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

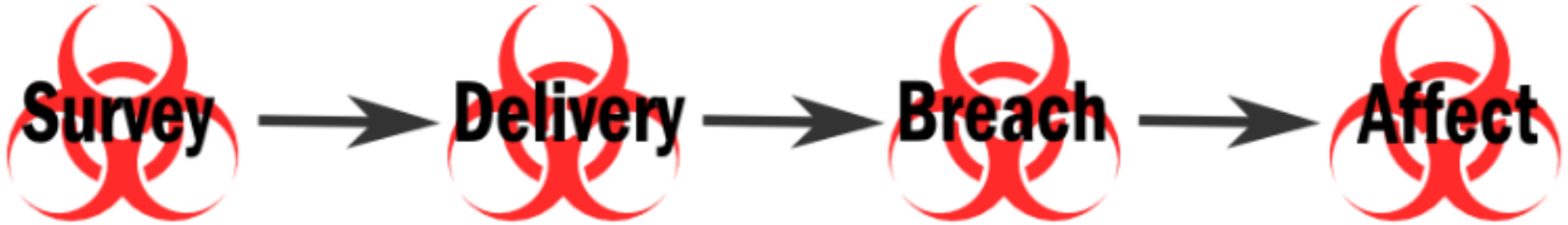
`http://doodle.com/poll/t7ia4mbv9vk8ekec`

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

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

First, the news …

- https://www.cesg.gov.uk/content/files/protected_files/guidance_files/common_cyber_attacks_2016.pdf

