Security threats II

Introduction

CSCI E 45b: The Cyber World – part B

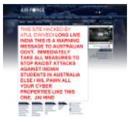
Copyright © Scott Bradner & Ben Gaucherin 2016

Introduction: learning goals

- Understand the types threats to web sites
- Understand the types of social engineering attacks and ways they can be mitigated
- Understand the specific type of social engineering that phishing represents
- Understand how to not get caught by phishing

Copyright © Scott Bradner & Ben Gaucherin 2016

Topics: all required



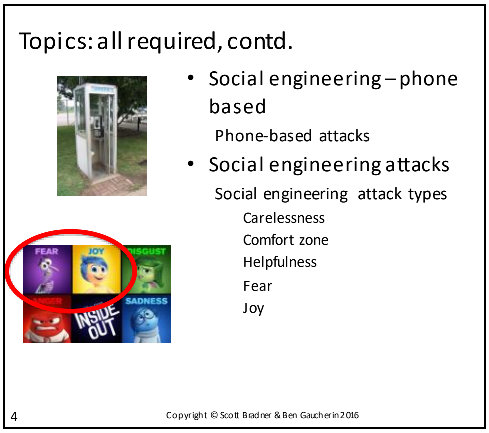
THIS SITE HACKED BY ATUL DWIVEDI LONG LIVE INDIA THIS IS A WARNING MESSAGE TO AUSTRALIAN GOVT. IMMEDIATELY TAKE ALL MEASURES TO STOP RACIST ATTACKS AGAINST INDIAN STUDENTS IN AUSTRALIA ELSE I WIL PAWN ALL YOUR CYBER PROPERTIES LIKE THIS ONE. JAI HIND

- Attacks on websites
  - Types of attacks directly on web sites: defacement as well as improper data access and modification
- Social engineering: base
  - Social engineering key concepts
  - Types of attacks
  - How users help
  - Reverse social engineering
  - People acting normal
  - Believable communications

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.



Topics: all required, contd.

- Social engineering – phone based

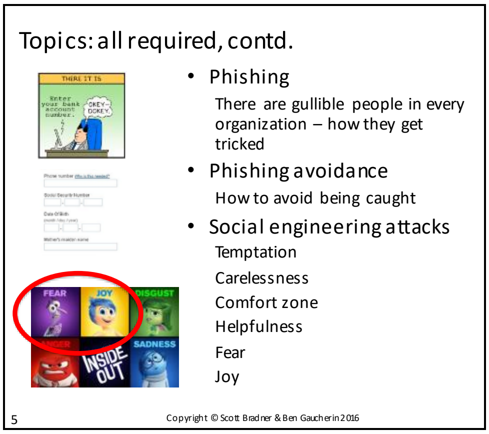
  Phone-based attacks

- Social engineering attacks

  Social engineering attack types

  Carelessness
  Comfort zone
  Helpfulness
  Fear
  Joy

4 Copyright © Scott Bradner & Ben Gaucher in 2016



Topics: all required, contd.

- Phishing

  There are gullible people in every organization – how they get tricked

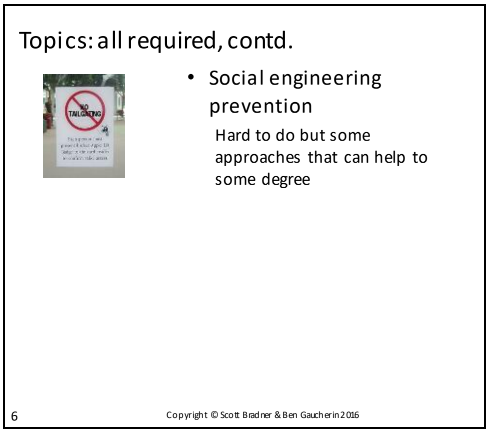
- Phishing avoidance

  How to avoid being caught

- Social engineering attacks

  Temptation
  Carelessness
  Comfort zone
  Helpfulness
  Fear
  Joy

5 Copyright © Scott Bradner & Ben Gaucher in 2016



Topics: all required, contd.

- Social engineering prevention

  Hard to do but some approaches that can help to some degree

6 Copyright © Scott Bradner & Ben Gaucher in 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

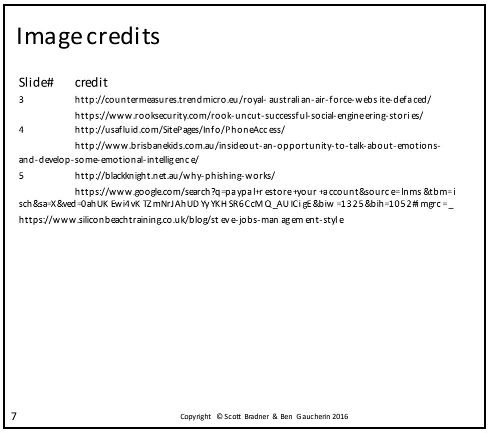


Image credits

Slide#	credit
3	http://countermeasures.trendmicro.eu/royal-australian-air-force-website-defaced/
	https://www.rooksecurity.com/rook-uncut-successful-social-engineering-stories/
4	http://usafluid.com/SitePages/Info/PhoneAccess/
	http://www.brisbanekids.com.au/insideout-an-opportunity-to-talk-about-emotions-and-develop-some-emotional-intelligence/
5	http://blackknight.net.au/why-phishing-works/
	https://www.google.com/search?q=paypal+restore+your+account&source=lnms&tbm=isch&sa=X&ved=0ahUKEwi4vKTZmNrJAhUDYyYKHSR6CcMQ_AUICigE&biw=1325&bih=1052#imgrc=_

https://www.siliconbeachtraining.co.uk/blog/steve-jobs-management-style

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

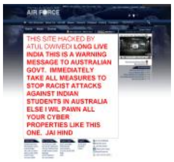
Security threats II

Attacks on websites

CSCI E 45b: The Cyber World – part B

Copyright © Scott Bradner & Ben Gaucherin 2016

Some of the more "popular" attacks

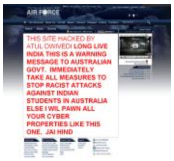


THIS SITE HACKED BY ATUL DWIVEDI LONG LIVE INDIA THIS IS A WARNING MESSAGE TO AUSTRALIAN GOVT. IMMEDIATELY TAKE ALL MEASURES TO STOP RACIST ATTACKS AGAINST INDIAN STUDENTS IN AUSTRALIA ELSE I WIL PAWN ALL YOUR CYBER PROPERTIES LIKE THIS ONE. JAI HIND

- Defacement
- SQL injections
- Cross-Site Scripting XSS
- Cross-Site Reference Forgery – CSRF
- UI Redressing, Click-jacking
- …

Copyright © Scott Bradner & Ben Gaucherin 2016

Defacement



THIS SITE HACKED BY ATUL DWIVEDI LONG LIVE INDIA THIS IS A WARNING MESSAGE TO AUSTRALIAN GOVT. IMMEDIATELY TAKE ALL MEASURES TO STOP RACIST ATTACKS AGAINST INDIAN STUDENTS IN AUSTRALIA ELSE I WIL PAWN ALL YOUR CYBER PROPERTIES LIKE THIS ONE. JAI HIND

- Changing or making it look like the content of a web page (preferably the home page of a site) has been changed

  Done by actually changing the page or by redirecting to a different site (DNS hijacking)

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

SQL Injection

- Entering SQL statements (partial or complete) in web forms to get/modify the information in the database of the application or force the display of information that should not be accessible

'OR 1=1; --

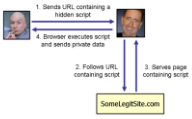
Robert'); DROP TABLE Students;--

HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

4

Copyright © Scott Bradner & Ben Gaucherin 2016

Cross-Site Scripting - XSS


1. Sends URL containing a hidden script
4. Browser executes script and sends private data
2. Follows URL containing script
3. Serves page containing script
SomeLegitSite.com

- XSS is the injection of malicious code in a web page (or a link to a page) resulting in un-expected results when people visit the page or use the link

Non-persistent (or reflected) – passing JavaScript code as a form parameter

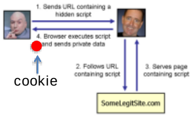
Persistent – embedding JavaScript code in a page (e.g. a post on a web forum)

DOM-based – reflected, but takes advantage of "in browser" processing

5

Copyright © Scott Bradner & Ben Gaucherin 2016

Cross-Site Request Forgery - CSRF


1. Sends URL containing a hidden script
4. Browser executes script and sends private data
cookie
2. Follows URL containing script
3. Serves page containing script
SomeLegitSite.com

- A CSRF takes advantage of the fact that a user's browser may have cookies from authenticating at a site

E.g., Alice goes to an on-line forum and sees a comment in her discussion thread and clicks on a link – unfortunately the link is a link to Alice's banking site (for which she has an active session cookie) and it includes parameters to perform a transfer from Alice's account to a bad guy's account

6

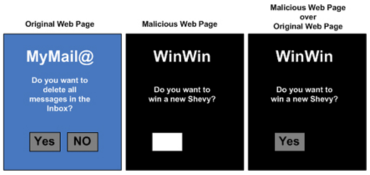
Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

UI redressing, Click-jacking

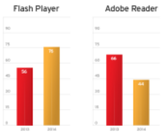
- Using visible or invisible HTML elements overlaid on legitimate ones to get information, or perform actions unbeknownst to the user (e.g., IFrame overlay)


Original Web Page
Malicious Web Page
Malicious Web Page over Original Web Page
MyMail@
Do you want to delete all messages in the Inbox?
Yes
NO
WinWin
Do you want to win a new Shevy?
WinWin
Do you want to win a new Shevy?
Yes

7 Copyright © Scott Bradner & Ben Gaucherin 2016

Browser as a major “facilitator” of attack

- Browsers are generic, complex, multi-purpose client software
- Being the software you use to visit websites, they are a prime targets to be compromised
- After far too long, Flash officially died at the end of 2020 when Adobe killed it



