INFO 310

Fall 2016

Week 11 – Lecture 2

HOUSEKEEPING

- Attendance
- Course Evaluation:

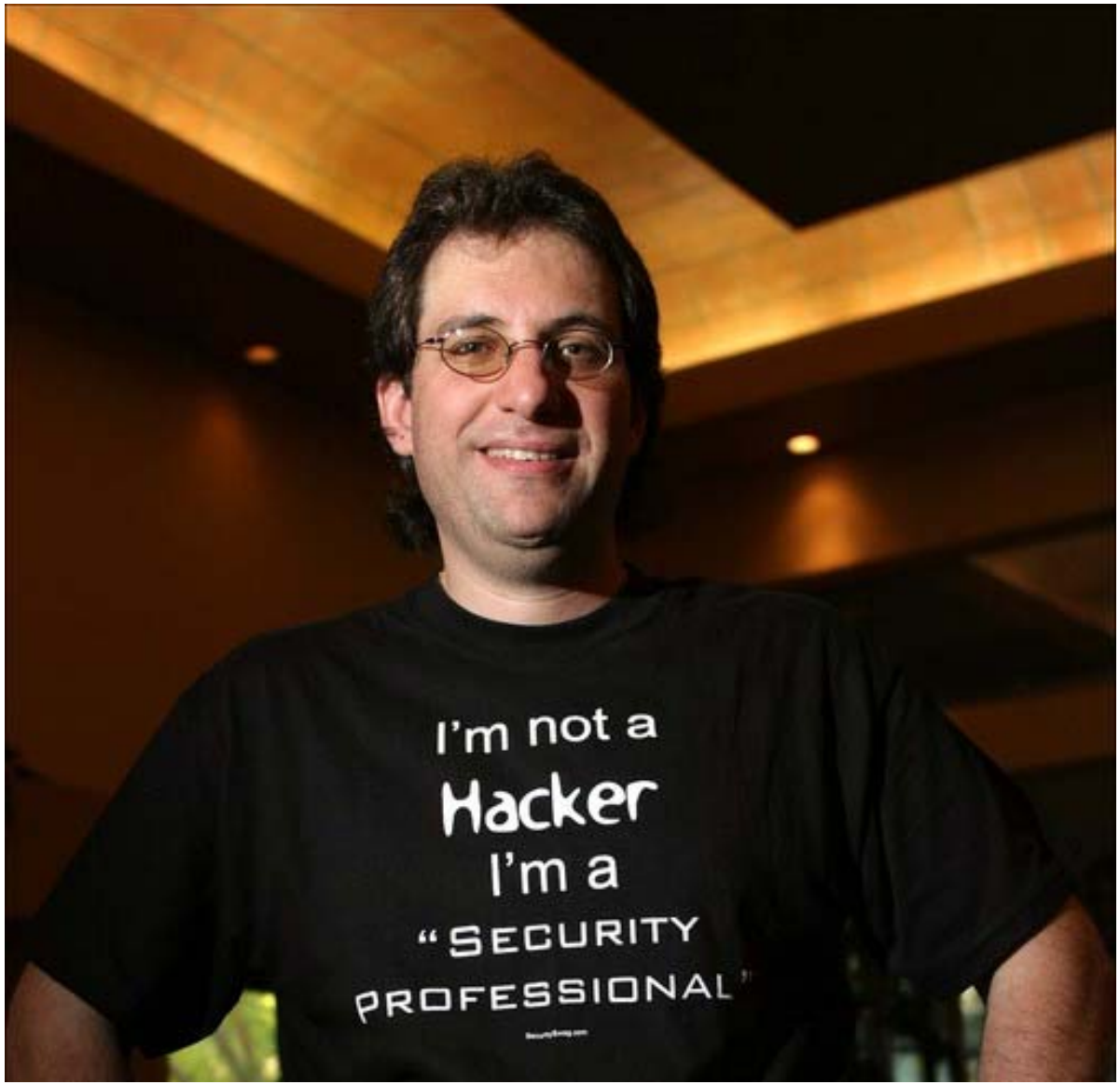
https://uw.iasystem.org/survey/168389

Social Engineering

In the context of information security, social engineering refers to psychological manipulation of people into performing actions or divulging confidential information.