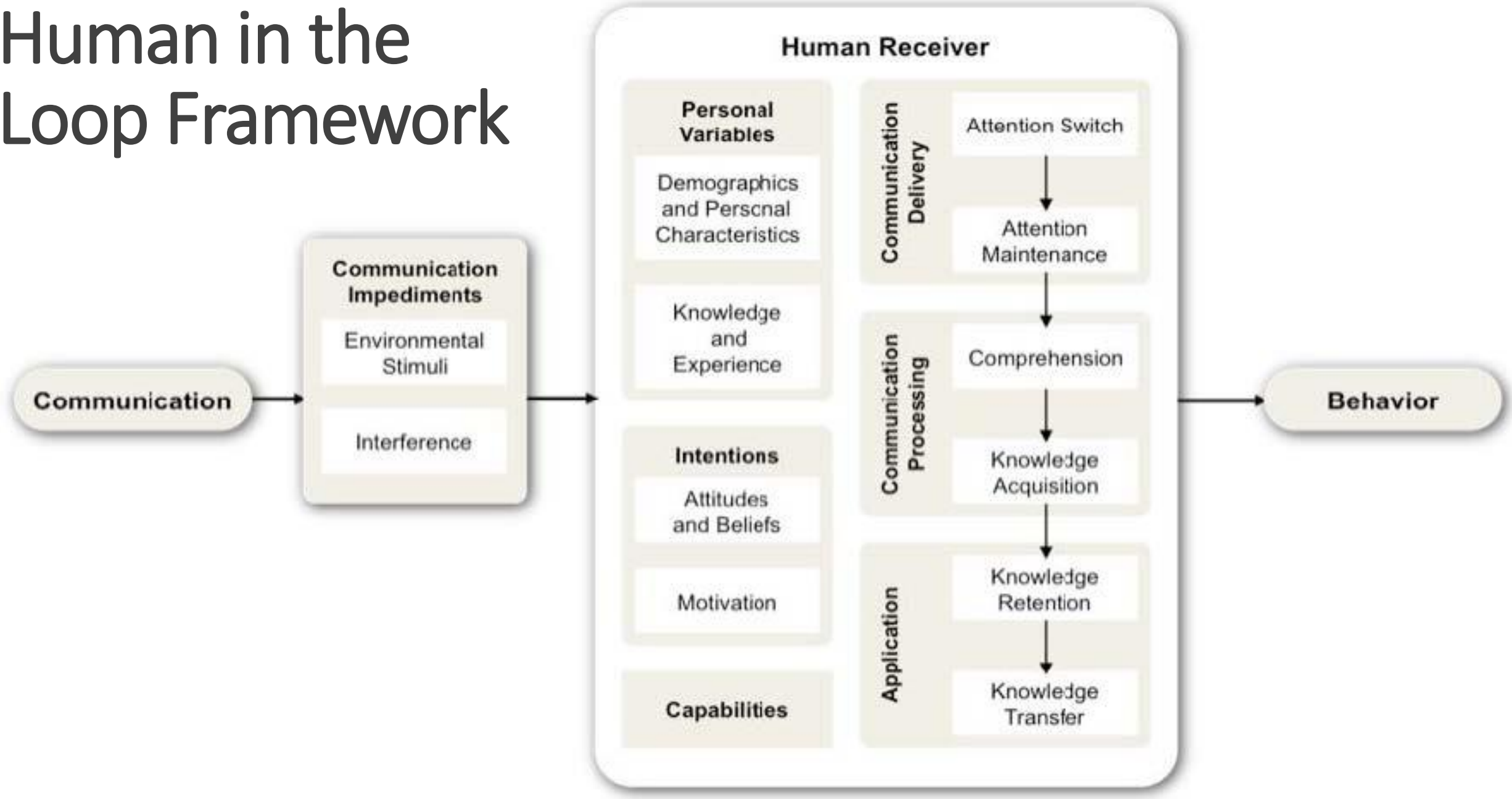


Stages in a cyber attack

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

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

Reply | Forward | Archive | Junk | Delete | More

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

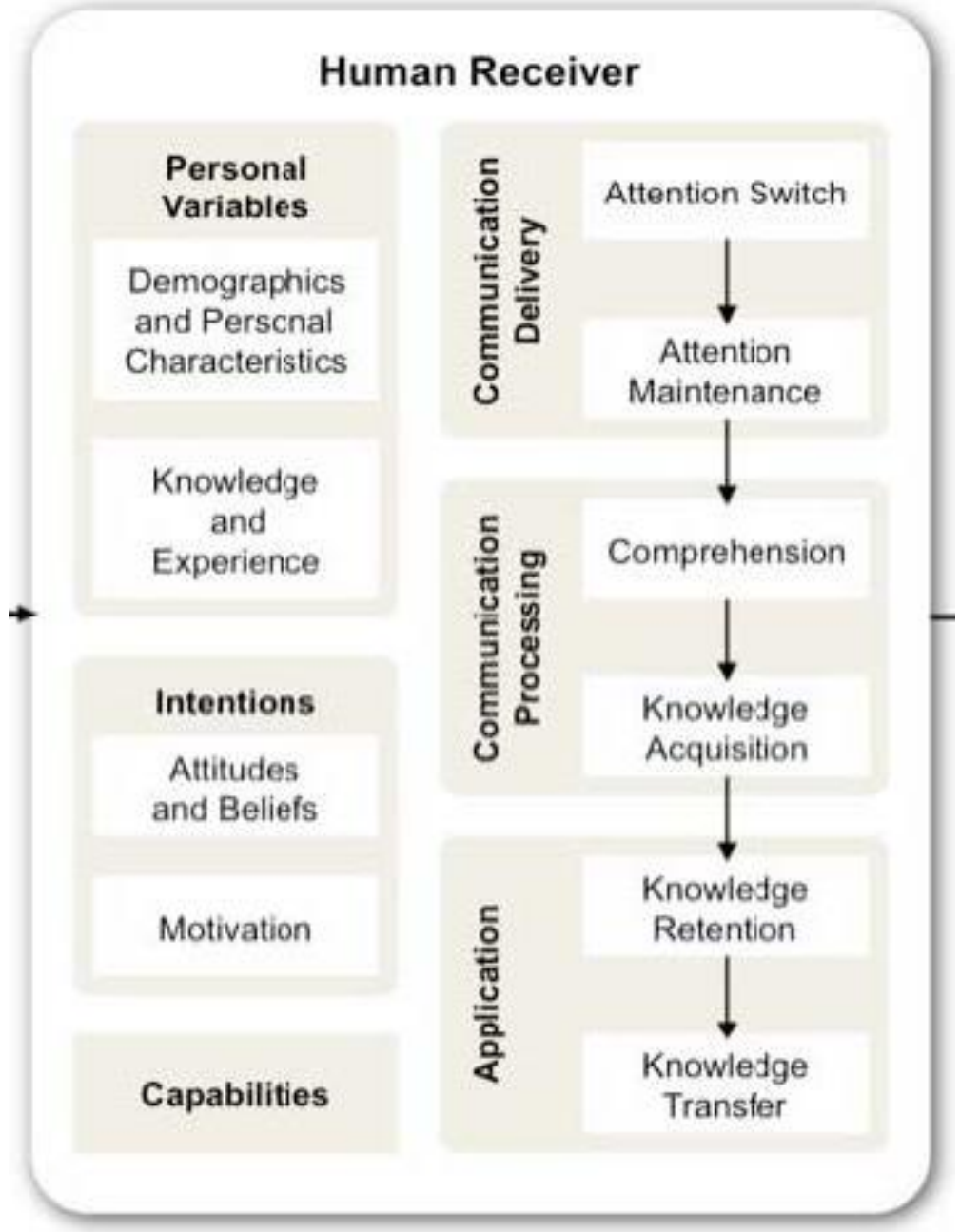
To Me <Kami.Vaniea@ed.ac.uk>

```
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
```