UPDATED

8 Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

Drawings by Scott Bradner unless noted

Slide# credit

2 & 3 - http://countermeasures.trendmicro.eu/royal-australian-air-force-website-defaced/

4 – car - http://www.petefinnigan.com/forum/yabb/YaBB.cgi?board=db_general;action=display;num=1209807861

- xkcd - https://xkcd.com/327/

5 & 6 - https://moz.com/ugc/protect-your-site-and-you-users-against-crosssite-scripting

7 - https://www.imperva.com/resources/glossary?term=clickjacking_ui_redressing

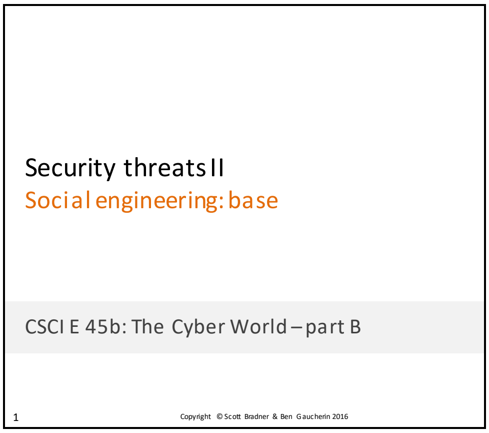
8 – firefox - http://cheeaun.com/blog/2005/01/firefox-logo-mania/

- chart - http://blog.trendmicro.com/trendlabs-security-intelligence/remembering-the-vulnerabilities-of-2014/

9 Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

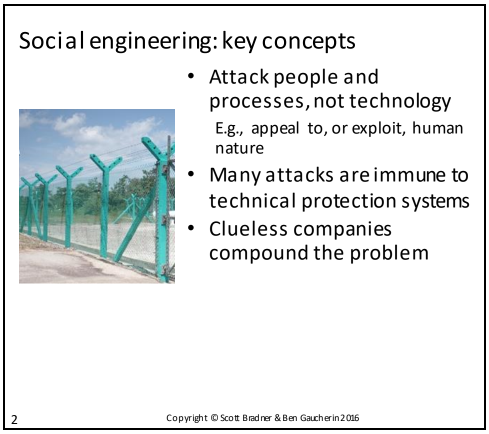


Security threats II

Social engineering: base

CSCI E 45b: The Cyber World – part B

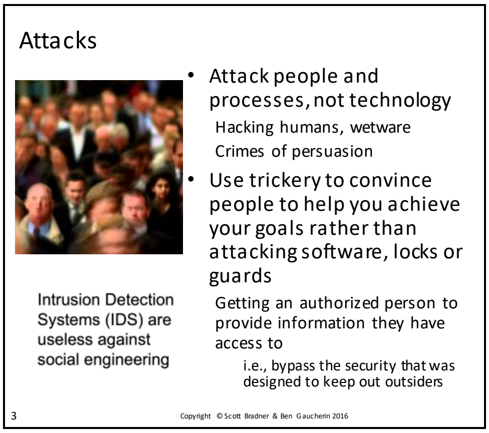
Copyright © Scott Bradner & Ben Gaucherin 2016



Social engineering: key concepts

- Attack people and processes, not technology
  - E.g., appeal to, or exploit, human nature
- Many attacks are immune to technical protection systems
- Clueless companies compound the problem

Copyright © Scott Bradner & Ben Gaucherin 2016



Attacks

- Attack people and processes, not technology
  - Hacking humans, wetware
  - Crimes of persuasion
- Use trickery to convince people to help you achieve your goals rather than attacking software, locks or guards
  - Getting an authorized person to provide information they have access to
    - i.e., bypass the security that was designed to keep out outsiders

Intrusion Detection Systems (IDS) are useless against social engineering

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

Attacks, contd.

- People acting “normal”
- Believable communications (a.k.a. phishing)
  - Snail mail
  - Phone-based
  - Email
- Temptation
- Carelessness
- Comfort zone
- Helpfulness
- Fear
- Joy

Copyright © Scott Bradner & Ben Gaucherin 2016

One thing that makes it easy

- People do not fully appreciate the importance of security controls and their role in following them

Copyright © Scott Bradner & Ben Gaucherin 2016

One thing that makes it easy, contd.

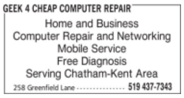
- Organizers of Infosecurity 2003 interviewed 152 office workers at London's Waterloo Station
  - 75% told the interviewer their password when asked (as part of a series of questions)
  - 2/3rds said they have given their password to a colleague
  - 2/3rds said they used the same password for all systems (including banking and website access)

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

Reverse social engineering



GEEK 4 CHEAP COMPUTER REPAIR
Home and Business
Computer Repair and Networking
Mobile Service
Free Diagnosis
Serving Chatham-Kent Area
258 Greenfield Lane 519 437-7343

- Attacker acts as someone that can help a user then gets a user to call the attacker for help
  - e.g., attacker posts signs advertising their computer repair business
    - Soon afterward the enterprise computers crash
  - e.g., insider attacker befriends staff in CEO's office and makes sure they know he is an expert that can help if anything goes wrong

Copyright © Scott Bradner & Ben Gaucherin 2016

Reverse social engineering, contd.

GEEK 4 CHEAP COMPUTER REPAIR
Home and Business
Computer Repair and Networking
Mobile Service
Free Diagnosis
Serving Chatham-Kent Area
258 Greenfield Lane 519 437-7343

- User calls to get things fixed and offers, without prompting, access information (username & password)

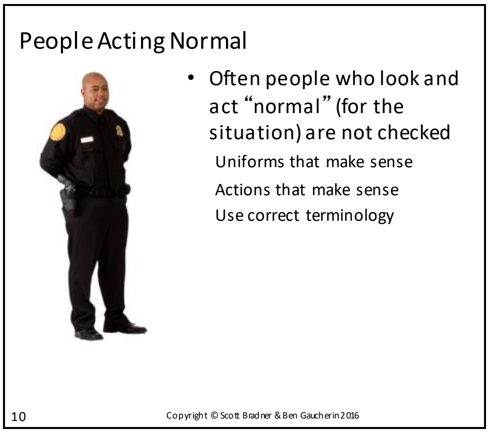
Copyright © Scott Bradner & Ben Gaucherin 2016

Social Engineering
People acting "normal"

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

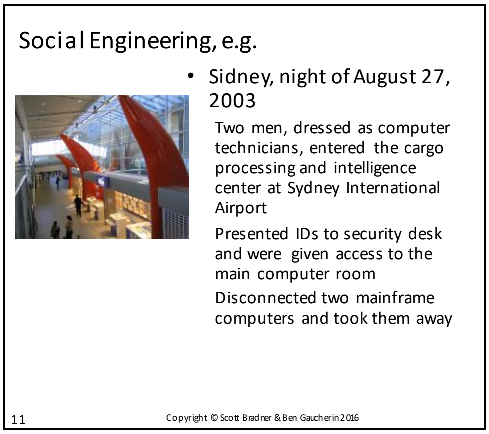


People Acting Normal

- Often people who look and act “normal” (for the situation) are not checked
  - Uniforms that make sense
  - Actions that make sense
  - Use correct terminology

10

Copyright © Scott Bradner & Ben Gaucherin 2016

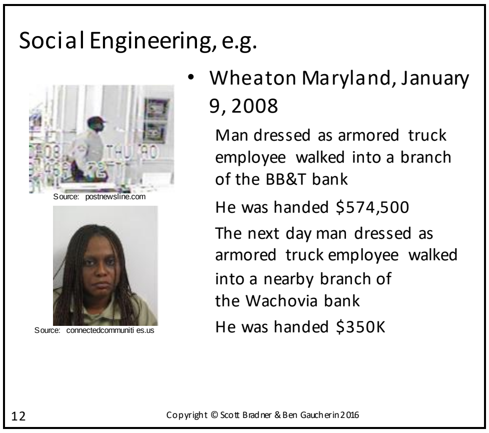


Social Engineering, e.g.

- Sidney, night of August 27, 2003
  - Two men, dressed as computer technicians, entered the cargo processing and intelligence center at Sydney International Airport
  - Presented IDs to security desk and were given access to the main computer room
  - Disconnected two mainframe computers and took them away

11

Copyright © Scott Bradner & Ben Gaucherin 2016



Social Engineering, e.g.

Source: postnewsline.com

Source: connectedcommunities.us

- Wheaton Maryland, January 9, 2008
  - Man dressed as armored truck employee walked into a branch of the BB&T bank
  - He was handed $574,500
  - The next day man dressed as armored truck employee walked into a nearby branch of the Wachovia bank
  - He was handed $350K

12

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

Social Engineering, e.g.

- An acquisition was in process

A team of auditors show up from the acquiring company to perform due diligence

They requested 5 years of customer records and to be left undisturbed in a conference room

They said that their CEO was on travel and unreachable but that the deal depended on the analysis of this information

Later it was determined that they were imposters

Copyright © Scott Bradner & Ben Gaucherin 2016

Social Engineering
Believable communications

Copyright © Scott Bradner & Ben Gaucherin 2016

Believable communications

- Correspondence that “looks right”
- Can appear to be from some person, organization or company you know
- Can have believable content
- But sometimes may be purposefully unbelievable to most people

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

Believable communications, contd.

