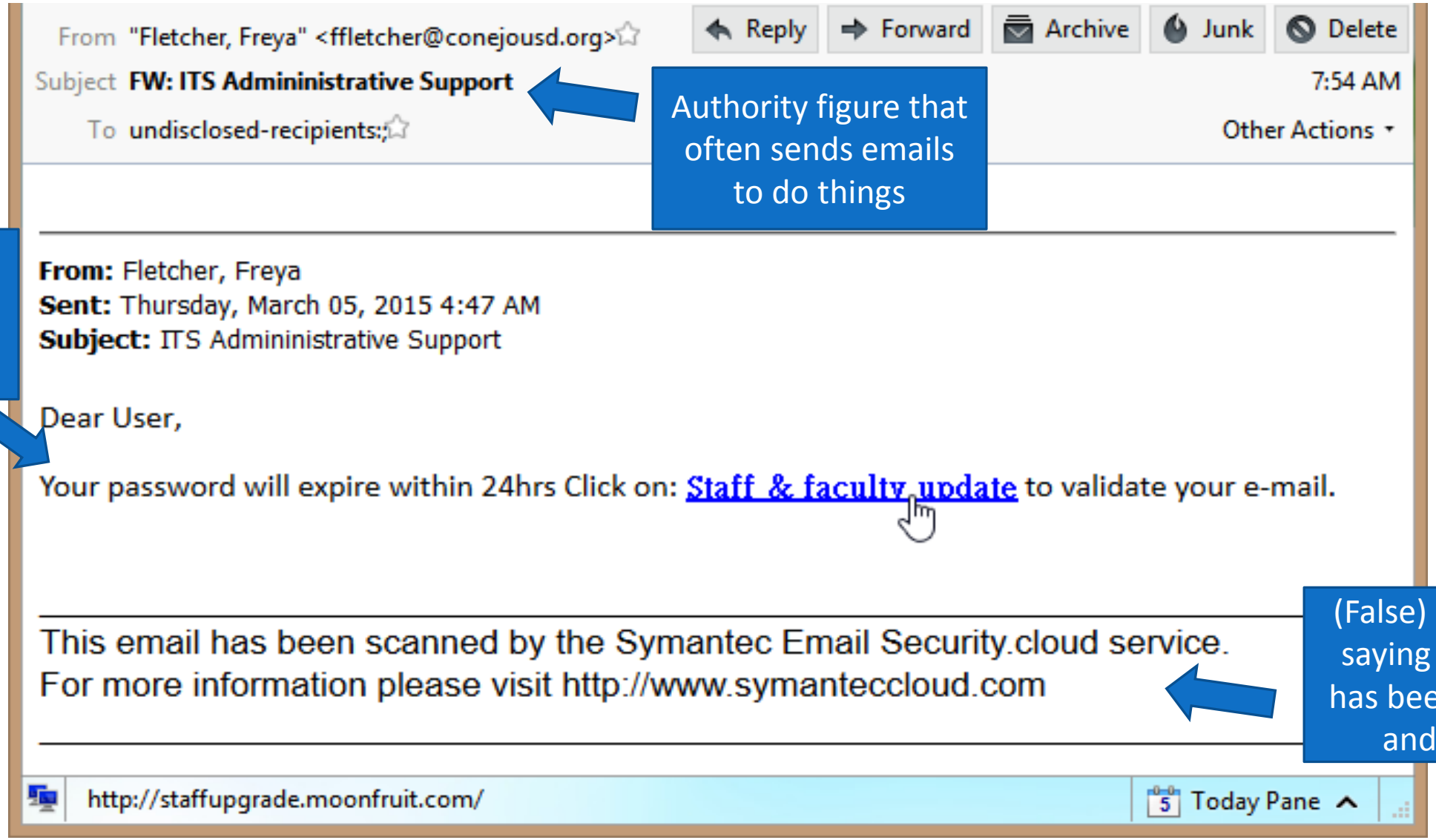
Phishing

- Phishing – Attempting to trick someone into taking the “bait” and interacting in a why 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