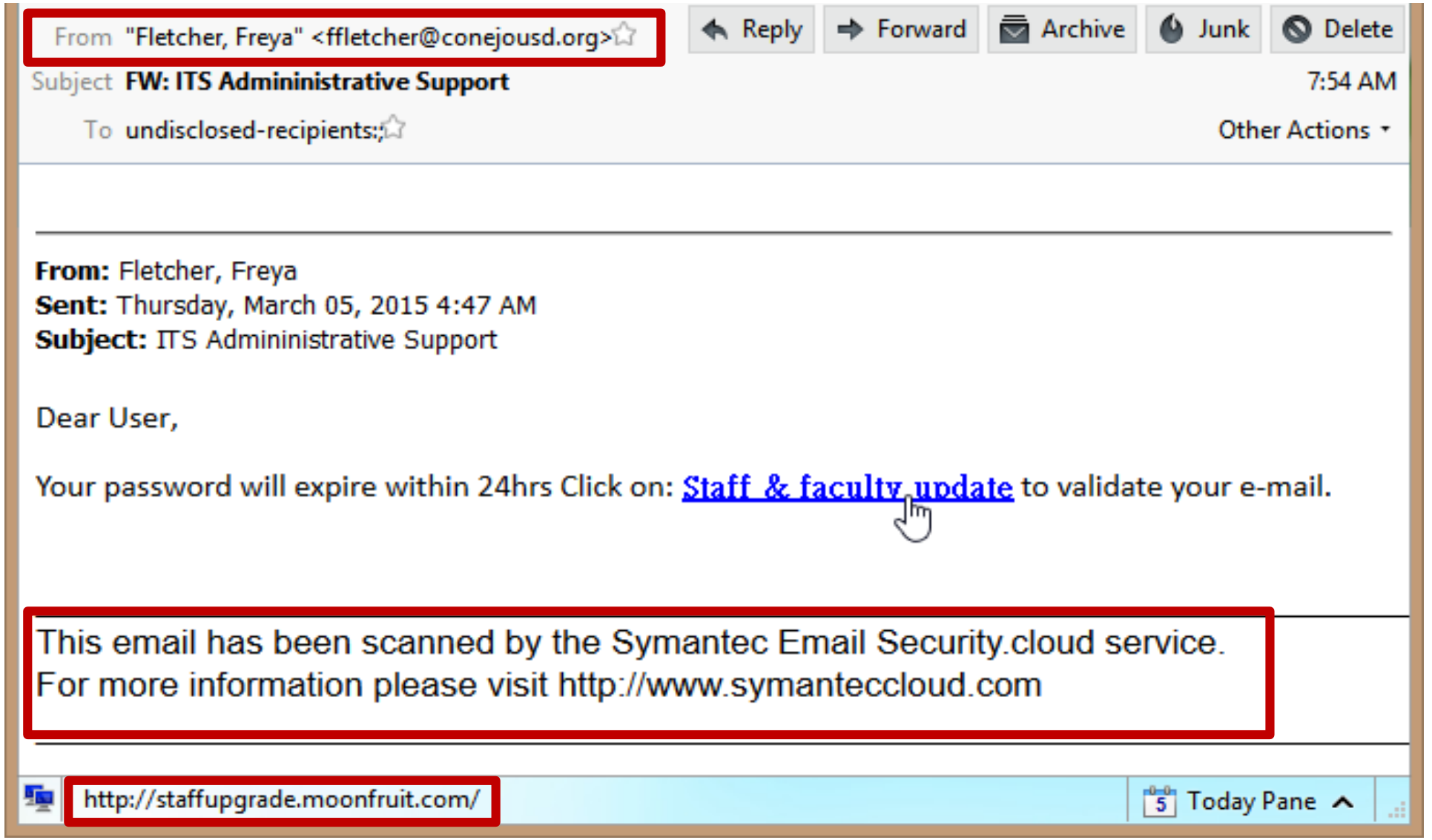


Phishing attacks and training

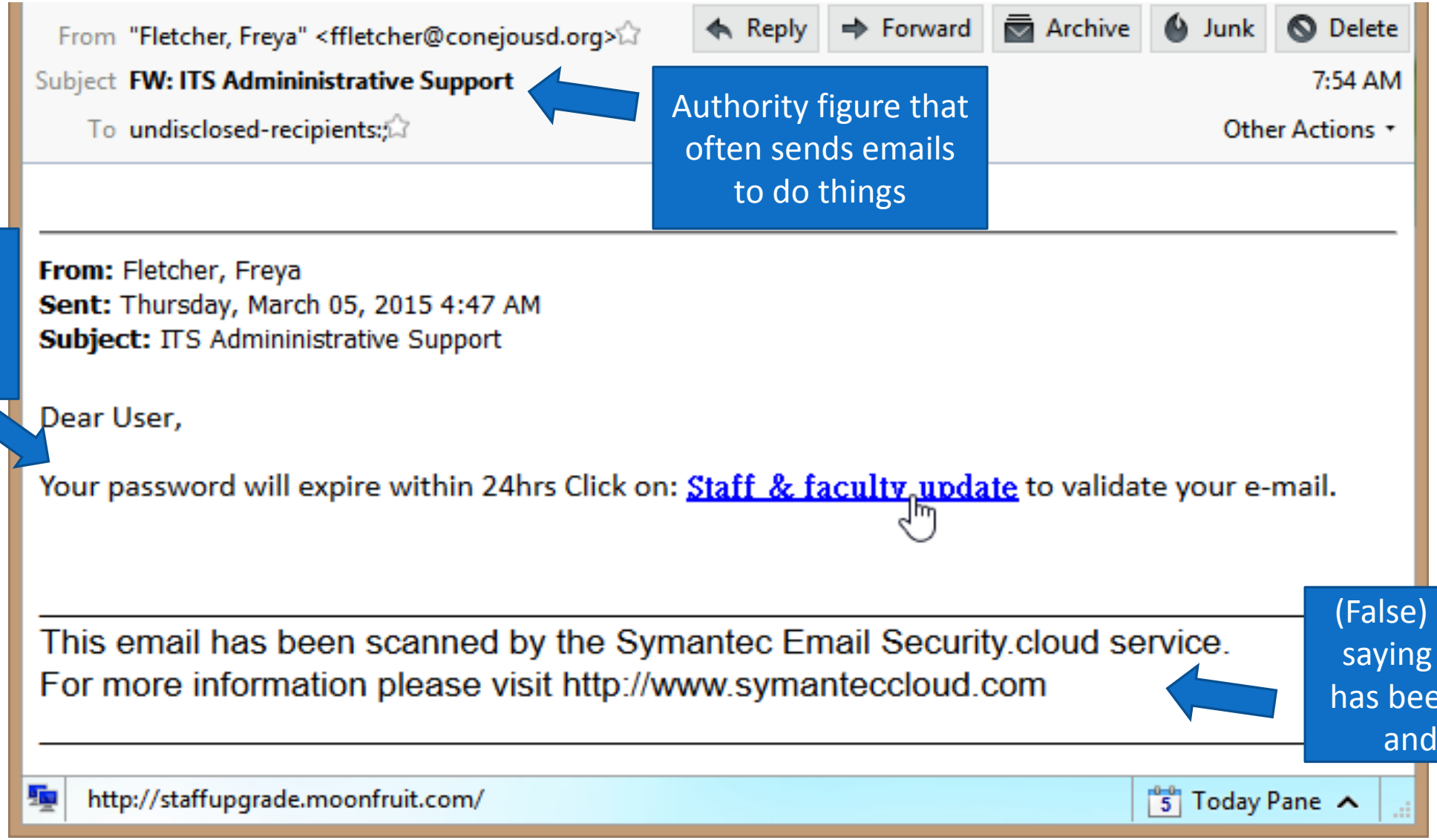
Phishing