1914 example

- Not a new concept
  - The Spanish Prisoner scheme – 1588
    - Provide money to release prisoner from a Spanish jail – will get reward
- Appeals to greed, fear, etc.
- Variants include a friend trapped at an airport after theft of purse
- Email makes the scams easier
  - Phishing & spear phishing

16

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

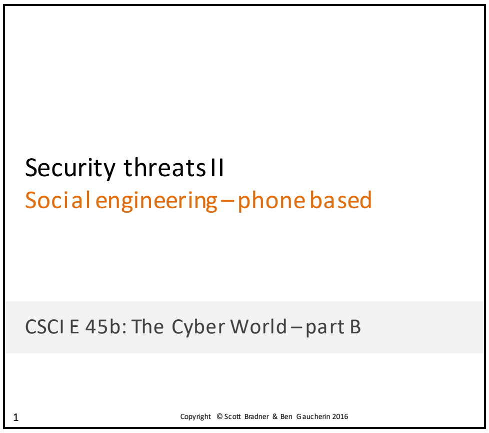
Slide#	credit
2	http://www.vectorinfotech.com/perimeter-fence-intrusion-detection-systems-pids-fids
3	https://www.youtube.com/watch?v=vkGP3nBpaAs
4	https://www.rooksecurity.com/rook-uncut-successful-social-engineering-stories/
5	http://www.ruggedbutts.com/black-who-me-knit-long-sleeve.html
6	http://www.britainfromabove.org.uk/image/eaw035651
7 & 8	http://www.yellowpages.ca/bus/Ontario/Chatham/Geek-4-Cheap-Computer-Repair/100208554.html
10	http://www.admiralsecurity.com/services/armed-uniformed-security-officers/index.html
11	http://www.misho.com.au/commercial.html
12	top – http://www.postnewsline.com/2008/01/cameroonians-ch.html#more bottom - http://connectedcommunities.us/showthread.php?t=16341
13	http://www.aihc-assn.org/Home.aspx
15	http://www.dwgdistribution.com/ecommerce/pc/viewcontent.asp?idpage=16
16	http://priceonomics.com/the-email-scam-with-centuries-of-history/

17

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

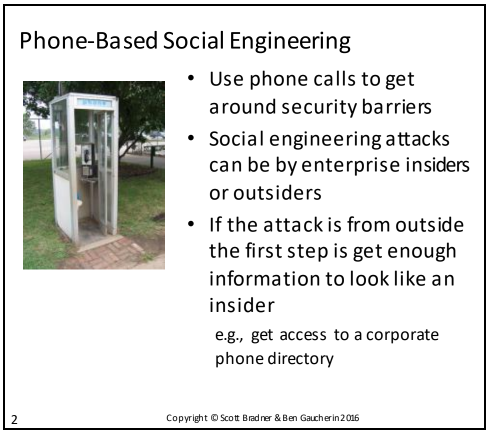


Security threats II

Social engineering – phone based

CSCI E 45b: The Cyber World – part B

Copyright © Scott Bradner & Ben Gaucherin 2016

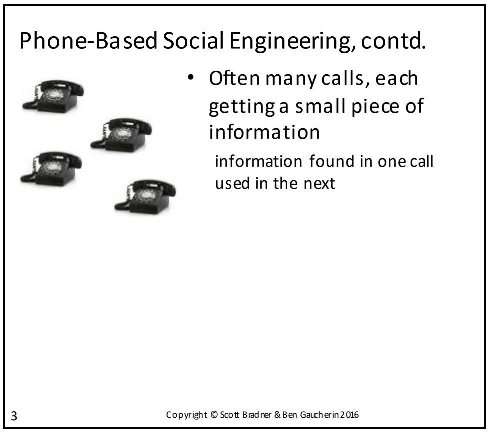


Phone-Based Social Engineering

- Use phone calls to get around security barriers
- Social engineering attacks can be by enterprise insiders or outsiders
- If the attack is from outside the first step is get enough information to look like an insider

  e.g., get access to a corporate phone directory

Copyright © Scott Bradner & Ben Gaucherin 2016



Phone-Based Social Engineering, contd.

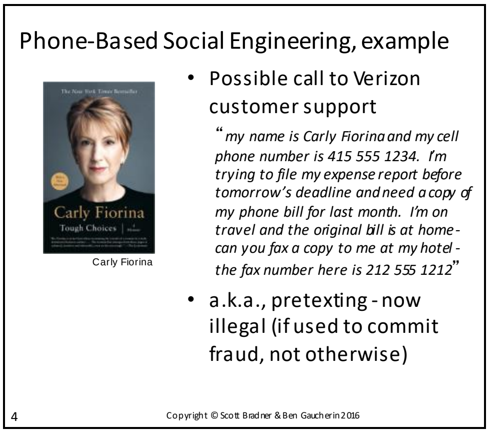
- Often many calls, each getting a small piece of information

  information found in one call used in the next

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.



Phone-Based Social Engineering, example

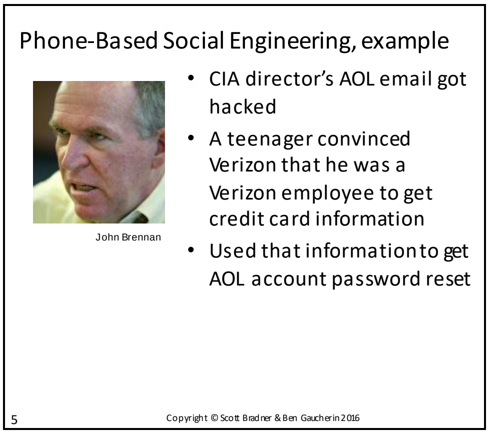
- Possible call to Verizon customer support

  "my name is Carly Fiorina and my cell phone number is 415 555 1234. I'm trying to file my expense report before tomorrow's deadline and need a copy of my phone bill for last month. I'm on travel and the original bill is at home - can you fax a copy to me at my hotel - the fax number here is 212 555 1212"

- a.k.a., pretexting - now illegal (if used to commit fraud, not otherwise)

Carly Fiorina

4 Copyright © Scott Bradner & Ben Gaucherin 2016

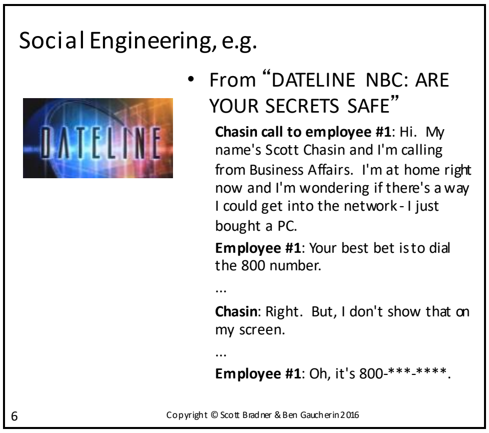


Phone-Based Social Engineering, example

- CIA director's AOL email got hacked
- A teenager convinced Verizon that he was a Verizon employee to get credit card information
- Used that information to get AOL account password reset

John Brennan

5 Copyright © Scott Bradner & Ben Gaucherin 2016



Social Engineering, e.g.

- From "DATELINE NBC: ARE YOUR SECRETS SAFE"

  Chasin call to employee #1: Hi. My name's Scott Chasin and I'm calling from Business Affairs. I'm at home right now and I'm wondering if there's a way I could get into the network - I just bought a PC.

  Employee #1: Your best bet is to dial the 800 number.

  ...

  Chasin: Right. But, I don't show that on my screen.

  ...

  Employee #1: Oh, it's 800-***-****.

6 Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

Social Engineering, e.g., contd.

Chasin call to employee #2: Hi, *****, this is Scott Chasin calling from the computer center

Employee #2: Hi.

...

Chasin: Is everything up and runnin' down there?

employee #2: Uhhh, why? 'we sposed to be down?

Chasin: Yeah we're having some problems, we've been having some reoccuring problems since last night.

employee #2: Believe me, I'm not a computer maven person. Hahaha.

Copyright © Scott Bradner & Ben Gaucherin 2016

Social Engineering, e.g., contd.

Chasin: Hahah. That's all right, I'll help ya out! If you log out and log back in, we'll go through the whole scenario so I can see if everything's ok on my end. Can you do that for me?

employee #2: I think so...hold on...

Chasin: Why don't you tell me what your login id is cuz I'm gonna watch you come across the network so I can see where the problem's arising from.

employee #2: What my login is?

Chasin: Yeah

employee #2: *****

Chasin: What password do you enter to get into the BIOS, [BIOC, BIAC {unintelligible}]?

employee #2: shy

...

Copyright © Scott Bradner & Ben Gaucherin 2016

Social Engineering, e.g., contd.

- **Chasin:** Ok, I'll tell ya what I'm gonna do, I'll go in there and see if you have any stuck processes and I'll call ya back and tell ya when it's all right.

Copyright © Scott Bradner & Ben Gaucherin 2016

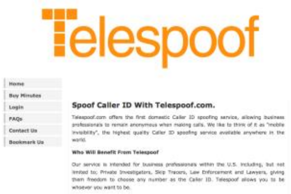
© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

Tools

Voice transformer

- Phone-based social engineering mostly depends on the ability of the caller - but some tools can help



Spoof Caller ID With Telespoof.com.

Telespoof.com offers the first domestic Caller ID spoofing service, allowing business professionals to remain anonymous when making calls. We like to think of it as "mobile invisibility", the highest quality Caller ID spoofing service available anywhere in the world.

Who Will Benefit From Telespoof

Our service is intended for business professionals within the U.S. including, but not limited to: Private Investigators, Skip Tracers, Law Enforcement and Lawyers, giving them freedom to choose any number as the Caller ID. Telespoof allows you to be whoever you want to be.

caller ID spoofing - now illegal, if ...

