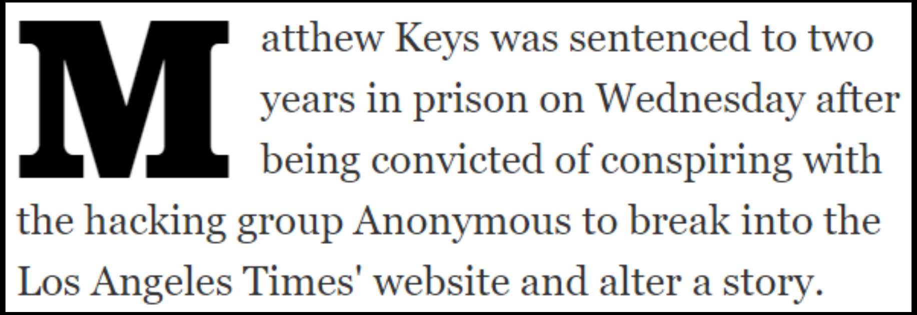
cyber@ucr:~$

Who Are We?

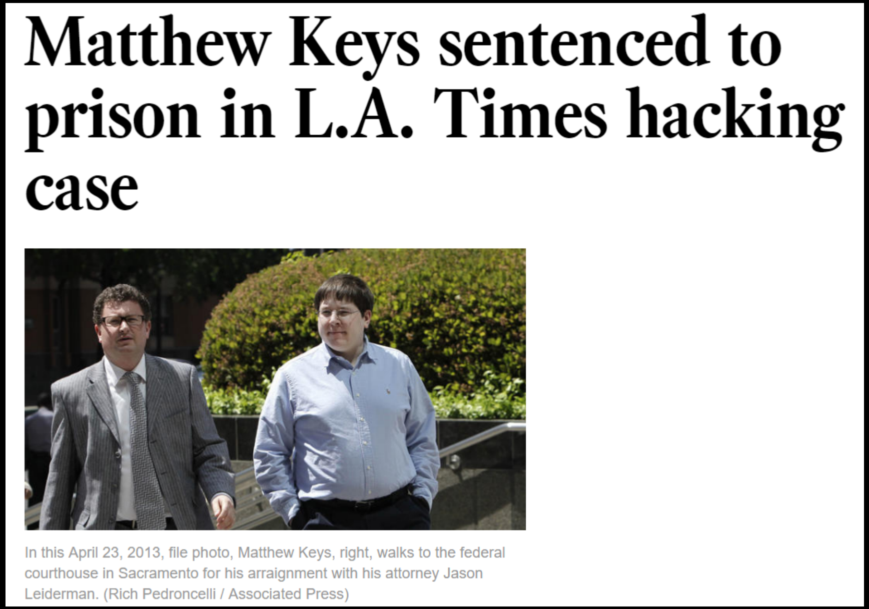
- Hackers (but in the "good way")
  - Study information security by understanding "defense in depth"
  - Study attack methods
  - Develop countermeasures and mitigate
- Adversarial training
  - Represent UCR in cybersecurity competitions: WRCCDC, National Cyber League, UCSB iCTF, other CTF competitions.
- Self study, teach each other
  - Many of us have "specialties": Windows systems, Linux systems, appliances (firewalls, routers, switches), reverse engineering, penetration testing, etc.

Cybersecurity is a Dangerous Game

- There are not a lot of “legal contexts” to practice information security (especially attack methodologies).
- Competitions provide a safe space to develop skills.
  - (You’re likely going to be terrible at this at first.)
- **Strict adherence to professional ethics.**
- Do not try this at home.
  - There are lots of “pranksters” in jail.



Matthew Keys was sentenced to two years in prison on Wednesday after being convicted of conspiring with the hacking group Anonymous to break into the Los Angeles Times' website and alter a story.



Matthew Keys sentenced to prison in L.A. Times hacking case

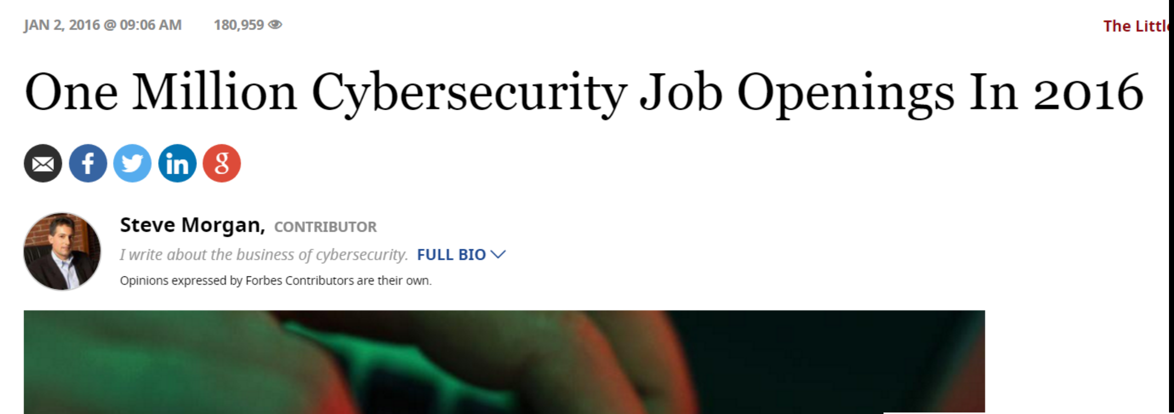
In this April 23, 2013, file photo, Matthew Keys, right, walks to the federal courthouse in Sacramento for his arraignment with his attorney Jason Leiderman. (Rich Pedroncelli / Associated Press)

Cybersecurity is a Hot Topic

There is a cybersecurity jobs shortage.

You **do not need** to be a computer scientist, engineer, or physicist to get into cyber.

Many do so with some certifications:
Cisco certifications, CISSP, CompTIA certifications, etc.