A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

The term "social engineering" as an act of psychological manipulation is also associated with the social sciences, but its usage has caught on among computer and information security professionals


I'm not a
Hacker
I'm a
"SECURITY
PROFESSIONAL"

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: .....MITNICK, KEVIN DAVID

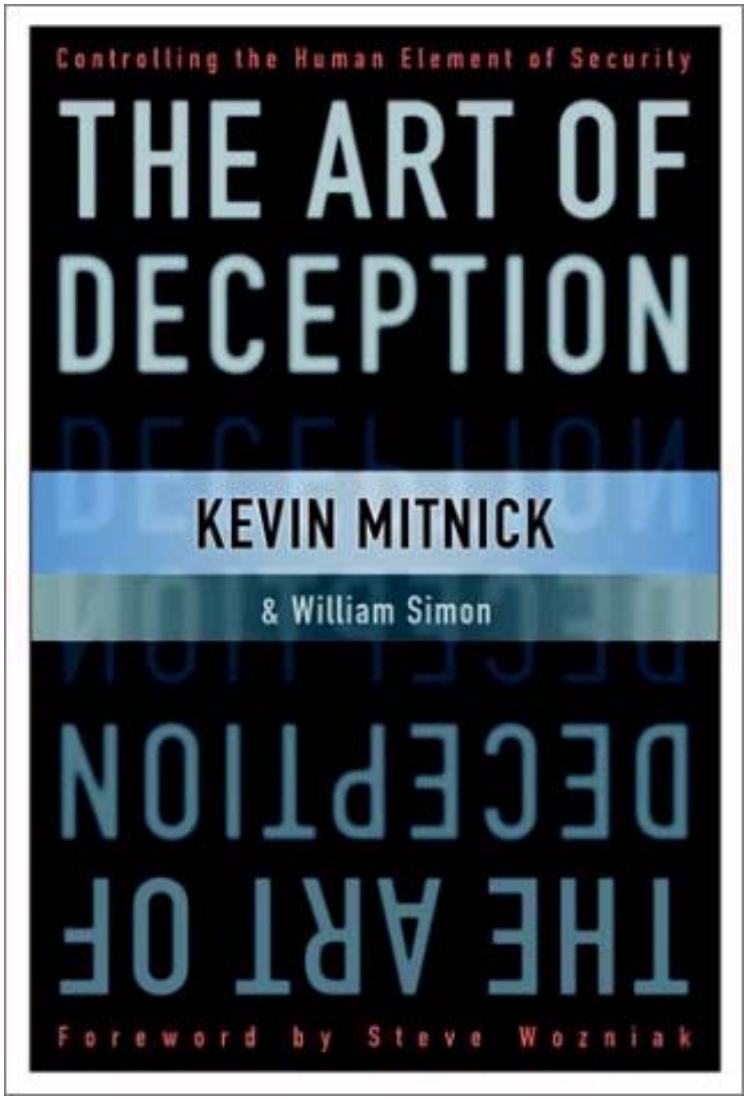
AKS (S): .....MITNIK, KEVIN DAVID
MORRILL, BRIAN ALLEN