Copyright © Scott Bradner & Ben Gaucherin 2016

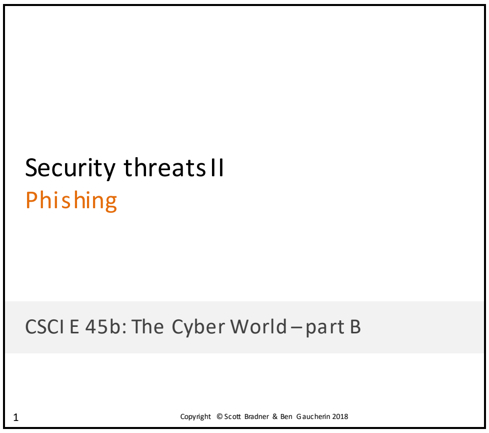
Image credits

Slide#	credit
2	http://usafluid.com/SitePages/Info/PhoneAcc ess/
3	http://blog.codinghorror.com/getting-the-interview-phone-scr een-ri ght/
4	http://www.ontheissues.org/Tough_Choices.htm
5	http://counterjihadreport.com/2013/01/30/obama-cia-nominee-hedged-on-hezbollah-terrorists-in-2006-you-cant-divide-the-world-into-good-and-evil/
6-9	http://www.peabodyawards.com/award-profile/datelin e-nbc-the-education-of-ms.-groves
10 – top	https://poetryandothersounds.wordpress.com/tag/portable-studio/
bottom	http://www.telespoof.com/

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

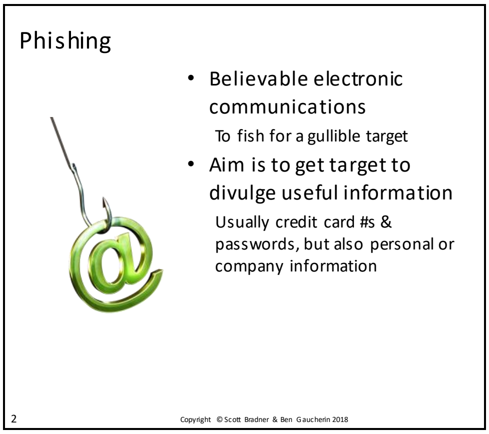


Security threats II

Phishing

CSCI E 45b: The Cyber World – part B

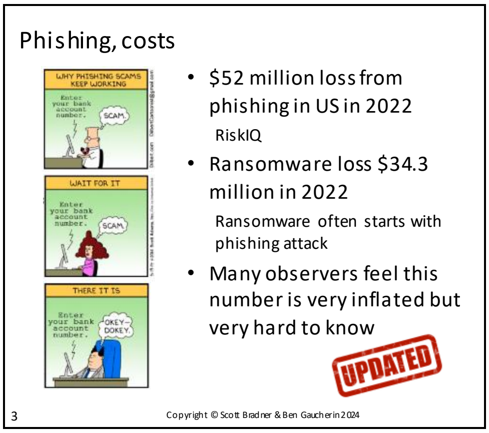
Copyright © Scott Bradner & Ben Gaucherin 2018



Phishing

- Believable electronic communications
  - To fish for a gullible target
- Aim is to get target to divulge useful information
  - Usually credit card #s & passwords, but also personal or company information

Copyright © Scott Bradner & Ben Gaucherin 2018



Phishing, costs

WHY PHISHING SCAMS KEEP WORKING
Enter your bank account number.
SCAM
WAIT FOR IT
Enter your bank account number.
SCAM
THERE IT IS
Enter your bank account number.
OKEY-DOKEY

- $52 million loss from phishing in US in 2022
  - RiskIQ
- Ransomware loss $34.3 million in 2022
  - Ransomware often starts with phishing attack
- Many observers feel this number is very inflated but very hard to know

UPDATED

Copyright © Scott Bradner & Ben Gaucherin 2024

© 2018-2023 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

Phishing: definition

> "Phishing is a broadly launched social engineering attack in which an electronic identity is misrepresented in an attempt to trick individuals into revealing personal credentials that can be used fraudulently."
>
> Anti-Phishing Working Group

- Social engineering attack - try to fool readers
- Broadly launched - not individually targeted

4 Copyright © Scott Bradner & Ben Gaucherin 2018

Phishing, Basics

- Phisher sends bulk email with forged source address
- Email appears to have come from legit site or person
  - e.g., AOL, eBay, bank, on-line merchant, …
- Many include URL for counterfeit web site
  - Looks like the real site
- Can ask for private information or install spyware
  - SSN, credit cards, etc.

5 Copyright © Scott Bradner & Ben Gaucherin 2018

Spear phishing

- A different type of phishing attack
- Differences:
  - Limited number of selected targets
  - Targets are individuals in an organization, because of their role in the organization

6 Copyright © Scott Bradner & Ben Gaucherin 2018

© 2018-2023 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

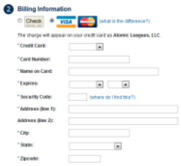
Spear phishing, example

RSA SECURITY

- Can be very successful - e.g., RSA breach
  - Send personalized email to low-level employees
    - Included file “2011 Recruitment plan.xls”
  - Mail system put message into junk mail folder
  - At least one employee retrieved the message out of junk mail folder and opened it

Copyright © Scott Bradner & Ben Gaucherin 2018

Phishing, Environment



2 Billing Information

○ Check ● VISA MasterCard (what is the difference?)

The charge will appear on your credit card as **Atomic Leagues, LLC**

*Credit Card:	
*Card Number:	
*Name on Card:	
*Expires:	
*Security Code:	(where do I find this?)
*Address (line 1):	
Address (line 2):	
*City:	
*State:	
*Zipcode:	

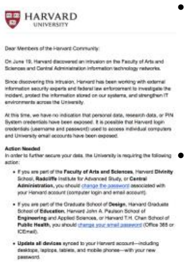
ebay

- Most Internet users deal with legitimate web sites that have or ask for private information
  - 78% of American bank account holders prefer online banking (2022) (Forbes)
  - Most Internet users use e-commerce
  - Many sell or buy on eBay

UPDATED

Copyright © Scott Bradner & Ben Gaucherin 2024

Phishing, Environment, contd.



HARVARD UNIVERSITY

Dear Members of the Harvard Community:

On June 19, Harvard discovered an intrusion on the Faculty of Arts and Sciences and Central Administration information technology networks.

Since discovering this intrusion, Harvard has been working with external information security experts and federal law enforcement to investigate the incident, protect the information stored on our systems, and strengthen IT environments across the University.

At this time, we have no indication that personal data, research data, or PIN System credentials have been exposed. It is possible that Harvard login credentials (username and password) used to access individual computers and University email accounts have been exposed.

Action Needed
In order to further secure your data, the University is requiring the following action:

- If you are part of the **Faculty of Arts and Sciences**, Harvard **Divinity** School, **Radcliffe** Institute for Advanced Study, or **Central Administration**, you should change the password associated with your Harvard account (computer login and email account).
- If you are part of the Graduate School of **Design**, Harvard Graduate School of **Education**, Harvard John A. Paulson School of **Engineering** and Applied Sciences, or Harvard T.H. Chan School of **Public Health**, you should change your email password (Office 365 or ICEmail).
- **Update all devices** synced to your Harvard account—including desktops, laptops, tablets, and mobile phones—with your new password.

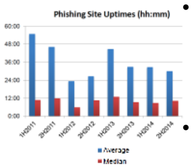
- Many Internet users do not understand what information legitimate web sites will ask you to provide
  - Especially if the web site initiates the contact
- Some web sites do not understand what they should not ask for

Copyright © Scott Bradner & Ben Gaucherin 2018

© 2018-2023 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

Phishing, Life Cycle

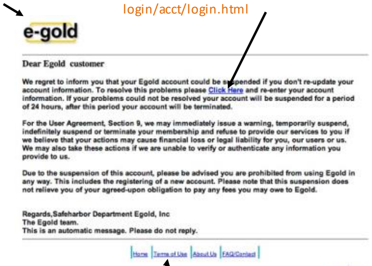


- Create fake web site
  - Configured to send info to a "blind drop"
  - Generally setup on a compromised user computer
- Create blind-drop to receive information
  - e.g., Hotmail account
- Send bulk email, wait for receivers to respond
- Remove fake web site
  - In hours to days
    - Most responses when mail received

Copyright © Scott Bradner & Ben Gaucherin 2018

Phishing, Example1

http://www.taroutschool.com/enter/mcm/login/acct/login.html


e-gold

Dear Egold customer

We regret to inform you that your Egold account could be suspended if you don't re-update your account information. To resolve this problems please Click Here and re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using Egold in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to Egold.

Regards,Safeharbor Department Egold, Inc
The Egold team.
This is an automatic message. Please do not reply.

http://www.e-gold.com/unsecure/terms.htm

G&SR

Copyright © Scott Bradner & Ben Gaucherin 2018

Phishing, Example1, contd.

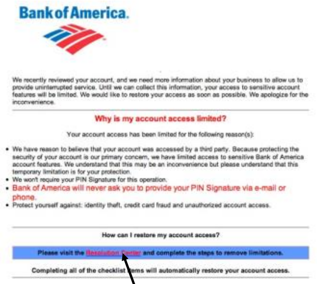
- Email headers

```
From nobody@www1.shopies.net  Fri Dec 22 08:34:33 2006
X-Original-To: sob@newdev.harvard.edu
Delivered-To: sob@newdev.harvard.edu
Received: from www1.shopies.net (unknown
[208.101.52.58])
To: sob@harvard.edu
Subject: Please re-update your egold account
information.
From:  2006 egold Ltd. <service@egold.com>
Reply-To:
Message-Id: <E1Gxkwe-0005BJ-Sk@www1.shopies.net>
...
Date: Fri, 22 Dec 2006 17:00:20 +0300
X-AntiAbuse: This header was added to track abuse,
please include it with any abuse report
X-AntiAbuse: Primary Hostname - www1.shopies.net
X-AntiAbuse: Original Domain - harvard.edu
X-AntiAbuse: Originator/Caller UID/GID - [99 32002] /
[47 12]
X-AntiAbuse: Sender Address Domain - www1.shopies.net
```

Copyright © Scott Bradner & Ben Gaucherin 2018

© 2018-2023 Scott Bradner & Ben Gaucherin. All rights reserved.

Phishing, Example2



Bank of America.

We recently reviewed your account, and we need more information about your business to allow us to provide uninterrupted service. Until we can collect this information, your access to sensitive account features will be limited. We would like to restore your access as soon as possible. We apologize for the inconvenience.

Why is my account access limited?