JAN 2, 2016 @ 09:06 AM 180,959

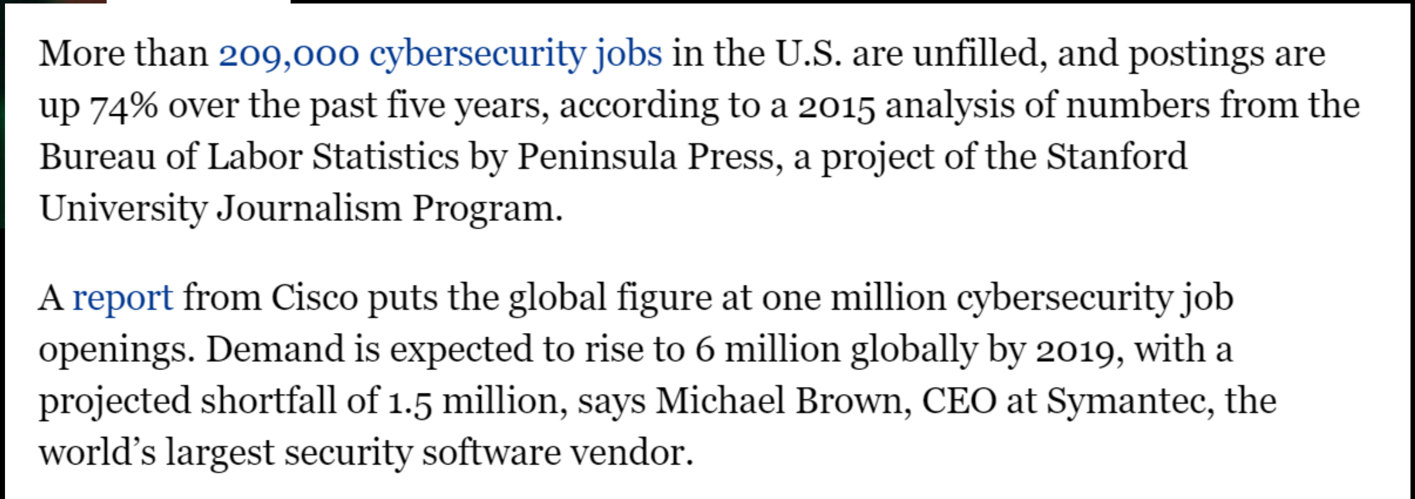
The Littl

One Million Cybersecurity Job Openings In 2016

Steve Morgan, CONTRIBUTOR

I write about the business of cybersecurity. FULL BIO

Opinions expressed by Forbes Contributors are their own.



More than 209,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74% over the past five years, according to a 2015 analysis of numbers from the Bureau of Labor Statistics by Peninsula Press, a project of the Stanford University Journalism Program.

A report from Cisco puts the global figure at one million cybersecurity job openings. Demand is expected to rise to 6 million globally by 2019, with a projected shortfall of 1.5 million, says Michael Brown, CEO at Symantec, the world's largest security software vendor.

How do I learn "hacking?"

You Google it. (This sounds like a joke, but it's true.)

Cybersecurity is a Hot Topic

HACKERS

Inside the hacker underworld of ISIS

s Angeles college

Democratic House Candidates Were s

Hacker activated all Dallas emergency sirens with a radio signal

by Jacob Kastrenakes | Apr 12, 2017, 5:34pm EDT

Hillary Clinton's Campaign Turns Email List To DN

Huffington Post · 2 d

cyberattack

ents uncovered by Russian

e

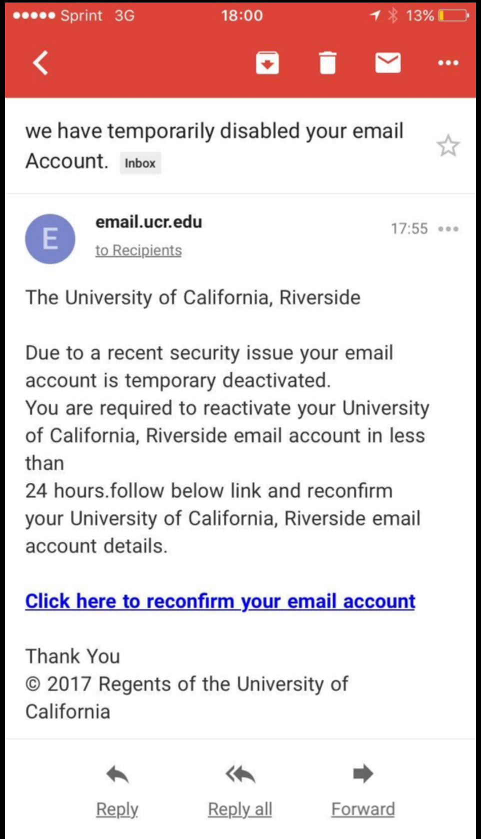
e fundamentally unsafe. No

Types of Threats

- Two principle attack types that concern you.
- **Social attacks (Social engineering)**
  - Phishing
  - Vishing
  - Hacking **you**, the user.
- **Technical attacks**
  - **Most often victim-initiated**
    - Using pirated software, out of date browsers, opening email attachments, etc.
    - Some “malware” (**mal**icious soft**ware**) may attempt to route your connection through a third party proxy server, allowing an attacker to capture your web traffic.
  - Sometimes caused by misconfiguration
    - Failing to update software (note: pirated software is rarely updated)
    - Bad settings at the network level
      - This is your sysadmin’s problem.
  - Exploits targeting insecure WiFi access points, lack of encryption.

Social Engineering

- Phishing and Vishing



we have temporarily disabled your email Account.