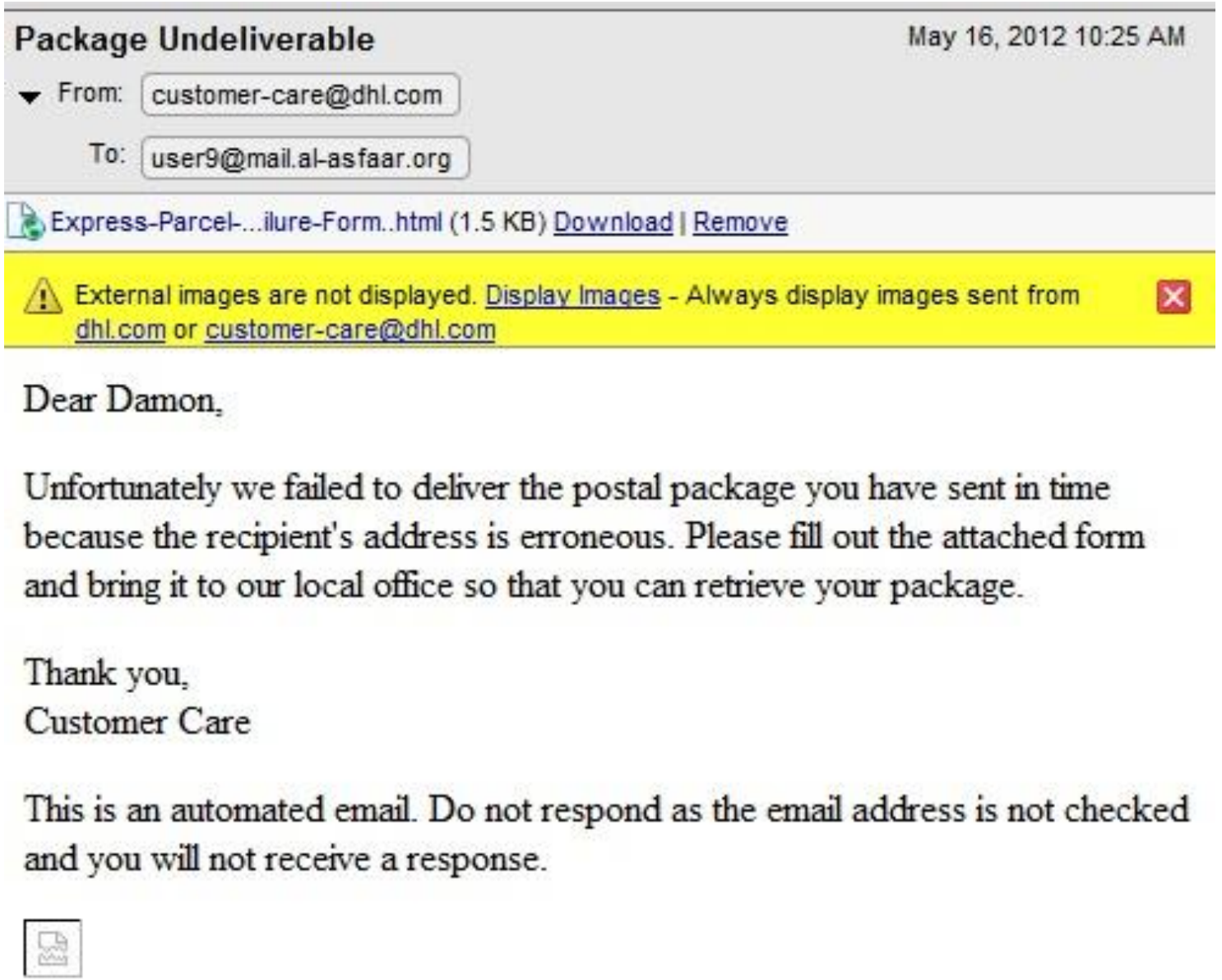
What on this email can be trusted?