Your account access has been limited for the following reason(s):

- We have reason to believe that your account was accessed by a third party. Because protecting the security of your account is our primary concern, we have limited access to sensitive Bank of America account features. We understand that this may be an inconvenience but please understand that this temporary limitation is for your protection.
- We won't require your PIN Signature for this operation.
- Bank of America will never ask you to provide your PIN Signature via e-mail or phone.
- Protect yourself against: identity theft, credit card fraud and unauthorized account access.

How can I restore my account access?

Please visit the Resolution Center and complete the steps to remove limitations.

Completing all of the checklist items will automatically restore your account access.

http://gscalw.de/.onlinebanking/bankofamerica.com/

Copyright © Scott Bradner & Ben Gaucherin 2018

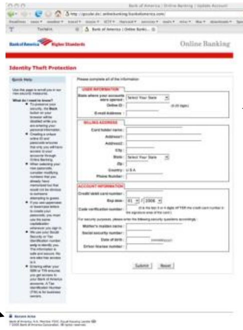
Phishing, Example2, contd.

- Email headers

```
From admin@boa.com   Fri Dec 22 08:58:11 2006
X-Original-To:  sob@newdev.harvard.edu
Delivered-To:  sob@newdev.harvard.edu
...
Received:  from User  ([63.138.5.234])  by mouse-
bgqh4229a  with  Microsoft  SMTPSVC(5.0.2195.6713);
Reply-To:  <no-reply@boa.com>
From:  "Bank of America" <admin@boa.com>
Subject:  Update Your Account !
Date: Fri,  22 Dec 2006 06:03:05  -0800
Message-ID:  <MOUSE-BGQH4229ArdFO00000547@mouse-
bgqh4229a>
...
To: undisclosed-recipients:  ;
```

Copyright © Scott Bradner & Ben Gaucherin 2018

Phishing, Example2 - Form



Bank of America | Online Banking | Update Account

Online Banking

Identity Theft Protection

Quick Help

Please complete all of the information

USER INFORMATION

State where your accounts were opened: Select Your State

Online ID: (6-20 digits)

E-mail Address:

BILLING ADDRESS

Card holder name:

Address1:

Address2:

City:

State: Select Your State

Zip:

Country: U.S.A

Phone Number:

ACCOUNT INFORMATION

Credit/ debit card number:

Exp date: 01 / 2006

Code verification number:

For security purposes, please enter the following security questions accordingly:

Mother's maiden name:

Social security number:

Date of birth:

Driver license number:

Submit Reset

not https

wants BoA ID

wants your address

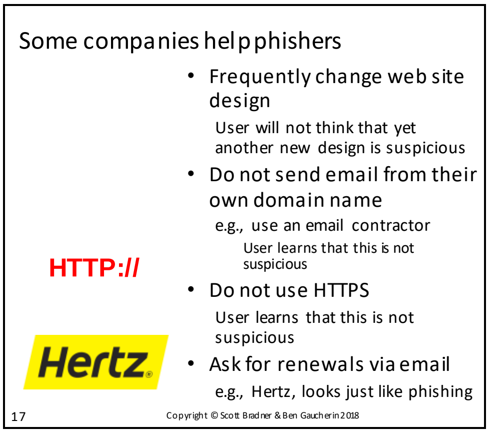
wants CC#, SSN, etc.

fake lock

Copyright © Scott Bradner & Ben Gaucherin 2018

© 2018-2023 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.



Some companies help phishers

HTTP://

Hertz

- Frequently change web site design
  - User will not think that yet another new design is suspicious
- Do not send email from their own domain name
  - e.g., use an email contractor
    - User learns that this is not suspicious
- Do not use HTTPS
  - User learns that this is not suspicious
- Ask for renewals via email
  - e.g., Hertz, looks just like phishing

Copyright © Scott Bradner & Ben Gaucherin 2018

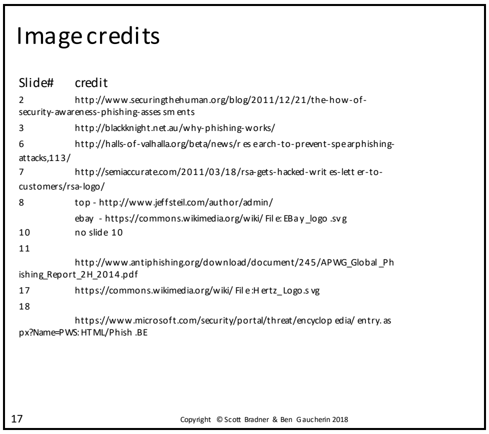


Image credits

Slide#	credit
2	http://www.securingthehuman.org/blog/2011/12/21/the-how-of-security-awareness-phishing-assessments
3	http://blackknight.net.au/why-phishing-works/
6	http://halls-of-valhalla.org/beta/news/research-to-prevent-spearphishing-attacks,113/
7	http://semiaccurate.com/2011/03/18/rsa-gets-hacked-writes-letter-to-customers/rsa-logo/
8	top - http://www.jeffsteil.com/author/admin/
	ebay - https://commons.wikimedia.org/wiki/File:EBay_logo.svg
10	no slide 10
11	http://www.antiphishing.org/download/document/245/APWG_Global_Phishing_Report_2H_2014.pdf
17	https://commons.wikimedia.org/wiki/File:Hertz_Logo.svg
18	https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=PWS:HTML/Phish.BE

Copyright © Scott Bradner & Ben Gaucherin 2018

© 2018-2023 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

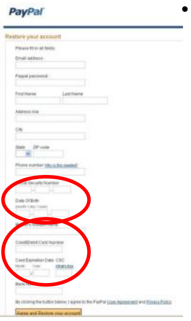
Security threats II

Phishing avoidance

CSCI E 45b: The Cyber World – part B

Copyright © Scott Bradner & Ben Gaucherin 2016

How to not get caught by a phisher



PayPal

Restore your account

Please fill in all fields.

Email address:

Paypal password:

First Name Last Name

Address line

City

State ZIP code

Phone number Why is this needed?

Social Security Number

Date Of Birth (month / day / year)

Mother's maiden name

Credit/Debit Card Number

Card Expiration Date CSC Month Year What's this

Bank name

By clicking the button below, I agree to the PayPal User Agreement and Privacy Policy.

Agree and Restore your account

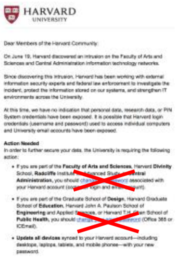
- Understand that almost no legit company would send you mail asking for credit card #s or SSNs

  Some may ask for such information when you contact them and apply for credit, etc.

  You do not want to do business with a company that is so clueless about security that they did ask

Copyright © Scott Bradner & Ben Gaucherin 2016

How to not get caught, contd.



HARVARD UNIVERSITY

Dear Members of the Harvard Community:

On June 19, Harvard discovered an intrusion on the Faculty of Arts and Sciences and Central Administration information technology networks.

Since discovering this intrusion, Harvard has been working with external information security experts and federal law enforcement to investigate the incident, protect the information stored on our systems, and strengthen IT environments across the University.

At this time, we have no indication that personal data, research data, or PIN System credentials have been exposed. It is possible that Harvard login credentials (username and password) used to access individual computers and University email accounts have been exposed.

Action Needed
In order to further secure your data, the University is requiring the following action:

- If you are part of the **Faculty of Arts and Sciences**, Harvard **Divinity** School, **Radcliffe** Institute for Advanced Study, or **Central Administration**, you should change the password associated with your Harvard account (common login and email account).
- If you are part of the Graduate School of **Design**, Harvard Graduate School of **Education**, Harvard John A. Paulson School of **Engineering** and Applied Sciences, or Harvard T.H. Chan School of **Public Health**, you should change your email password (Office 365 or ICEmail).
- **Update all devices** synced to your Harvard account—including desktops, laptops, tablets, and mobile phones—with your new password.

- Never fill in any information on any form that results from you clicking on a URL in a email message

  Type in the URL of the company yourself

- Always look for https when entering any confidential information

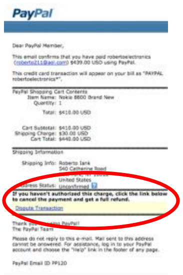
  Even if you typed the URL yourself

  Check for lock (may help)

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

How to not get caught, contd.



PayPal

Dear PayPal Member,

This email confirms that you have paid robertoelectronics (roberto211@aol.com) $439.00 USD using PayPal.

This credit card transaction will appear on your bill as "PAYPAL robertoelectronics*".

PayPal Shopping Cart Contents
Item Name: Nokia 8800 Brand New
Quantity: 1
Total: $410.00 USD

Cart Subtotal: $410.00 USD
Shipping Charge: $30.00 USD
Cart Total: $440.00 USD

Shipping Information
Shipping Info: Roberto Iank
540 Catherine Road
New York, NY 10025
United States
Address Status: Unconfirmed

If you haven't authorized this charge, click the link below to cancel the payment and get a full refund.

Dispute Transaction

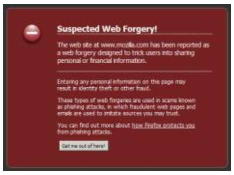
Thank you for using PayPal!
The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

PayPal Email ID PP120

- Never just accept the certificate from a site you do not actually know
- Always question anyone compelling you to immediate action: impending crisis, report of action taken by you that you did not actually take, giving a near-term deadline, etc.

Browsers try to help



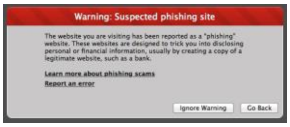
Suspected Web Forgery!

The web site at www.mozilla.com has been reported as a web forgery designed to trick users into sharing personal or financial information.

Entering any personal information on this page may result in identity theft or other fraud.

These types of web forgeries are used in scams known as phishing attacks, in which fraudulent web pages and emails are used to imitate sources you may trust.

You can find out more about how Firefox protects you from phishing attacks.



Warning: Suspected phishing site

The website you are visiting has been reported as a "phishing" website. These websites are designed to trick you into disclosing personal or financial information, usually by creating a copy of a legitimate website, such as a bank.