- 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

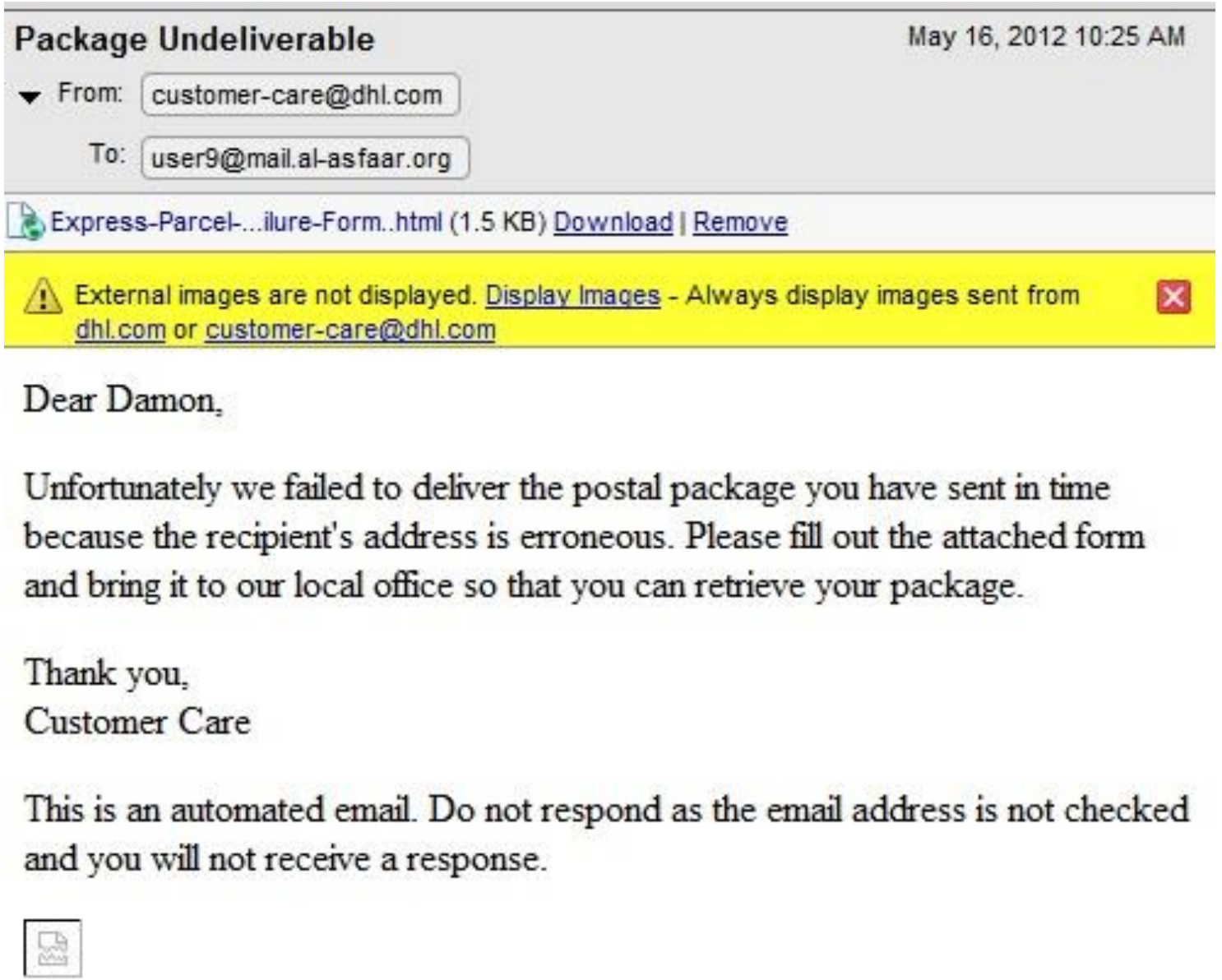
What on this email can be trusted?