(Wrong) Trust indicators



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



Package Undeliverable May 16, 2012 10:25 AM

From: customer-care@dhl.com

To: user9@mail.al-asfaar.org

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

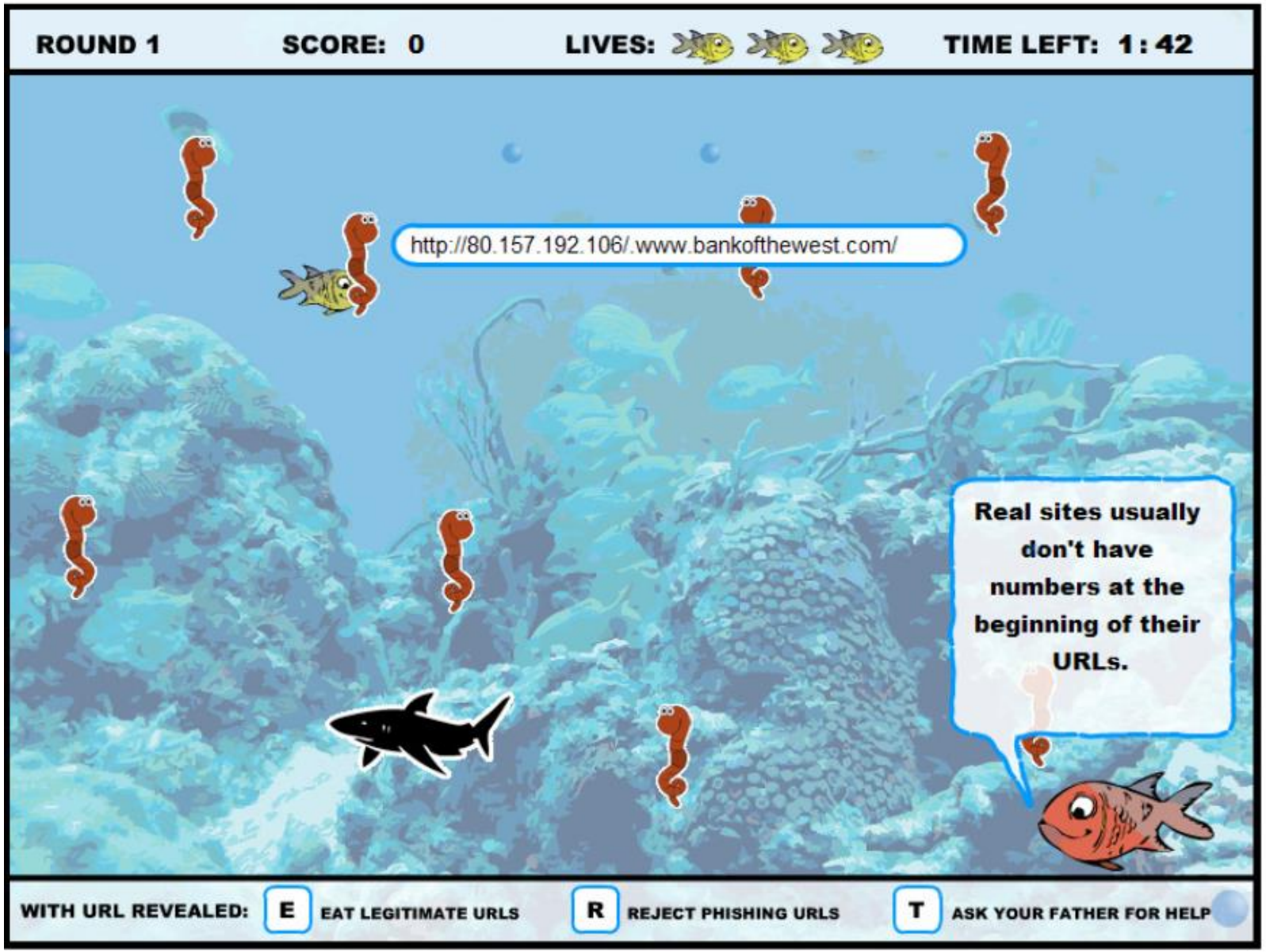
This is an automated email. Do not respond as the email address is not checked and you will not receive a response.