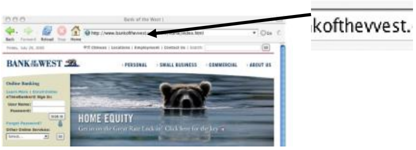
Learn more about phishing scams
Report an error

Certificates

- Certificates (& yellow URL bar and/or green lock) are not good enough by themselves

  Could be legit certificate for deceptive URL

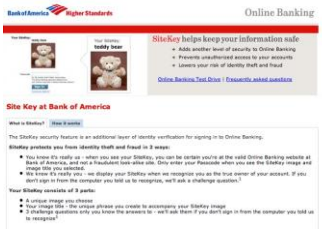
  paypa1.com (digit one vs. lower case “L”)
  Unicode glyph in URL (looks like an “e” but is not)
  Bank of the vvest (rather than Bank of the West)



© 2016 Scott Bradner & Ben Gaucher. All rights reserved.

What can a site do?

- What can a phishing target do?
- e.g., let user customize experience - e.g., BoA



SiteKey helps keep your information safe

- Adds another level of security to Online Banking
- Prevents unauthorized access to your accounts
- Lowers your risk of identity theft and fraud

Online Banking Test Drive | Frequently asked questions

Site Key at Bank of America

What is SiteKey? | How it works

The SiteKey security feature is an additional layer of identity verification for signing in to Online Banking.

SiteKey protects you from identity theft and fraud in 2 ways:

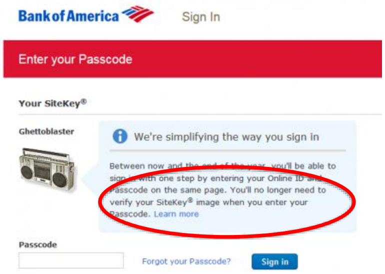
- You know it's really us - when you see your SiteKey, you can be certain you're at the valid Online Banking website at Bank of America, and not a fraudulent look-alike site. Only enter your Passcode when you see the SiteKey image and image title you selected.
- We know it's really you - we display your SiteKey when we recognize you as the true owner of your account. If you don't sign in from the computer you told us to recognize, we'll ask a challenge question.[1]

Your SiteKey consists of 3 parts:

- A unique image you choose
- Your image title - the unique phrase you create to accompany your SiteKey image
- 3 challenge questions only you know the answers to - we'll ask them if you don't sign in from the computer you told us to recognize[1]

What can a site do, contd.

- BoA gave up



We're simplifying the way you sign in

Between now and the end of the year, you'll be able to sign in with one step by entering your Online ID and Passcode on the same page. You'll no longer need to verify your SiteKey® image when you enter your Passcode. Learn more

What can a site do?, contd.

MarkMonitor AntiFraud

Powerful protection from damaging phishing and malware attacks

MarkMonitor AntiFraud™ is the most comprehensive solution available for protecting an enterprise's reputation and customers against phishing and malware attacks. Leveraging the industry's most extensive network of industry alliances, MarkMonitor AntiFraud emphasizes prevention and loss mitigation while quickly detecting, monitoring and responding to attacks that do get underway. Enterprises use this powerful solution to preserve brand equity and customer trust while minimizing the potentially heavy costs and losses associated with attacks.

- Solutions for spoofed sites
  - Monitor mail for phishing attacks using company name
    - Then trace site & demand ISP take site down
  - Monitor domain name registrations
  - Monitor selling of stolen information
  - Multi-factor & mutual authentication
- Solutions for targeted users
  - Client toolbars
  - Web and email filters

Why is it hard?

Rachna Dhamija

Doug Tygar

Marti Hearst

- Why is it hard to protect against phishing?
  - People are fallible, and do not pay enough attention
    - Research: most customers ignore "wrong" picture
  - Client systems have general purpose graphics support
  - Customer identification of company by logos, etc.
  - Unmotivated users - focus on task at hand, security secondary

Copyright © Scott Bradner & Ben Gaucherin 2016

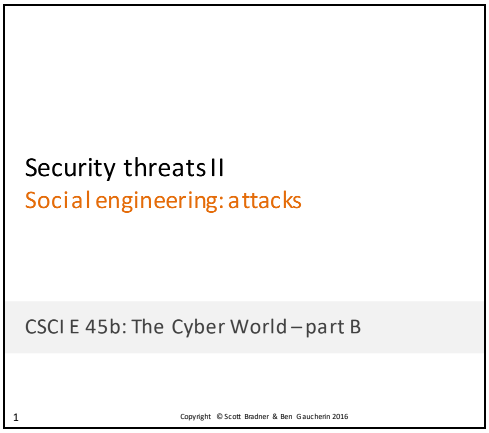
Image credits

Slide#	credit
2	https://www.google.com/search?q=paypal+restore+your+account&source=lnms&tbm=isch&sa=X&ved=0ahUKEwi4vKTZmNrJAhUDYyYKHSR6CcMQ_AUICigE&biw=1325&bih=1052#imgrc=_
4	http://blog.mxlab.eu/tag/phishing/page/7/
5	http://phildawson.tumblr.com/post/20058505/new-firefox-3-suspected-web-forgery-page http://www.freefixer.com/b/wkj-datropy-com-web-forgery/
6	http://www.eecs.berkeley.edu/~tygar/papers/Phishing/why_phishing_works.pdf
7	https://www.bankofamerica.com
8	http://chicagolibrarian.com/node/1110
9	https://www.markmonitor.com/services/antifraud.php
10	Dhamija - https://angel.co/rachna-dhamija tygar - http://citris-uc.org/phishers-beware/ hearst - https://www.eecs.berkeley.edu/Faculty/Homepages/hearst.html

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

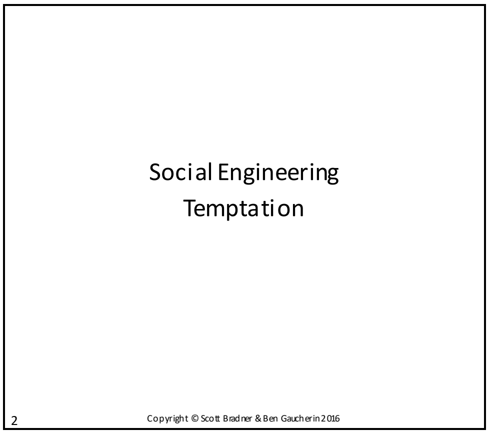


Security threats II

Social engineering: attacks

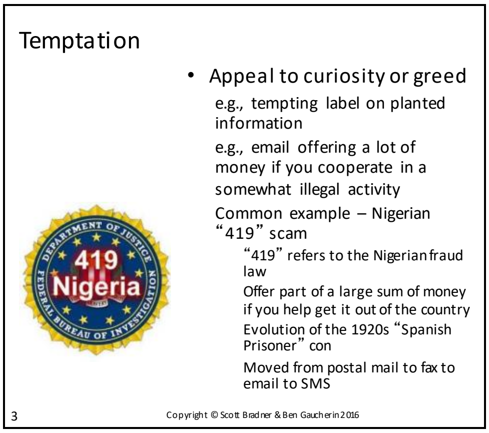
CSCI E 45b: The Cyber World – part B

Copyright © Scott Bradner & Ben Gaucherin 2016



Social Engineering
Temptation

Copyright © Scott Bradner & Ben Gaucherin 2016



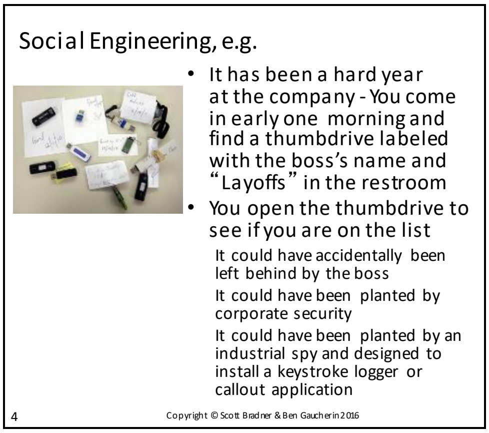
Temptation

- Appeal to curiosity or greed
  - e.g., tempting label on planted information
  - e.g., email offering a lot of money if you cooperate in a somewhat illegal activity
  - Common example – Nigerian "419" scam
    - "419" refers to the Nigerian fraud law
    - Offer part of a large sum of money if you help get it out of the country
    - Evolution of the 1920s "Spanish Prisoner" con
    - Moved from postal mail to fax to email to SMS

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

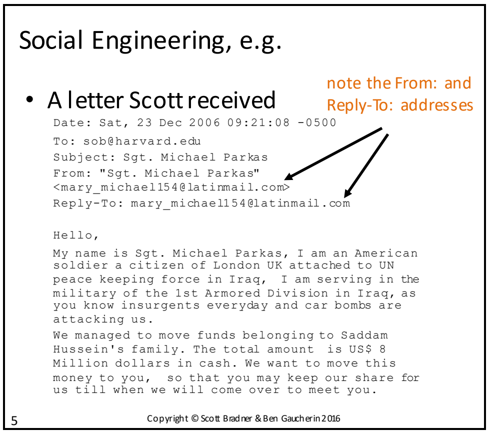
For use by students in Harvard Extension School CSCI E-45b only. Do not copy.



Social Engineering, e.g.

- It has been a hard year at the company - You come in early one morning and find a thumbdrive labeled with the boss's name and "Layoffs" in the restroom
- You open the thumbdrive to see if you are on the list
  - It could have accidentally been left behind by the boss
  - It could have been planted by corporate security
  - It could have been planted by an industrial spy and designed to install a keystroke logger or callout application

Copyright © Scott Bradner & Ben Gaucherin 2016



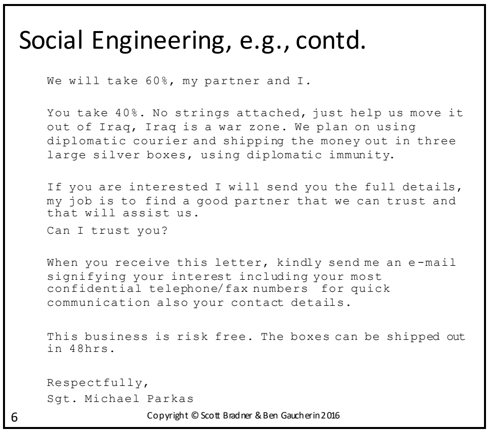
Social Engineering, e.g.