(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

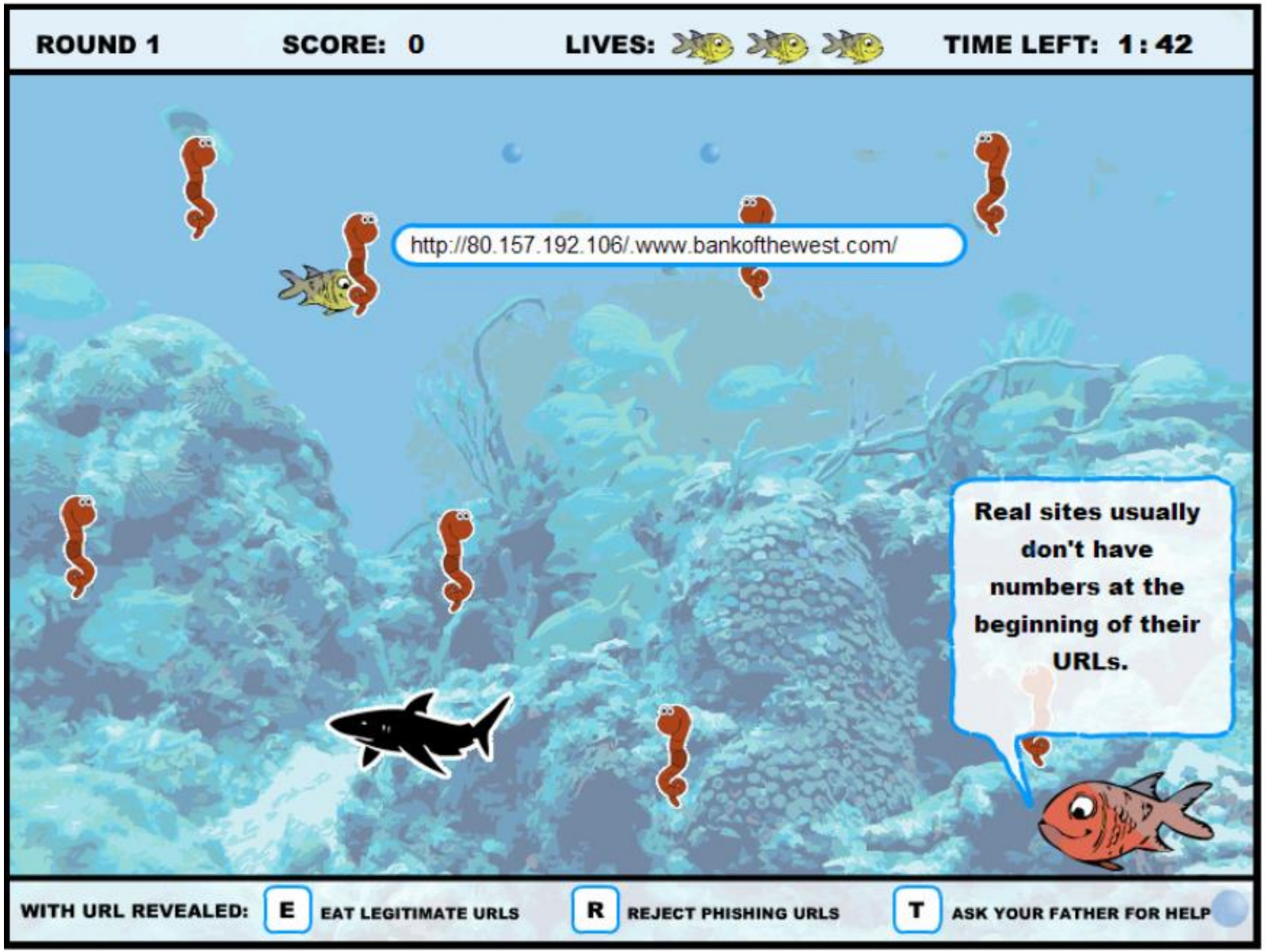
This is an automated email. Do not respond as the email address is not checked and you will not receive a response.