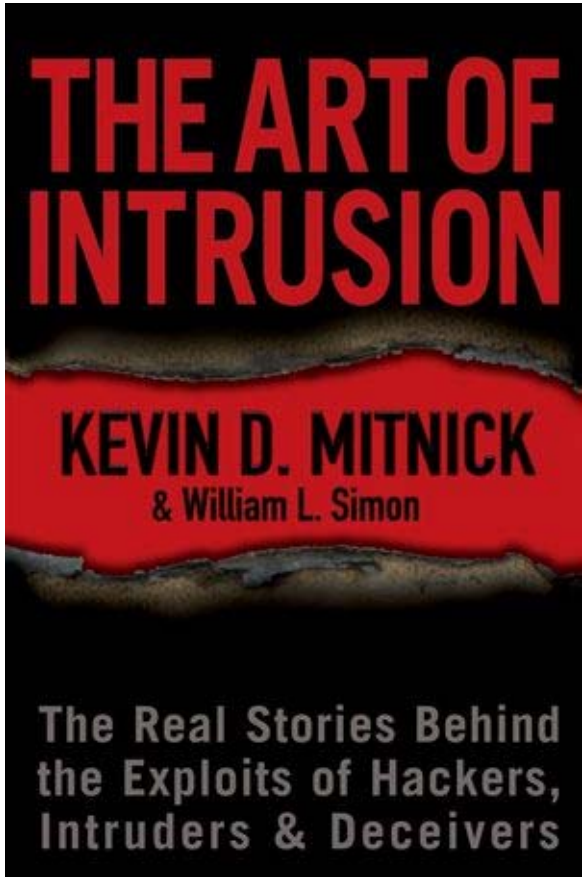
DESCRIPTION:

Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13I13PM19PM09

Kevin Mitnick

He wrote the book on it (literally)





Some useful tools

Tactics, Techniques and Procedures (TTPs)

- Pretexting
- Tailgating
- Baiting
- Quid Pro Quo
- Phishing
  - Spear Phishing
  - Whaling
  - Catphishing

From: IT Service Help Desk <allenvioletlarge47@gmail.com>
Date: October 29, 2015 at 12:04:19 PM PDT
To: undisclosed-recipients:;
Subject: [IT Services] UW NetID Security Modifications - Effective Immediately

IT Services Help Desk

Thursday, October 29, 2015

Dear UW NetID Account User,

Your mailbox has been compromised because you have accessed a sensitive information on our data base, please you are requested to kindly authenticate your **UW NetID** account by reconfirming your identity and eligibility below to help help protect your account and make sure no one is using your information without your knowledge.

UW NetID

Due to some confidential data that was encrypted for your security purpose on our database, this email server is duly required to click on the **"UW NetID"** above, to view the webpage by reconfirm your identity in person and the digital certificate that uses SSL (Secure Sockets Layer) technology to encrypt your data and information for your safety use in order to ensure that it remain private and confidential to you solely.

IT Service Help Desk

Grim, Jason A. Assignee Group Help Desk
© 2015 University of Washington | Seattle, WA
helpdesksecurity@uw.edu

IT Note: please do not reply to this message this is an automated message, and replies are not monitored.

Sun 12/6/2015 11:20 AM

[redacted] <[redacted]@uw.edu>

Mailbox Update

To

Dear Staff,

You are required to verify your details to resolve access issues and irregularities which we have noticed with your webmail account.

Click Here to Verify Now

Failure to do so within 24 hours may lead to temporary account deactivation. Thank you for your understanding and cooperation.

Warning Code: UW2903312

---------- Forwarded message ----------
Date: Mon, 9 Nov 2015 22:02:49 +0530
From: Admin Support@s.uw.edu
Reply-To: noreply@noreply.com
To: Recipients@s.uw.edu
Subject: Your mailbox has been temporally suspended

Dear User

We recently detected an unusual activity from your email account, hence your mailbox has been temporally suspended by the system administrator, please recover your account by clicking on the following link OR copy to your browser:
http://systemuqdatepanelpad1738.razuka.net/BE3/ITupdate_10_28_2015_en_US.ISO88591WebMailSupport.htm

As a result to this, you might receive this message in your spam folder, kindly move it to your inbox and click the link.

We apologize for the inconvenience.
Administrator.

Dear Webmail user,

On behalf of the Webmail team, we regret to announce the shutdown of our email service. The database virus detective has detected DFXG Virus on large number of email account: This virus was spread as a result of the anonymous spam email and spyware sent to some users email account, unknowingly to them. This breakdown is affecting our hosting service. The remedy to this situation is to deactivate the service of INACTIVE ACCOUNTs and scan all email.

USERS (Account Owner) are required verify the continuous use of their email (Email you receiving this message). Kindly click here or copy the Validation link below to your browser and logon to your account for confirmation and avoid suspension/shutdown of your email service at any time.