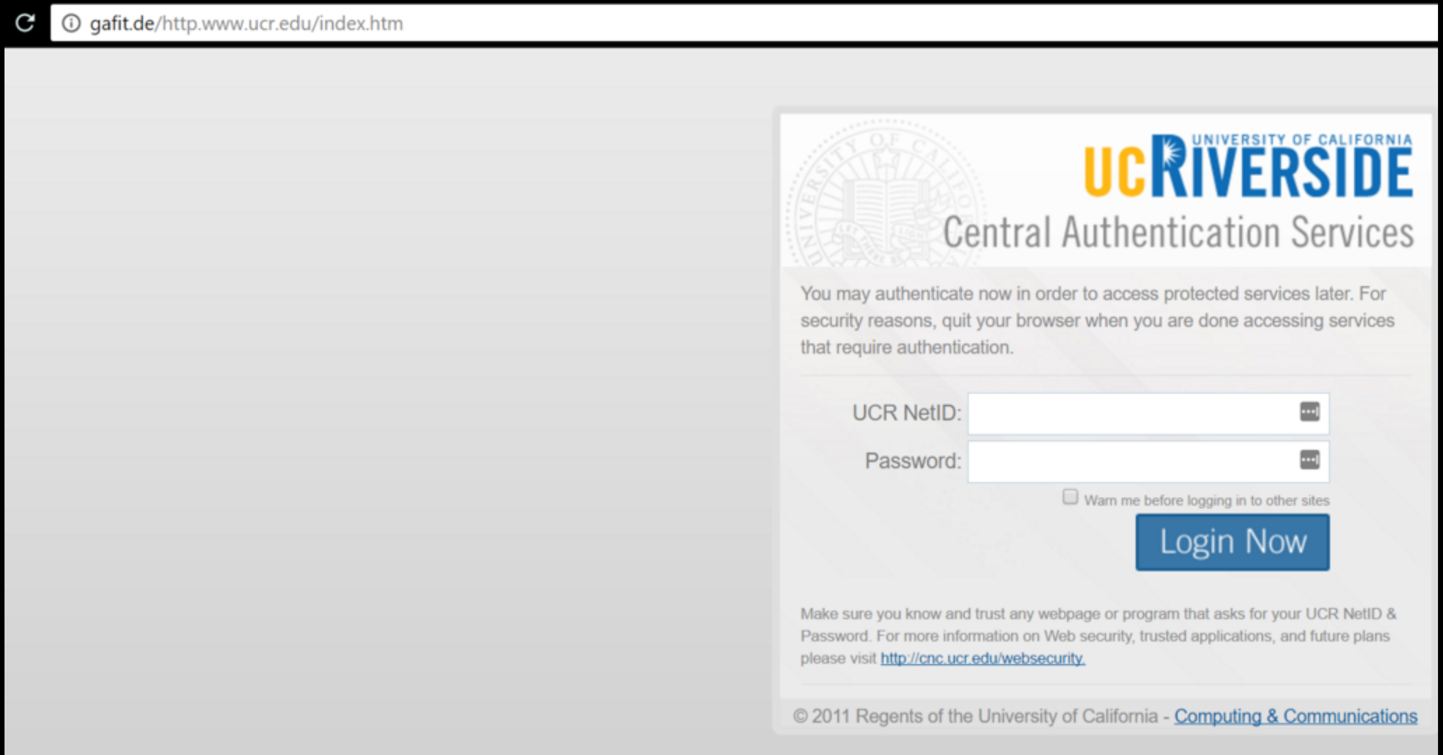
email.ucr.edu 17:55
to Recipients

The University of California, Riverside

Due to a recent security issue your email account is temporary deactivated.
You are required to reactivate your University of California, Riverside email account in less than
24 hours.follow below link and reconfirm your University of California, Riverside email account details.

Click here to reconfirm your email account

Thank You
© 2017 Regents of the University of California



gafit.de/http.www.ucr.edu/index.htm

Central Authentication Services

You may authenticate now in order to access protected services later. For security reasons, quit your browser when you are done accessing services that require authentication.

UCR NetID:

Password:

□ Warn me before logging in to other sites

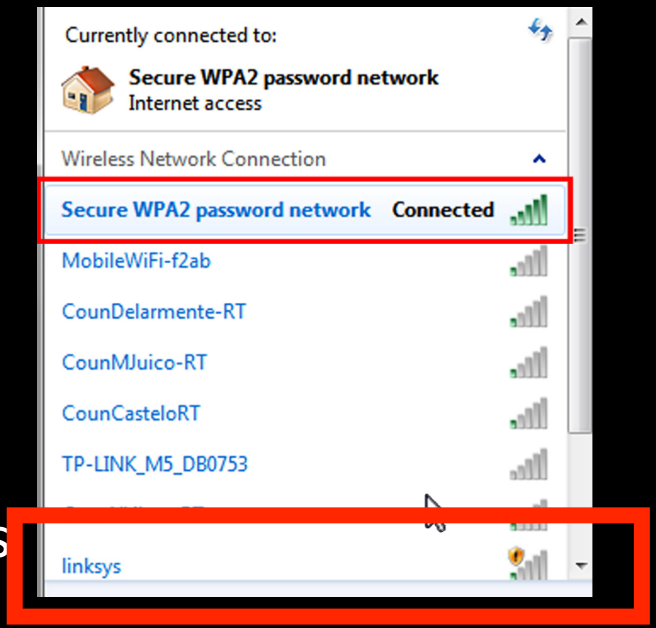
Login Now

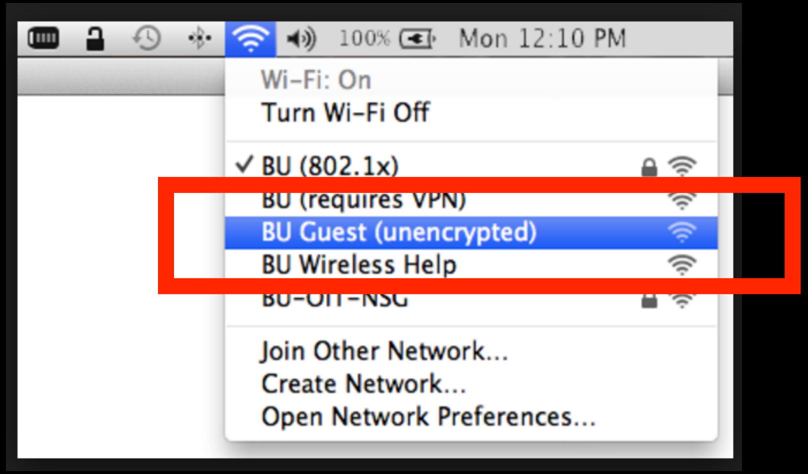
Make sure you know and trust any webpage or program that asks for your UCR NetID & Password. For more information on Web security, trusted applications, and future plans please visit http://cnc.ucr.edu/websecurity.