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

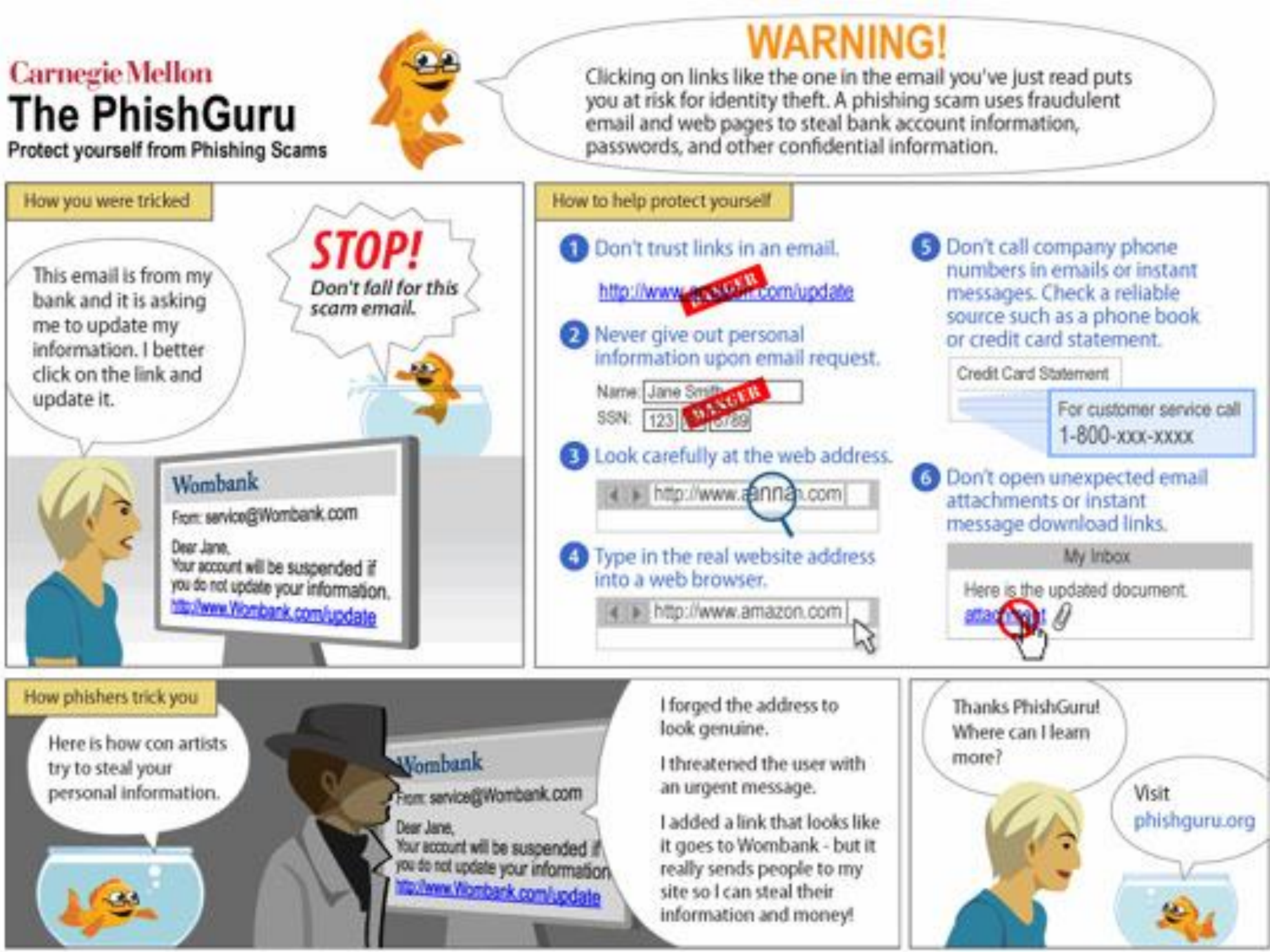
Anti-Phishing Phill

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



PhishGuru

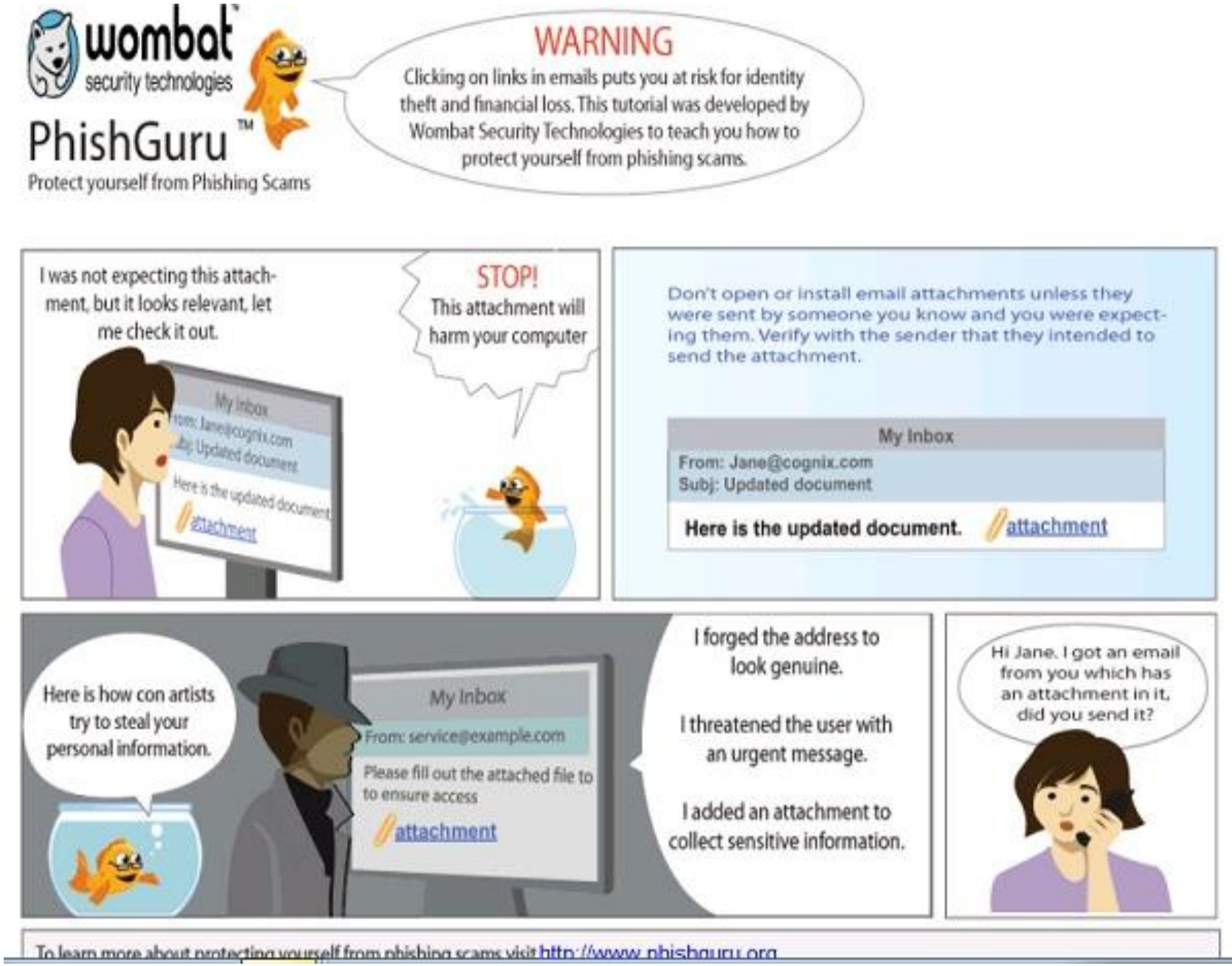
- Comic to train people to spot phishing attacks
- Best time to train is after a users has already fallen for an attack
- Send out fake attacks and train those who click on them