On the click of Login, you will be redirect to a Verified Successfully Page. Please when you reach this page, do not try to submit another request, multiple request and invalid information, will lead to deactivation of your email account, take serious note of this.

Validation Link: http://webadminportalbase.com/portal/

DO NOT ignore this message if you wish to save your account and also do not send your Password to any one via email; Webmail Admin will NEVER ask you to send your password via email...

Thanks for your understanding and Co-operation.

System Management Team,

From: UW Information Technology Service Center <help@uw.edu <mailto:help@uw.edu> >

Subject: ALERT: Your UW Email will be shut off unless you act!

Date: November 25, 2014 at 5:58:57 PM PST

To: [redacted]@u.washington.edu <mailto:[redacted]@u.washington.edu>

You have exceeded your allotted email storage space quota for the UW
Email service. Unless you act soon, all incoming email will be returned
to sender, and you may not be able to send email.

Is there a grace period?

Yes. You have 14 days from the time this message was sent to you. However,
if at any time you exceed your quota by 512 MB or more, your receipt of
new incoming email is stopped immediately.

How to solve the problem in three steps
---
1. View what's taking up your email storage space using the disk storage tool at:

http://uwnetid.washington.edu/disk/

[For tips, click "Managing Your Storage Space" in the top right.]

2. Delete or move unneeded email folders and messages, using your preferred email software,
then EXIT the email program(s) and any Smart Phone so that your continued activity doesn't
prevent true elimination of the deleted messages. Web Alpine users should be sure to exit
using the "Sign Out" icon at the upper right; closing the Web browser may not close Web Alpine.

3. Click "Update Now" in the viewer (Step 1) to see how much space you've freed up.

Repeat steps 2 and 3 above until you are under quota.

Can't get under quota?

If you can't delete enough email to get under quota, use the link on the disk storage
page (1.) to adjust or purchase storage space. If problems persist contact UW Information
Technology for help:

- Reply to this message, or send email to help@uw.edu, or
- Call the UW Technology Service Center at 206-221-5000 during
business hours: 8am - 8pm Monday - Friday; Sunday 1pm - 8pm.

Thank you.
UW Information Technology Service Center
help@uw.edu
206-221-5000

-----Original Message-----
From: UW Information Technology Service Center [mailto:help@uw.edu]
Sent: Thursday, November 05, 2015 7:44 AM
To: [redacted]@u.washington.edu
Subject: YOUR UW EMAIL IS SHUT OFF: Act now!

Your UW Email has been shut off because you did not reduce your UW Email storage space within the 14 days grace period. You can't recover lost messages, but you can get your email working again.

How to solve the problem in three steps
---
1. View what's taking up most of your space using the storage space tool at:

http://uwnetid.washington.edu/disk/

[For tips, click "Managing Your Storage Space" in the top right.]

2. Delete or move unneeded email folders and messages, using your preferred email software, then exit the email program(s) and Smart phones so that your continued activity does not prevent true elimination of the deleted messages. Web Alpine users should be sure to exit using the "Sign Out" Icon at the upper right of the screen; closing the browser may not exit Web Alpine.

3. Click "Update Now" in the storage space tool (Step 1) to see how much space you've freed up.

Repeat steps 2 and 3 above until you are under quota.

Can't get under quota?

If you can not delete enough email to get under quota, use the link on the storage space tool to adjust or purchase storage space. If problems persist contact UW Information Technology for help.

o reply to this message, or send email to help@uw.edu, or o call the UW Information Technology Service Center at 206-221-5000 8am - 8pm Monday-Friday; Sunday 1pm - 8pm.

Thank you!
UW Information Technology Service Center help@uw.edu
206-221-5000

Other considerations

- Reconnaissance
- Supply Chain Injects
- Online Banking
- DNS Poisoning
- Global Routing manipulation
- …

Watch at home:

https://www.youtube.com/watch?v=HN9p4r-l3io

(break)

The Internet is out to get you…

- Companies are not your friend. You are more commodity than customer.
- Mining your data is big business
  - Not just for advertisers
  - Your bank may buy your behavioral profile
  - So does your insurance company
- Digital Profiles are opaque at best
- Free != Free
  - ‘nuff said
- Could you get away from it if you tried?