© 2011 Regents of the University of California - Computing & Communications

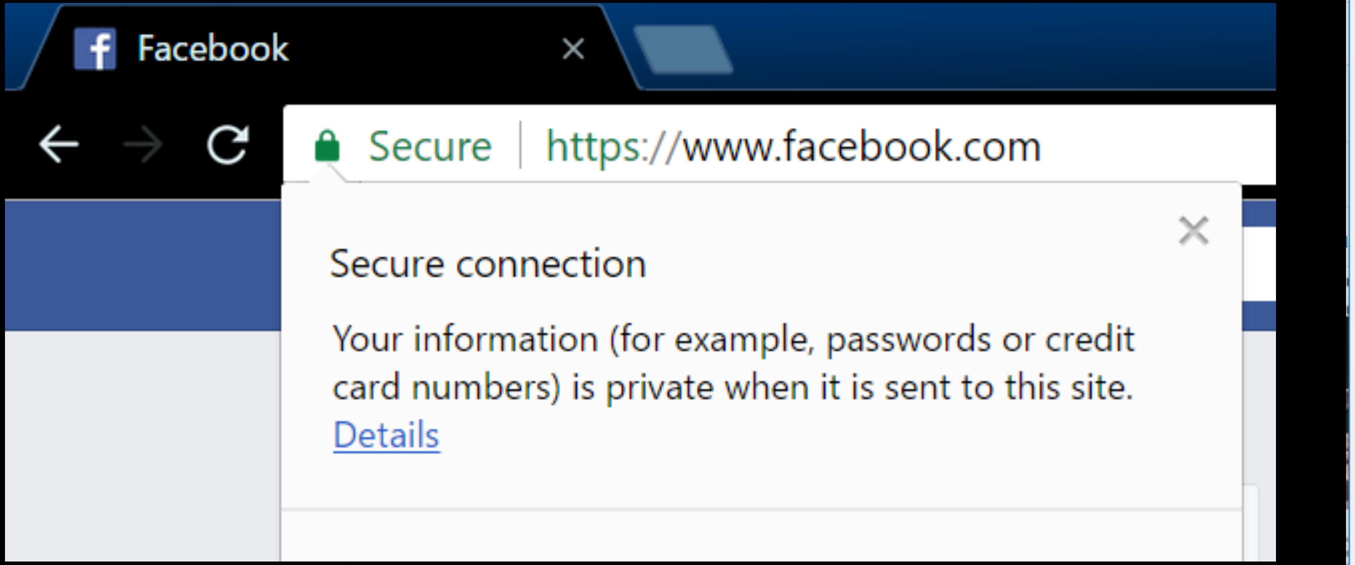
Technical attacks

- Technical attacks are usually victim initiated!
  - You are tricked into downloading malicious software.
  - You used pirated software or files that contain malicious software as a component.
- Be careful using public WiFi
  - Some access points are **unencrypted.**
  - Evil Twin attacks
- Use only trusted, encrypted connections for your most private transactions.
  - Banking, etc.





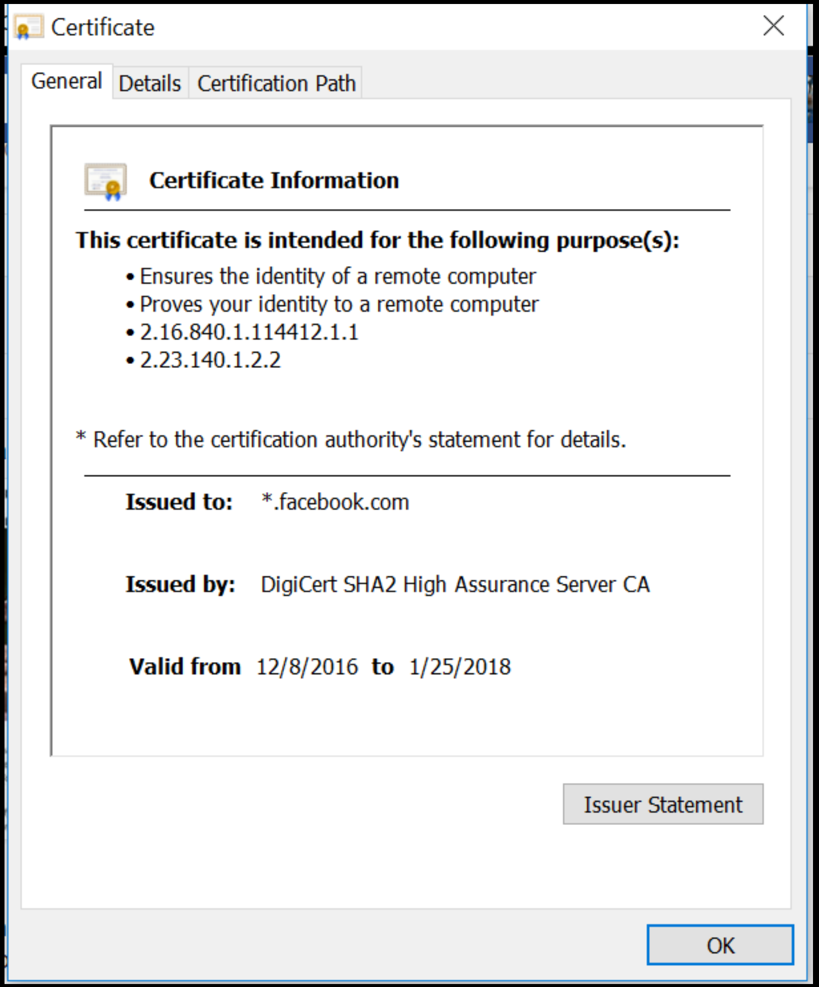
Technical attacks



Secure https://www.facebook.com

Secure connection

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Details



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 2.16.840.1.114412.1.1
- 2.23.140.1.2.2