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

Passwords

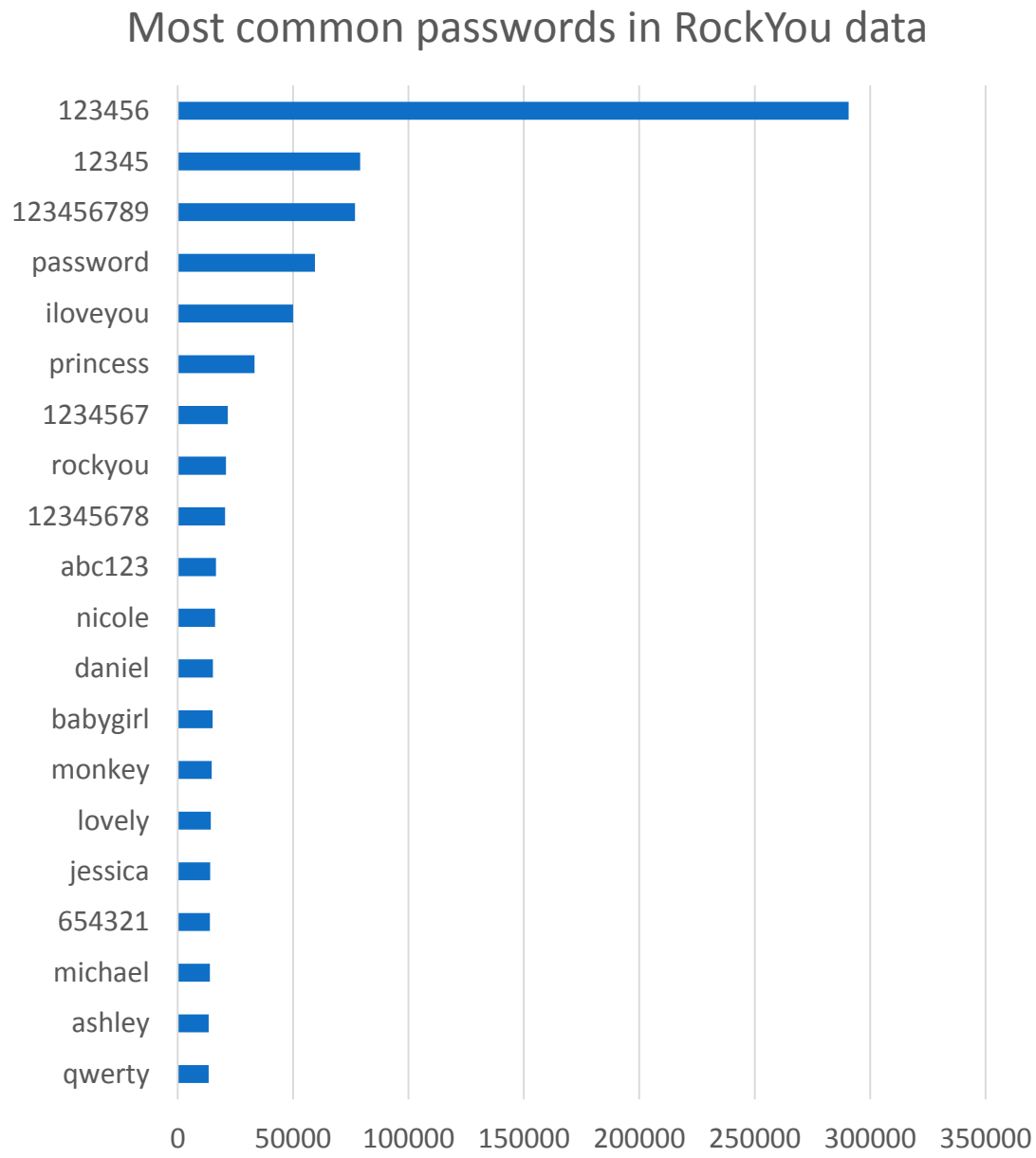
Most recommended security behaviors

- 2/5 non-experts advice involves authentication
- 4/5 expert advice involves authentication

https://googleonlinesecurity.blogspot.com.au/2015/07/new-research-comparing-how-security.html

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



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?