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

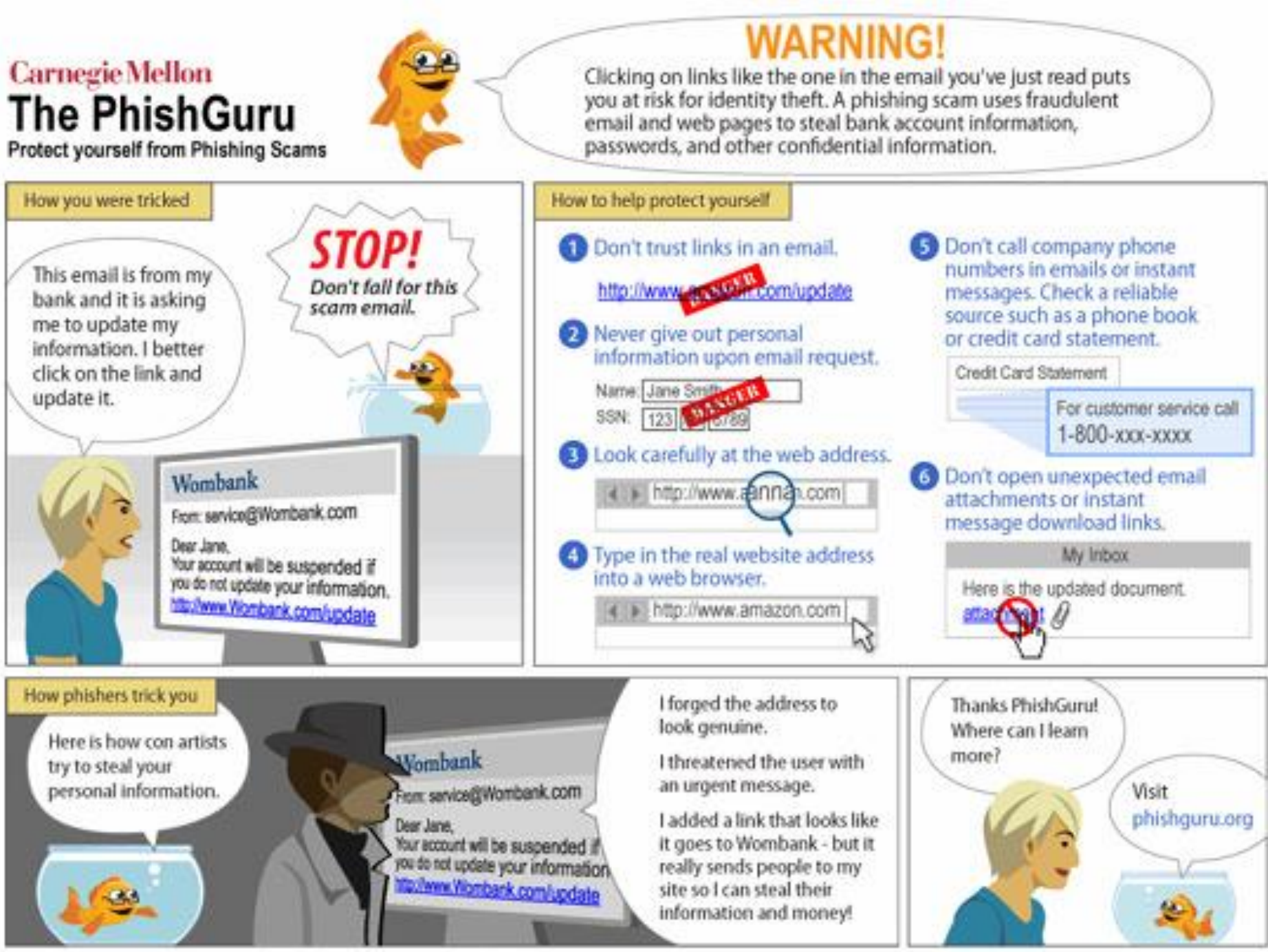
Anti-Phishing Phill

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



PhishGuru

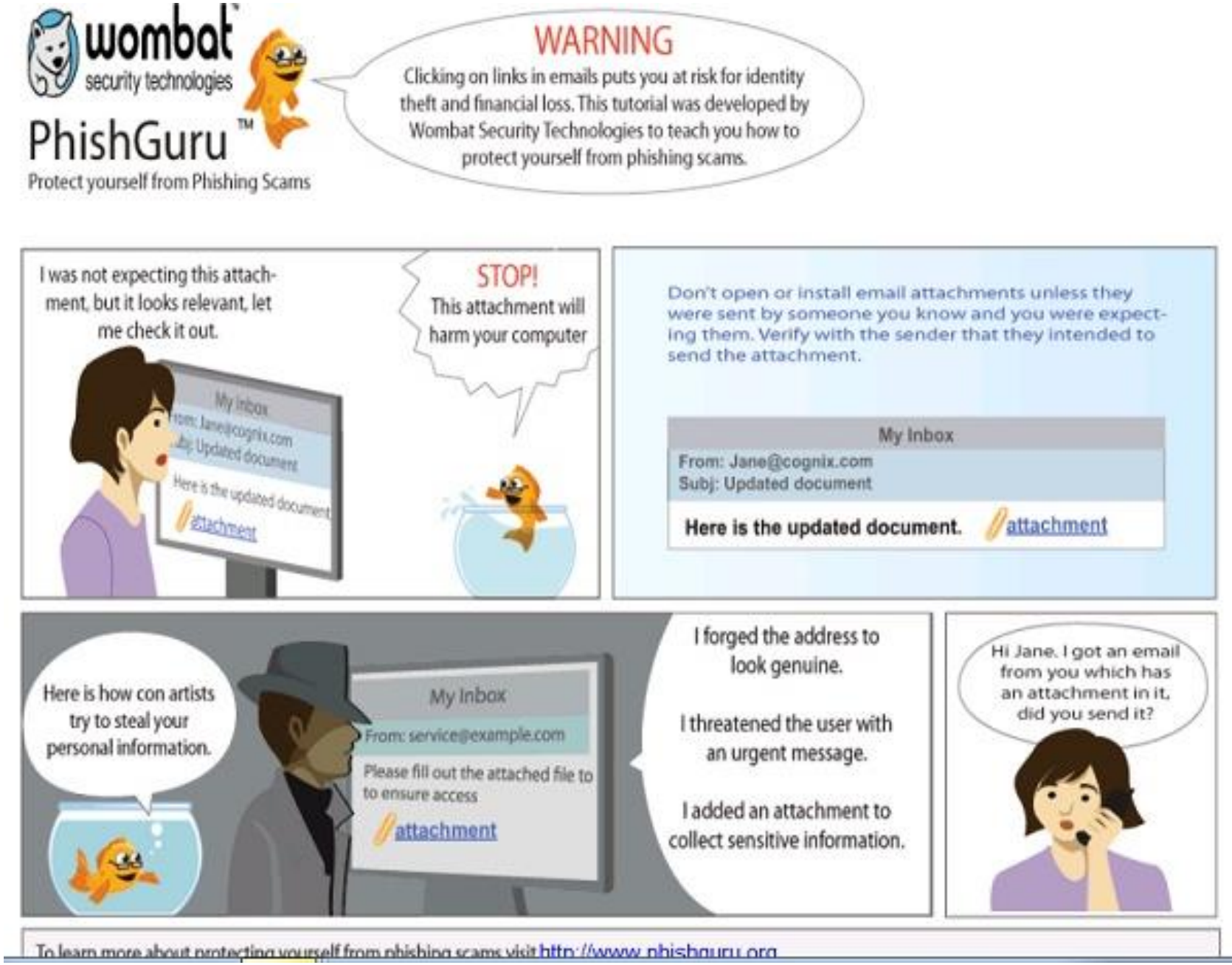
- Comic to train people to spot phishing attacks
- Best time to train is after a users has already fallen for an attack
- Send out fake attacks and train those who click on them



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



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

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.

Questions