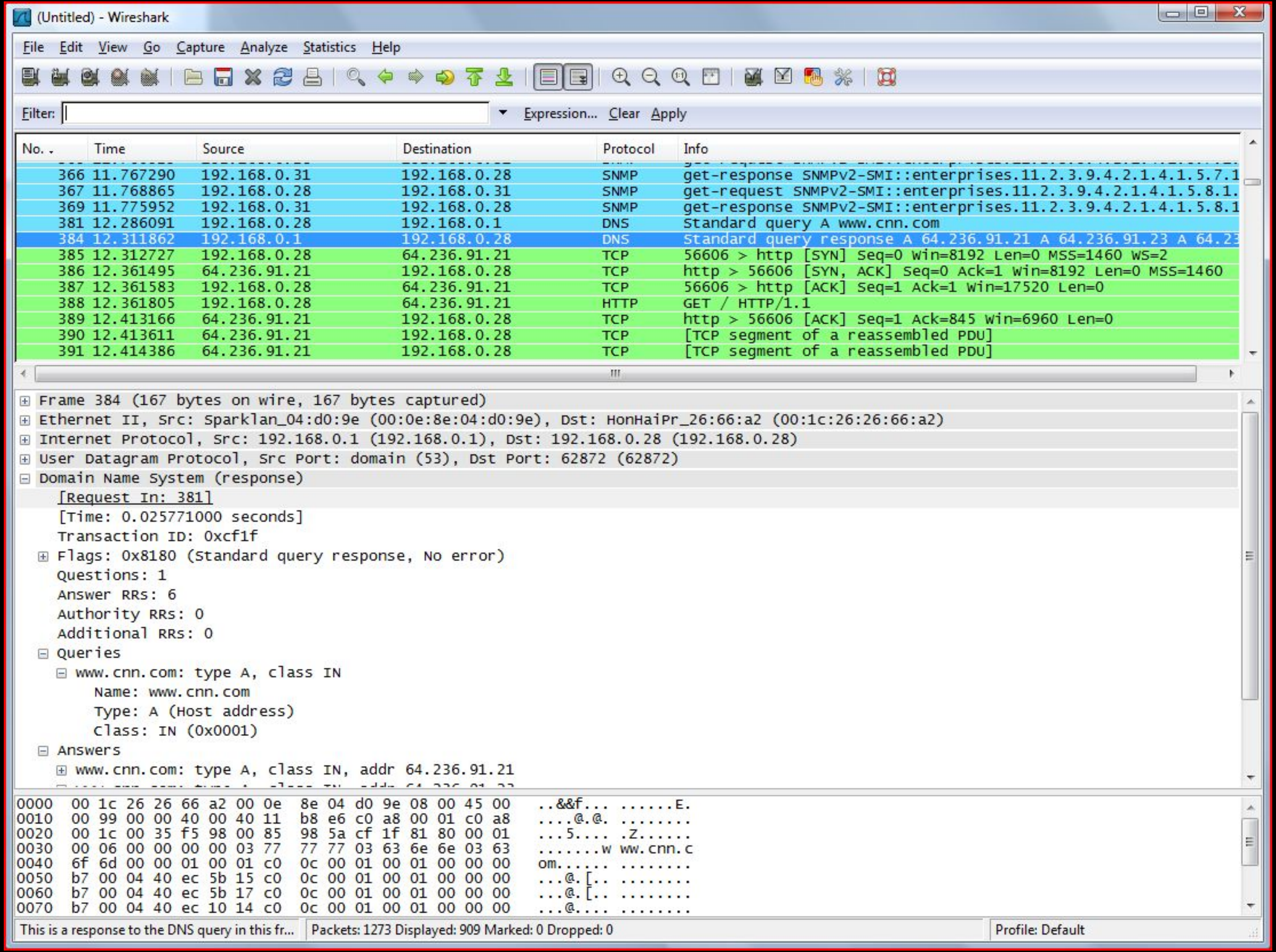
* Refer to the certification authority's statement for details.

Issued to: *.facebook.com

Issued by: DigiCert SHA2 High Assurance Server CA

Valid from 12/8/2016 **to** 1/25/2018

Technical attacks


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. .  Time       Source          Destination     Protocol  Info
  366 11.767290  192.168.0.31    192.168.0.28    SNMP      get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.7.1
  367 11.768865  192.168.0.28    192.168.0.31    SNMP      get-request SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1.
  369 11.775952  192.168.0.31    192.168.0.28    SNMP      get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1
  381 12.286091  192.168.0.28    192.168.0.1     DNS       Standard query A www.cnn.com
  384 12.311862  192.168.0.1     192.168.0.28    DNS       Standard query response A 64.236.91.21 A 64.236.91.23 A 64.23
  385 12.312727  192.168.0.28    64.236.91.21    TCP       56606 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
  386 12.361495  64.236.91.21    192.168.0.28    TCP       http > 56606 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
  387 12.361583  192.168.0.28    64.236.91.21    TCP       56606 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
  388 12.361805  192.168.0.28    64.236.91.21    HTTP      GET / HTTP/1.1
  389 12.413166  64.236.91.21    192.168.0.28    TCP       http > 56606 [ACK] Seq=1 Ack=845 Win=6960 Len=0
  390 12.413611  64.236.91.21    192.168.0.28    TCP       [TCP segment of a reassembled PDU]
  391 12.414386  64.236.91.21    192.168.0.28    TCP       [TCP segment of a reassembled PDU]
```