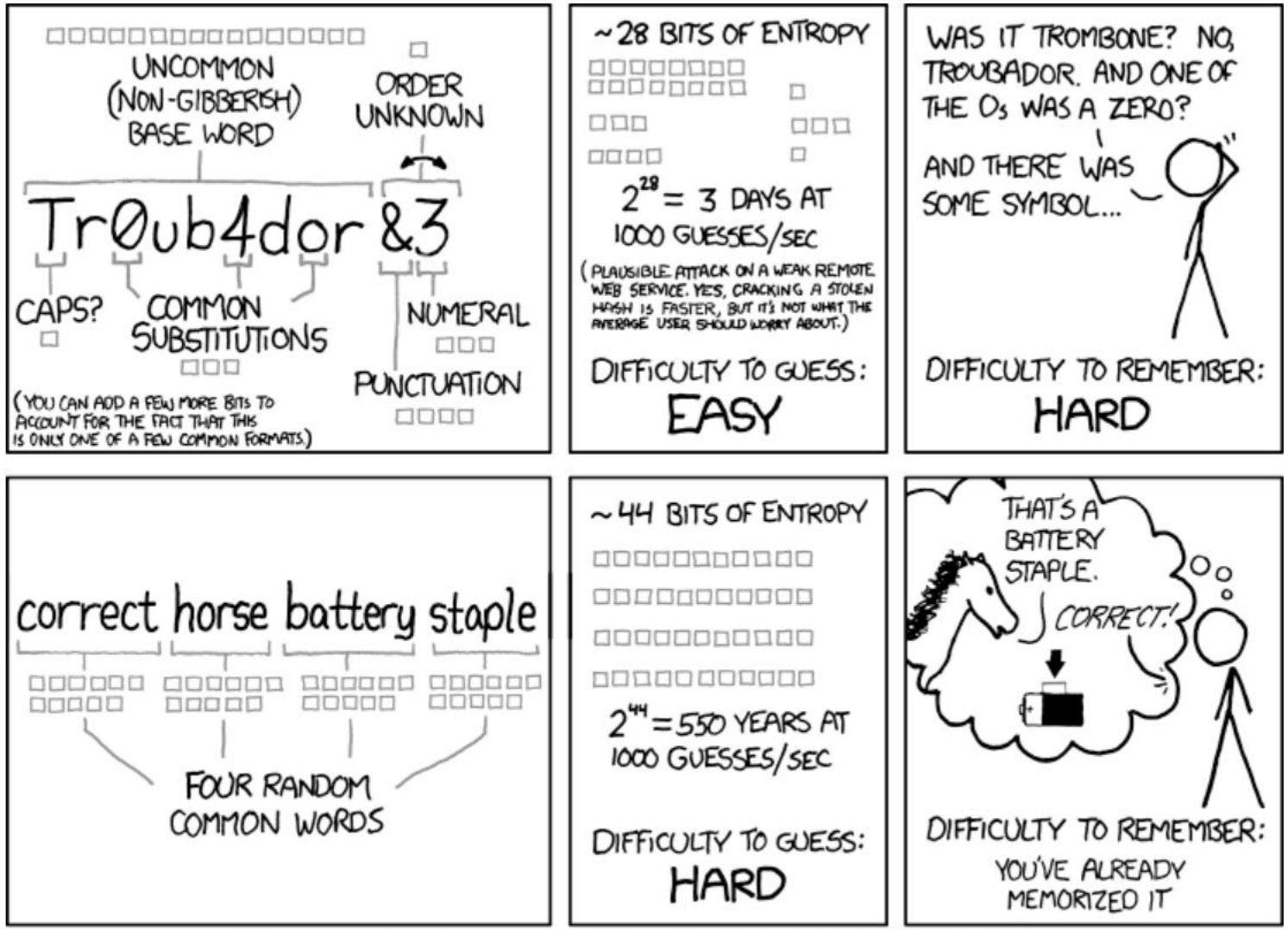
- At least 8 characters, longer better
- No words (any language, especially English)
- Avoid common patterns
  - Upper case letter as first letter
  - Putting the number at the end
  - Putting the special character at the end
- High entropy
  - Lowercase letters
  - Upper case letters
  - Numbers
  -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



https://xkcd.com/936/

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

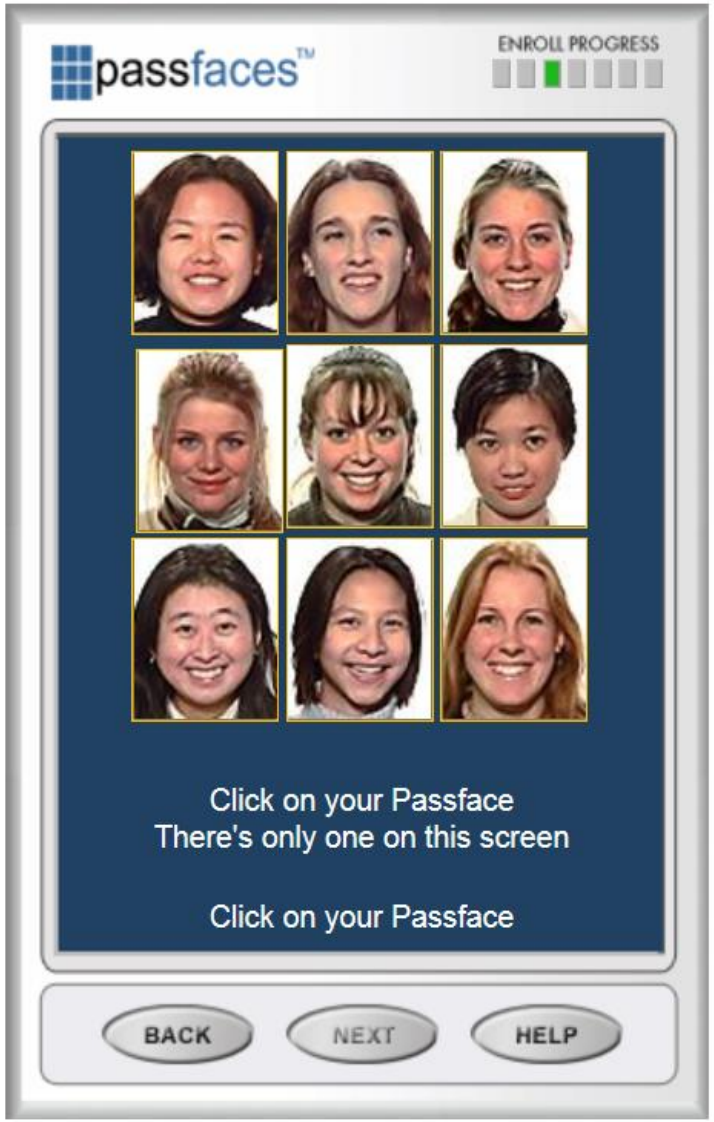
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf

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

Writing usable warnings

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.

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