- A letter Scott received

note the From: and Reply-To: addresses

```
Date: Sat, 23 Dec 2006 09:21:08 -0500
To: sob@harvard.edu
Subject: Sgt. Michael Parkas
From: "Sgt. Michael Parkas"
<mary_michael154@latinmail.com>
Reply-To: mary_michael154@latinmail.com

Hello,
My name is Sgt. Michael Parkas, I am an American
soldier a citizen of London UK attached to UN
peace keeping force in Iraq,  I am serving in the
military of the 1st Armored Division in Iraq, as
you know insurgents everyday and car bombs are
attacking us.
We managed to move funds belonging to Saddam
Hussein's family. The total amount  is US$ 8
Million dollars in cash. We want to move this
money to you,  so that you may keep our share for
us till when we will come over to meet you.
```

Copyright © Scott Bradner & Ben Gaucherin 2016



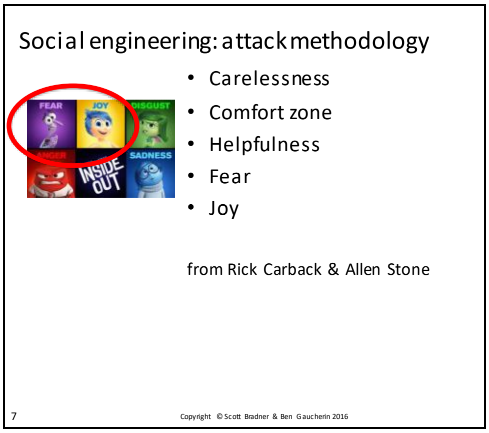
Social Engineering, e.g., contd.

```
We will take 60%, my partner and I.

You take 40%. No strings attached, just help us move it
out of Iraq, Iraq is a war zone. We plan on using
diplomatic courier and shipping the money out in three
large silver boxes, using diplomatic immunity.

If you are interested I will send you the full details,
my job is to find a good partner that we can trust and
that will assist us.
Can I trust you?

When you receive this letter, kindly send me an e-mail
signifying your interest including your most
confidential telephone/fax numbers  for quick
communication also your contact details.

This business is risk free. The boxes can be shipped out
in 48hrs.

Respectfully,
Sgt. Michael Parkas
```

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

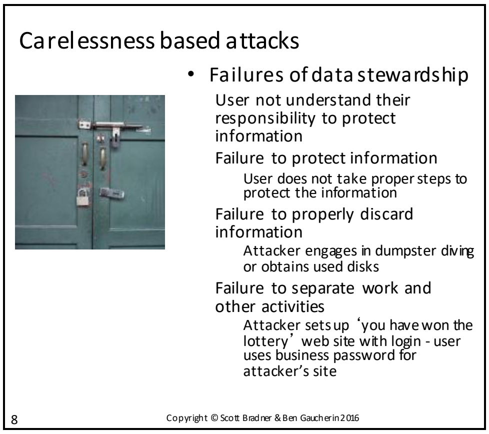

FEAR
JOY
DISGUST
ANGER
INSIDE OUT
SADNESS

Social engineering: attack methodology

- Carelessness
- Comfort zone
- Helpfulness
- Fear
- Joy

from Rick Carback & Allen Stone

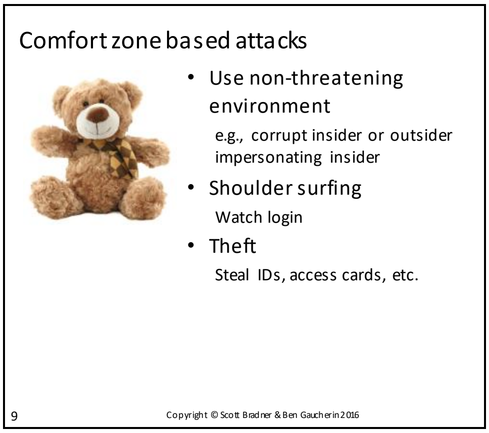
7 Copyright © Scott Bradner & Ben Gaucherin 2016



Carelessness based attacks

- Failures of data stewardship
  - User not understand their responsibility to protect information
  - Failure to protect information
    - User does not take proper steps to protect the information
  - Failure to properly discard information
    - Attacker engages in dumpster diving or obtains used disks
  - Failure to separate work and other activities
    - Attacker sets up 'you have won the lottery' web site with login - user uses business password for attacker's site

8 Copyright © Scott Bradner & Ben Gaucherin 2016



Comfort zone based attacks

- Use non-threatening environment
  - e.g., corrupt insider or outsider impersonating insider
- Shoulder surfing
  - Watch login
- Theft
  - Steal IDs, access cards, etc.

9 Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

Helpfulness based attacks

- People try to help - even strangers
  - Often attacker does not have to request help
  - Building access
    - Wait in outside smoking area and tailgate on reentry
    - Carry large box - someone will hold the door
    - Fumble for door key or badge
  - User seeking help
    - Ask for account password to be reset

Copyright © Scott Bradner & Ben Gaucherin 2016

Fear based attacks

- Put user in state of fear or anxiety
  - Conformity
    - Claim that the user is the only person who has not helped in the past
  - Time pressure
    - Invent a deadline to create urgency
  - Importance
    - Impersonate management to get password reset
    - Pull fire alarm and come dressed as a firefighter

Copyright © Scott Bradner & Ben Gaucherin 2016

Joy based attacks

- Put target off guard by making him/her happy
  - Mail to an office worker that says 'you have just won a trip to Las Vegas'
    - Instruct the reader to go to a web site and create an account for more details
      - Target too often uses office account name and password

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

Mitnick's List of Attacks

Copyright © Scott Bradner & Ben Gaucherin 2016

Some of Mitnick's List of Attacks

- Posing as fellow employee
- Posing as a new employee and requesting help
- Posing as an employee from a remote office and asking for local email access
- Posing as an authority figure (e.g., police)
- Posing as vendor employee
- Posing as a vendor offering security patch, etc.

Copyright © Scott Bradner & Ben Gaucherin 2016

Mitnick's List, contd.

- In advance offering help if a problem occurs
- Sending free software or security patch
- Use keystroke logger
- Leaving CD sitting around with malicious code
- Gain trust by using insider lingo
- Offering a prize for creating an account on a web site with username and password

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

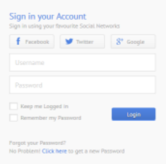
For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

Mitnick's List, contd.

- Dropping document or file at company mail room for "in-house" delivery
- Modifying fax machine heading to appear to come from a different location
- Asking receptionist to receive then forward a fax
- Asking for a file to be transferred to an apparently internal location

Copyright © Scott Bradner & Ben Gaucherin 2016

Mitnick's List, contd.



- Getting voice mailbox set up for callbacks, making attacker seem internal
- Sending email with a virus or Trojan horse
- Ask for log-in on a false pop-up window

Mitnick p 332

Copyright © Scott Bradner & Ben Gaucherin 2016

Mitnick's Warning Signs

- Caller:

  Refuses to give a callback number

  Makes an out of the ordinary request

  Makes claims of authority

  Stresses urgency

  Threatens negative consequences of noncompliance

  Shows discomfort when questioned

  Engages in name dropping

  Compliments or flatters

  Flirts

Mitnick p 333

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

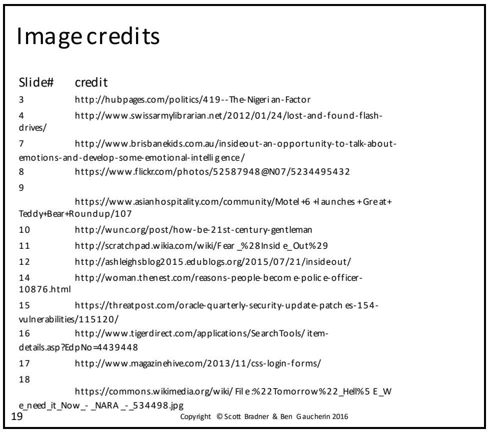


Image credits

Slide#	credit
3	http://hubpages.com/politics/419--The-Nigerian-Factor
4	http://www.swissarmylibrarian.net/2012/01/24/lost-and-found-flash-drives/
7	http://www.brisbanekids.com.au/insideout-an-opportunity-to-talk-about-emotions-and-develop-some-emotional-intelligence/
8	https://www.flickr.com/photos/52587948@N07/5234495432
9	https://www.asianhospitality.com/community/Motel+6+launches+Great+Teddy+Bear+Roundup/107
10	http://wunc.org/post/how-be-21st-century-gentleman
11	http://scratchpad.wikia.com/wiki/Fear_%28Inside_Out%29
12	http://ashleighsblog2015.edublogs.org/2015/07/21/insideout/
14	http://woman.thenest.com/reasons-people-become-police-officer-10876.html
15	https://threatpost.com/oracle-quarterly-security-update-patches-154-vulnerabilities/115120/
16	http://www.tigerdirect.com/applications/SearchTools/item-details.asp?EdpNo=4439448
17	http://www.magazinehive.com/2013/11/css-login-forms/
18	https://commons.wikimedia.org/wiki/File:%22Tomorrow%22_Hell%5E_We_need_it_Now_-_NARA_-_534498.jpg

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

Security threats II

Social engineering - prevention

CSCI E 45b: The Cyber World – part B

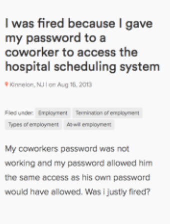
Copyright © Scott Bradner & Ben Gaucherin 2016

Protecting Against Social Engineering

- Multi level defense
  - Security policy, management support, risk analysis, and user education
- Some hard cases: ‘flirting robot’
  - “CyberLover”
  - Automated chat room software
  - Gets people to share important information
  - Software person is not a new idea - see ELIZA from 1966
    - http://en.wikipedia.org/wiki/ELIZA

Copyright © Scott Bradner & Ben Gaucherin 2016

Security Policy



I was fired because I gave my password to a coworker to access the hospital scheduling system

Kinnelon, NJ | on Aug 16, 2013

Filed under: Employment Termination of employment Types of employment At-will employment

My coworkers password was not working and my password allowed him the same access as his own password would have allowed. Was i justly fired?