```
⊞ Frame 384 (167 bytes on wire, 167 bytes captured)
⊞ Ethernet II, Src: Sparklan_04:d0:9e (00:0e:8e:04:d0:9e), Dst: HonHaiPr_26:66:a2 (00:1c:26:26:66:a2)
⊞ Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.28 (192.168.0.28)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 62872 (62872)
⊟ Domain Name System (response)
    [Request In: 381]
    [Time: 0.025771000 seconds]
    Transaction ID: 0xcf1f
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 6
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.cnn.com: type A, class IN
        Name: www.cnn.com
        Type: A (Host address)
        Class: IN (0x0001)
  ⊟ Answers
    ⊞ www.cnn.com: type A, class IN, addr 64.236.91.21
```

```
0000  00 1c 26 26 66 a2 00 0e  8e 04 d0 9e 08 00 45 00   ..&&f... ......E.
0010  00 99 00 00 40 00 40 11  b8 e6 c0 a8 00 01 c0 a8   ....@.@. ........
0020  00 1c 00 35 f5 98 00 85  98 5a cf 1f 81 80 00 01   ...5.... .Z......
0030  00 06 00 00 00 00 03 77  77 77 03 63 6e 6e 03 63   .......w ww.cnn.c
0040  6f 6d 00 00 01 00 01 c0  0c 00 01 00 01 00 00 00   om...... ........
0050  b7 00 04 40 ec 5b 15 c0  0c 00 01 00 01 00 00 00   ...@.[.. ........
0060  b7 00 04 40 ec 5b 17 c0  0c 00 01 00 01 00 00 00   ...@.[.. ........
0070  b7 00 04 40 ec 10 14 c0  0c 00 01 00 01 00 00 00   ...@.... ........
```

This is a response to the DNS query in this fr... | Packets: 1273 Displayed: 909 Marked: 0 Dropped: 0 | Profile: Default

Hackers can “sniff” (intercept and observe) network traffic sent over unsecure connections, such as the local Starbucks free wifi.

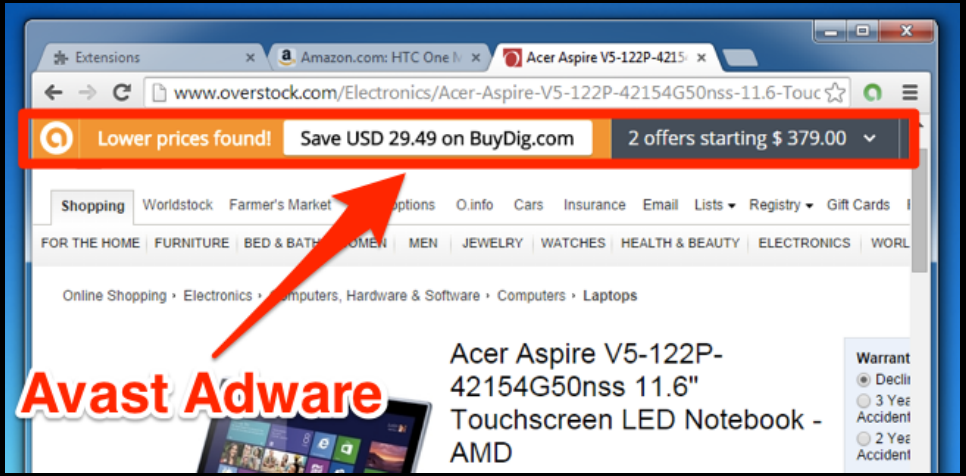
Your neighbor can do something similar if you “steal” his or her wifi.

Best Practices

- Don’t provide login information. To **anyone.**
  - If they have a legitimate reason to access information in an account you control, then that organization will give them the access.
  - Remember: Security Questions, key numbers (like SID)
- Use an encrypted connection (https) wherever possible.