Specific technologies examined

- Browser Fingerprinting
  - User Agent Strings
- Location Tracking
  - Now also on laptops & desktops
- Automated Facial Recognition
  - Scary good!
- Voice Printing
  - Hey Siri, Hey Google
- Behavioral analysis – eg. keystrokes
- RFID tracking
- The Cloud
  - Aggregation of Risk
  - Virtualization
  - Trusting the hypervisor (don’t)

The Internet of Things

- Everything seems to talk TCP/IP nowadays
  - Clothes Dryers
  - Fridges
  - Kid's digital cameras
  - Deadbolts
  - Home alarm systems
- You lock your door, but you let the world into your house virtually?
  - Thermostats
  - Smoke Alarms
  - Surveillance Cameras
  - Other "Cloud managed" devices

What can you do?

- 1st question: Do you WANT to do anything?
- Security vs. Convenience
- Pulling up your low-hanging fruit
  - Limit location tracking
  - Use more cash
  - Use “burner” email accounts
  - Use privacy tools while browsing
  - TOR
  - …

(this page intentionally left blank)

Final Exam – “Study Guide”

- Computer Forensics: Definitions & Goals
- Reasons for conducting forensics
- Device examples
- Ability to discuss chain of custody, evidence integrity, and report writing
- Evidence acquisition & software tools
- Data storage on spinning disk media
- Data recovery – what’s possible?
- Tips for protecting your privacy in the context of forensics and data recovery

Final Exam – “Study Guide” cont’d

- Mobile Device Security
  - Ability to discuss device lifecycle compared to availability of OS updates
  - The App Store ecosystem
  - Potential privacy issues around location services
  - App permission pitfalls
  - International travel with smartphones – concerns, risks

Final Exam – “Study Guide” cont’d

- Web Application Security – Definition
- Ability to name the vulnerabilities that made the news (and explain how HeartBleed “works)
- Ability to discuss, explain, and recommend counter measures for
  - SQLi
  - XSS
  - CSRF
  - Remote File Includes
  - Direct Object References

Final Exam – “Study Guide” cont’d

- Ability to discuss UNIX file permissions
  - Read & interpret examples
- .htaccess basics
- Ability to discuss Company Datamining of users
- Techniques / technologies involved in user tracking
- The Internet of Things – Definition, implications
- Ability to explain and recommend personal protection measures

Final Exam – “Study Guide” cont’d

- Social Engineering – Definition
- Tactics, Techniques, and Procedures (TTPs)
- Ability to design and describe a potential scenario involving different social engineering tactics to obtain specific information.
- Basic knowledge of Red-Team / Blue-Team exercises.

Final Exam – “Study Guide” cont’d

- DNS
  - Definition, what does it do?
  - Common resource records and their purposes
  - DNS Administration – Governing Bodies
  - Components
  - Root servers, root zone, purpose
  - Different types of DNS servers
- Firewall – definition, purpose
- IDS & IPS definition, purpose, difference.

Final Exam – “Study Guide” cont’d

- Define Computer Virus, Trojan Horse, Worm and their specific differences
- Define malware, including examples (both types and names)
- Describe malware delivery mechanisms
- Describe AV software, and, at a (very) high level, how it works

Final Exam – “Study Guide” cont’d

- Define Bot & Botnet
- Describe Botnet components & lifecycle
- Describe different types of botnets
- Describe what botnets are used for
- Describe methods for detecting botnet activity
- Use of ping, traceroute, dig,
- Knowledge of the purpose / capabilities of nmap, wirershark

Final Exam – “Study Guide” cont’d

- Citizenfour (2014) – Documentary
  - Who are the main characters, what are their roles?
  - What are Ed Snowden’s main claims?
  - What was Ed Snowden accused of by the US Government?