- Clear rules on handling of confidential information
  - e.g., data destruction, portable devices, …
    - shredding, encryption, no important data on laptops, …
- Clear rules on password (non)sharing
  - e.g., passwords are never to be told to anyone - one warning then firing - undercover testing …

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

Security Policy, contd.

NO TAILGATING
Each person must present his/her Apple I.D. Badge to the card reader to confirm valid access.

- Clear rules on building access
  - No tailgating - all individuals must individually swipe IDs
- Needs to be clear enough to avoid need for employee to think about what to do

4

Copyright © Scott Bradner & Ben Gaucherin 2016

Management Support

- Requirement to support security plan must come from upper management
  - Not just security officer
- Upper management must be on-board from the start
  - Should be or look like a management initiated effort
- Line management must support security plan
  - e.g., must backup refusal to disclose passwords

5

Copyright © Scott Bradner & Ben Gaucherin 2016

Management Support

- Must not weaken security plan to save money
- Corporate audit should review compliance regularly

6

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

Risk Analysis

- Analyze areas of risk for social engineering and develop mitigations - e.g.,
  - Phone - train employees to recognize social engineering signs, different training based on access to information
  - Building - train guards, require picture IDs be worn, video monitors
  - Office - train employees to watch for people without IDs and shoulder surfers
  - Machine room - restrict access to a few well identified people, video monitors

Copyright © Scott Bradner & Ben Gaucherin 2016

User Education

- Basic defense against social engineering cannot be technical
  - since the attack is on people and not on equipment
- Must educate users to be suspicious
  - Training on hire & annually
  - Annual sign off/reminder to abide by security policy
- And on what to do if they suspect a social engineering attack

Copyright © Scott Bradner & Ben Gaucherin 2016

User Education, contd.

Incidental personal use is permitted so long as it does not interfere with job performance, consume significant time or resources, interfere with the activities of other employees or otherwise violate this policy, the rules of an employee's local unit, or other University policies.

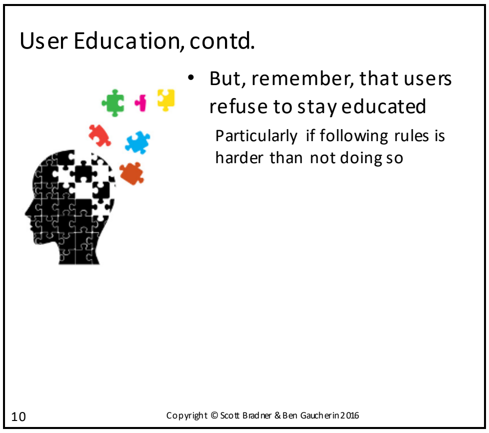
Harvard Personnel Manual

- Keep training message simple & consistent
  - But change slogans and training materials often
- Be clear about OK level of personal use of corporate resources
- Must have reporting mechanisms in place and well known
  - And monitored!

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.



User Education, contd.

- But, remember, that users refuse to stay educated

  Particularly if following rules is harder than not doing so

10

Copyright © Scott Bradner & Ben Gaucherin 2016

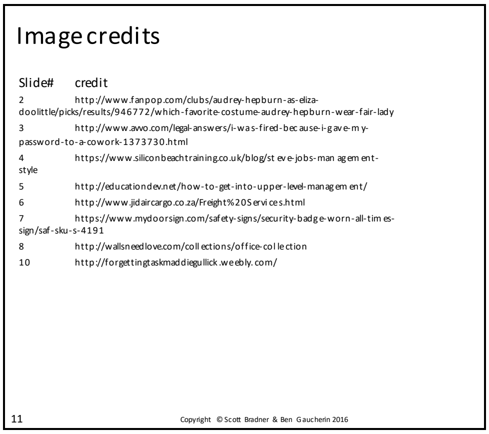


Image credits

Slide#	credit
2	http://www.fanpop.com/clubs/audrey-hepburn-as-eliza-doolittle/picks/results/946772/which-favorite-costume-audrey-hepburn-wear-fair-lady
3	http://www.avvo.com/legal-answers/i-was-fired-because-i-gave-my-password-to-a-cowork-1373730.html
4	https://www.siliconbeachtraining.co.uk/blog/steve-jobs-management-style
5	http://educationdev.net/how-to-get-into-upper-level-management/
6	http://www.jidaircargo.co.za/Freight%20Services.html
7	https://www.mydoorsign.com/safety-signs/security-badge-worn-all-times-sign/saf-sku-s-4191
8	http://wallsneedlove.com/collections/office-collection
10	http://forgettingtaskmaddiegullick.weebly.com/

11

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

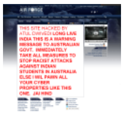
Security threats II

Conclusion

CSCI E 45b: The Cyber World – part B

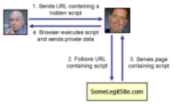
Copyright © Scott Bradner & Ben Gaucherin 2016

Websites are often vulnerable



THIS SITE HACKED BY ATUL DWIVEDI LONG LIVE INDIA THIS IS A WARNING MESSAGE TO AUSTRALIAN GOVT. IMMEDIATELY TAKE ALL MEASURES TO STOP RACIST ATTACKS AGAINST INDIAN STUDENTS IN AUSTRALIA ELSE I WIL PAWN ALL YOUR CYBER PROPERTIES LIKE THIS ONE. JAI HIND

- Multiple attack vectors
- Attack website itself
  - Defacement
    - Attacks on reputation
    - Get publicity for a cause
- Attack underlying information on this or another website
  - Get or modify back end data
    - SQL injection
    - Cross-site scripting
    - Cross-site reference forgery



1. Sends URL containing a hidden script
4. Browser executes script and sends private data
2. Follows URL containing script
3. Serves page containing script
SomeLegitSite.com

Copyright © Scott Bradner & Ben Gaucherin 2016

Social engineering

- Trick people to do something they should not
  - Provide personal information
  - Provide access information
  - Open doors
- Some users make it easy by not internalizing their own responsibility to protect company information
- Believable communications attacks are an old concept
  - Email makes them easier – a.k.a., phishing

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

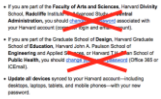
For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

Social engineering, Phishing

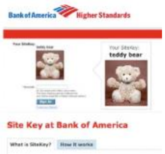
- Send email that tricks recipient into installing spyware or into revealing information
- Spyware can capture keystrokes including login or encryption credentials
- User often directed to a temporary web site that looks like a legit site but captures information

Copyright © Scott Bradner & Ben Gaucherin 2016

Social engineering protection



- If you are part of the **Faculty of Arts and Sciences**, Harvard **Divinity** School, **Radcliffe** Institute ~~for Advanced Study, or~~ **Central Administration**, you should ~~change your password~~ associated with your Harvard account (~~computer login and email~~ account).
- If you are part of the Graduate School of **Design**, Harvard Graduate School of **Education**, Harvard John A. Paulson School of **Engineering** and Applied ~~Sciences, or Harvard T.H. Chan~~ School of **Public Health**, you should ~~change your password~~ (Office 365 or ICEmail).
- **Update all devices** synced to your Harvard account—including desktops, laptops, tablets, and mobile phones—with your new password.



Site Key at Bank of America

- Social engineering is hard to protect against
- Never click on a link in an unexpected email
- People do not understand what a legitimate company would ask for
- People do not pay attention to details

Copyright © Scott Bradner & Ben Gaucherin 2016

Social engineering protection, contd.

- Basic defense against social engineering cannot be technical
  - since the attack is on people and not on equipment
- Must educate users to be suspicious
  - Training on hire & annually
  - Annual sign off/reminder to abide by security policy
- And on what to do if they suspect a social engineering attack

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.

For use by students in Harvard Extension School CSCI E-45b only. Do not copy.

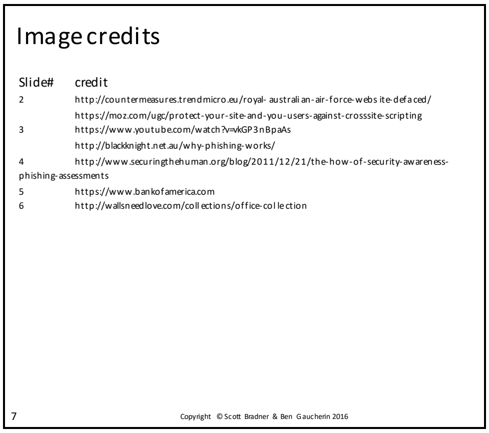


Image credits

Slide#	credit
2	http://countermeasures.trendmicro.eu/royal- australian-air-force-website-defaced/
	https://moz.com/ugc/protect-your-site-and-you-users-against-crosssite-scripting
3	https://www.youtube.com/watch?v=vkGP3nBpaAs
	http://blackknight.net.au/why-phishing-works/
4	http://www.securingthehuman.org/blog/2011/12/21/the-how-of-security-awareness-phishing-assessments
5	https://www.bankofamerica.com
6	http://wallsneedlove.com/collections/office-collection

Copyright © Scott Bradner & Ben Gaucherin 2016

© 2016 Scott Bradner & Ben Gaucherin. All rights reserved.