  - If https is not working for you, then consider the possibility that you’ve been infected by malware.
- Don’t download software from untrusted sources.
  - Piracy, email attachments, etc.
- Keep software up-to-date.
  - Exploits target out of date software.

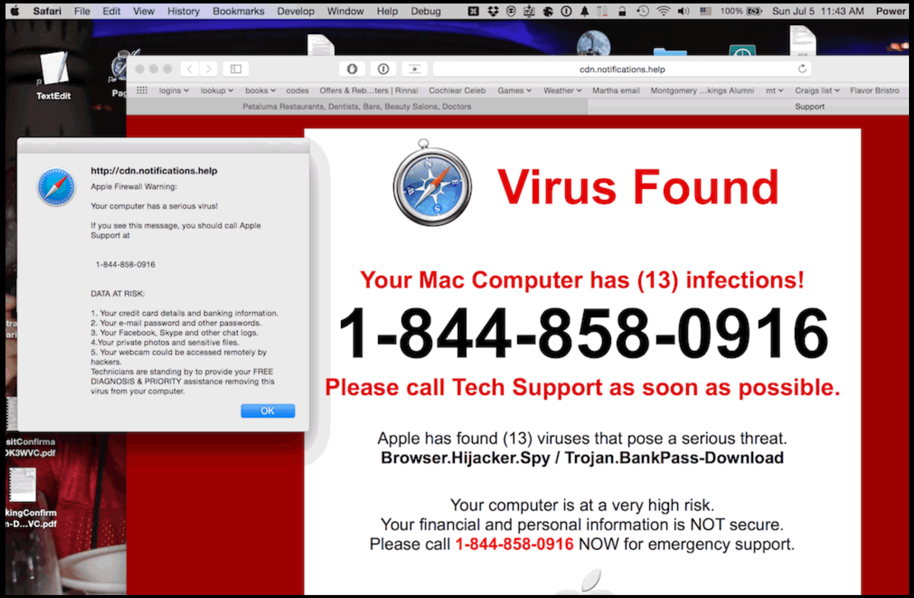
Best Practices

- Watch out for malware
  - Computer behaves strangely.
    - Weird proxies redirecting you to sites other than the one you typed in.
    - Pop up ads.
    - Unusual ads integrated into web pages that weren't there before (and aren't on other computers)



Lower prices found! Save USD 29.49 on BuyDig.com 2 offers starting $ 379.00

Acer Aspire V5-122P-42154G50nss 11.6" Touchscreen LED Notebook - AMD



Safari File Edit View History Bookmarks Develop Window Help Debug
100% Sun Jul 5 11:43 AM Power
TextEdit
cdn.notifications.help
logins lookup books codes Offers & Reb...ters | Rinnai Cochlear Celeb Games Weather Martha email Montgomery ...kings Alumni mt Craigs list Flavor Bristro
Petaluma Restaurants, Dentists, Bars, Beauty Salons, Doctors
Support
sitConfirma K3WVC.pdf
kingConfirm -D...VC.pdf

http://cdn.notifications.help

Apple Firewall Warning:

Your computer has a serious virus!

If you see this message, you should call Apple Support at

1-844-858-0916

DATA AT RISK:

1. Your credit card details and banking information.
2. Your e-mail password and other passwords.
3. Your Facebook, Skype and other chat logs.
4.Your private photos and sensitive files.
5. Your webcam could be accessed remotely by hackers.

Technicians are standing by to provide your FREE DIAGNOSIS & PRIORITY assistance removing this virus from your computer.

OK

Virus Found

Your Mac Computer has (13) infections!

1-844-858-0916

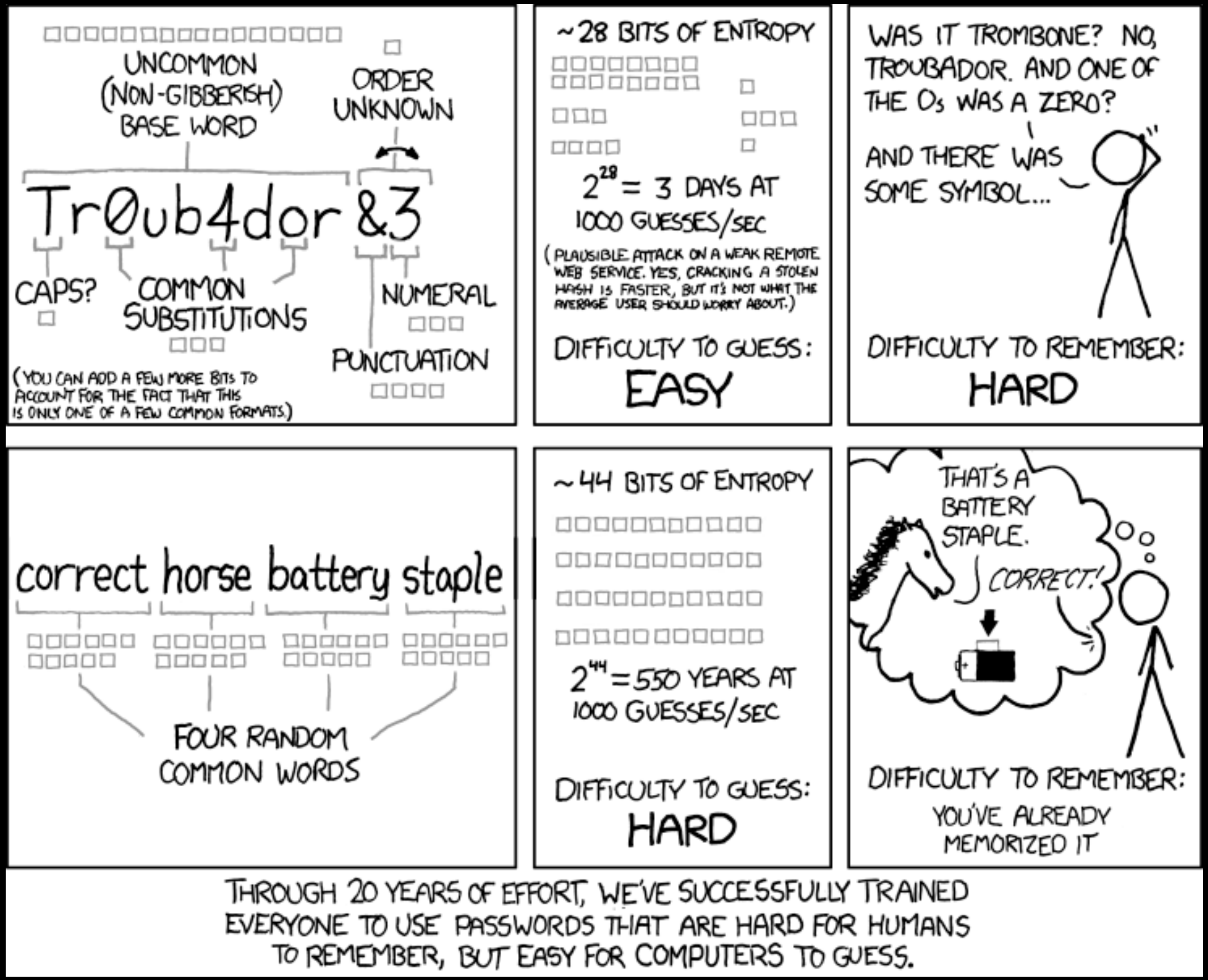
Please call Tech Support as soon as possible.

Apple has found (13) viruses that pose a serious threat.
Browser.Hijacker.Spy / Trojan.BankPass-Download

Your computer is at a very high risk.
Your financial and personal information is NOT secure.
Please call 1-844-858-0916 NOW for emergency support.

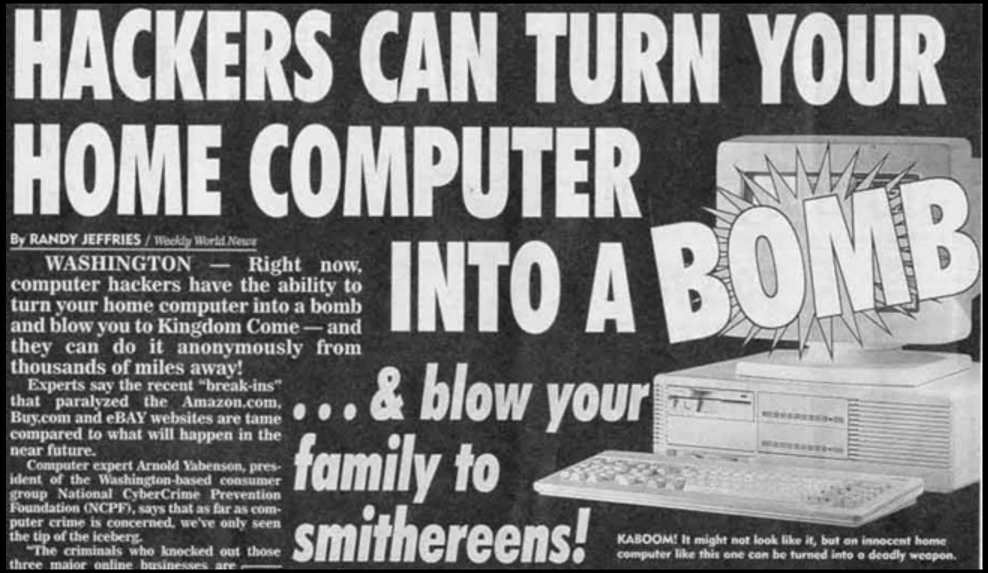
Best Practices

- Use a Strong Password
  - Use common sense here.
  - LastPass and 1Password


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Conclusion

- Hackers are scary, but remember that most attacks are victim initiated.
  - Black belts and mixed martial artists exist, but you're normally not worried about meeting one in a parking lot.
- Have a sensible threat model.
- It's impossible to stop a determined, persistent threat, but basic best practices make you harder (and therefore less worthwhile) to attack.



HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

. . . & blow your family to smithereens!

By RANDY JEFFRIES / Weekly World News

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBAY websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knocked out those three major online businesses are —

KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

(no they can't)

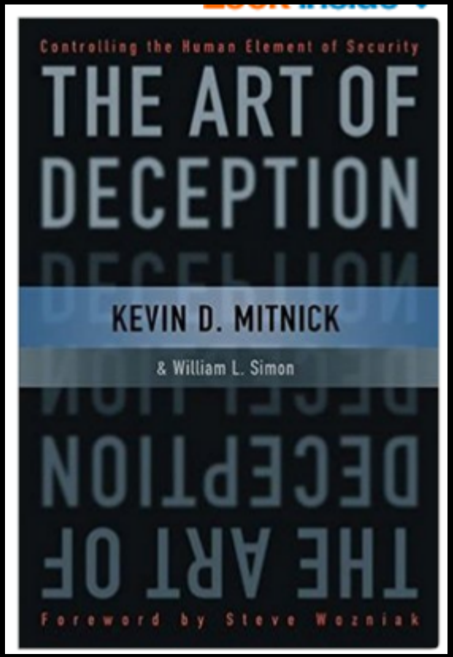
Would you like to know more?
https://decentsecurity.com/

(https all day)

Would you like to know more?

- https://decentsecurity.com
- https://facebook.com/groups/ucrcyber

Decent Security
Start somewhere. Start here.

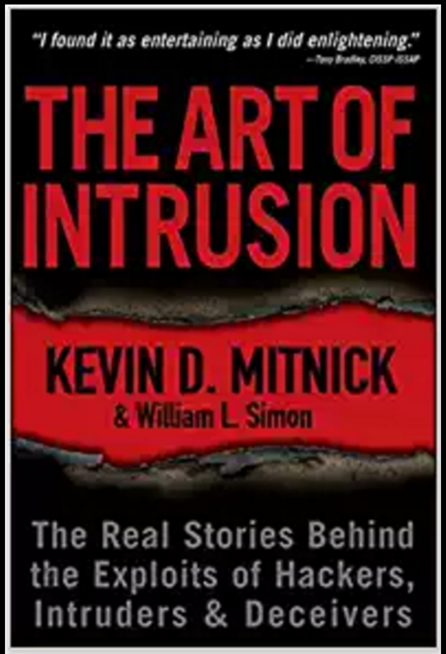

Controlling the Human Element of Security

THE ART OF DECEPTION

KEVIN D. MITNICK

& William L. Simon

Foreword by Steve Wozniak

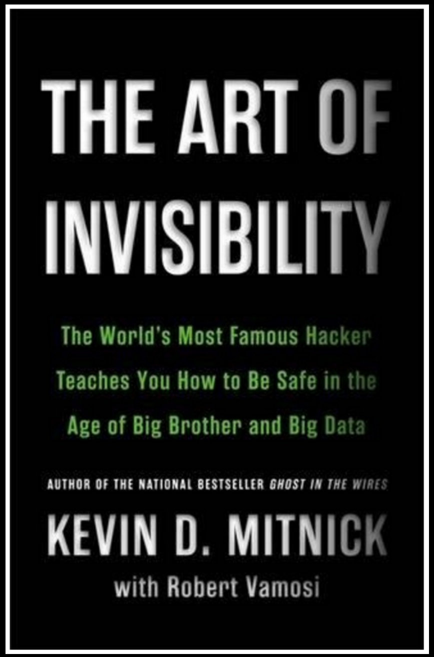

"I found it as entertaining as I did enlightening."
—Tony Bradley, CISSP-ISSAP

THE ART OF INTRUSION

KEVIN D. MITNICK

& William L. Simon

The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers


THE ART OF INVISIBILITY

The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data

AUTHOR OF THE NATIONAL BESTSELLER *GHOST IN THE WIRES*

KEVIN D. MITNICK

with Robert Vamosi

```
cyber@ucr:~$
```