An Introduction to

SECURITY AWARENESS

Jerome Griffith

Security Awareness Presentation

11/10/2015

SECURITY TOPICS

- INTRODUCTION
- COMPUTER SECURITY
- PASSWORDS
- NETWORK SECURITY
- SOCIAL ENGINEERING
- MALWARE
- HACKERS
- MOBILE DEVICES
- BYOD POLICIES
- POP CULTURE TRIVIA
- RESOURCES

INTRODUCTION

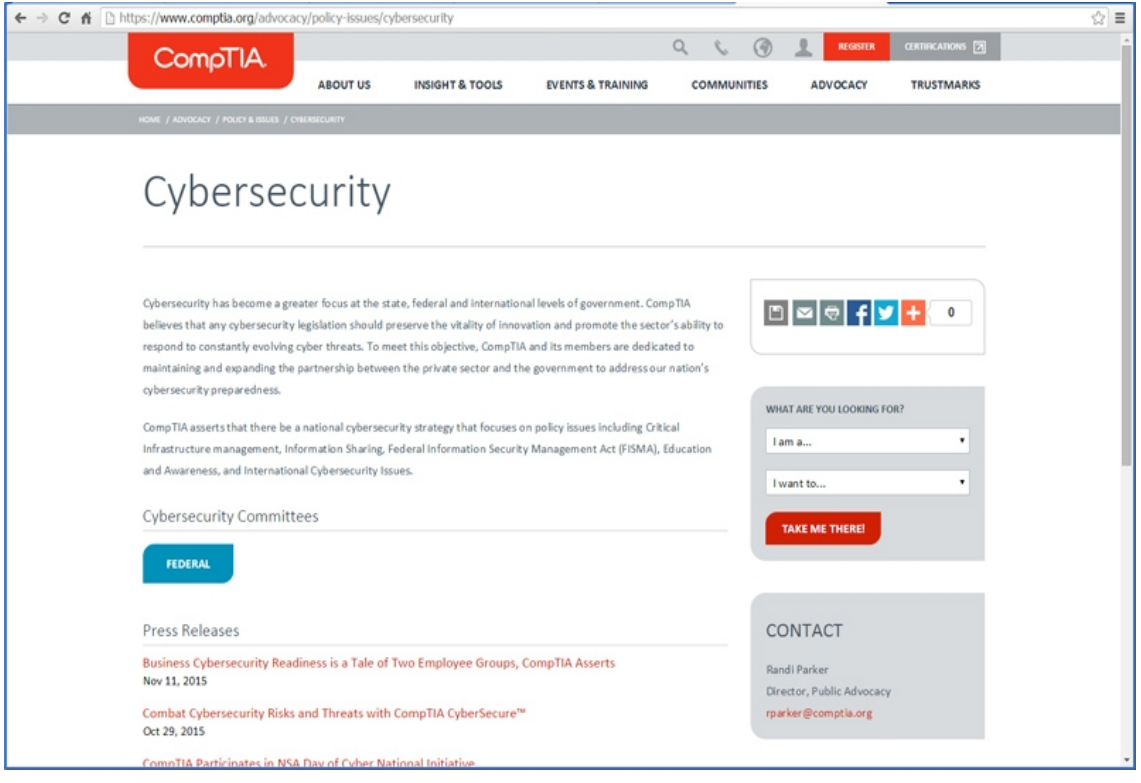
CompTIA Security+ CERTIFIED

- Jerome Griffith
- Security+ certified since February 2015
- The Security+ exam covers the most important foundational principles for securing a network and managing risk. Access control, identity management and cryptography are important topics on the exam, as well as selection of appropriate mitigation and deterrent techniques to address network attacks and vulnerabilities.

http://certification.comptia.org/getCertified/certifications/security.aspx

RESOURCES

comptia.org/advocacy/policy-issues/cybersecurity



cnet.com/topics/security/

cyberark.com/blog/

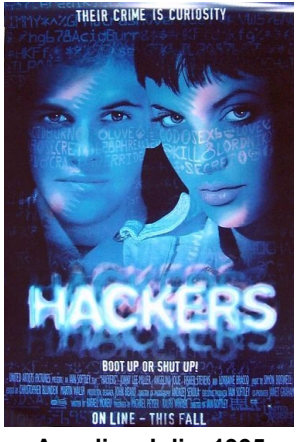
www.infosecnews.org/

lifehacker.com/

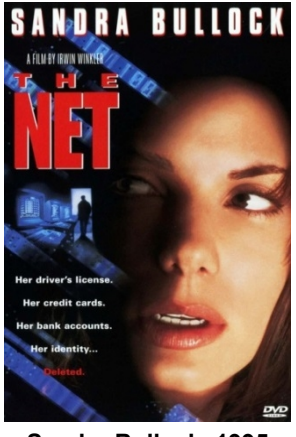
COMPUTER SECURITY

Movies about Computers and Technology

Matthew Broderick, 1983



Angelina Jolie, 1995



Sandra Bullock, 1995

Dir. Mamoru Oshii, 1995

Keanu Reeves, 1999

Bruce Willis, 2007

Chris Hemsworth, 2015

Is Your Computer Secure?

- Do you have sensitive data?
- Who has access?
- Your Location/neighborhood?
- Passwords strong enough?
- Your Mobile devices?
- Your surroundings?

Image from it.amid.com

Personal Computer Security

- If there are multiple users on one computer, let each user log in with their own profile.
- Back up your files to an external hard drive or cloud storage. You never know what could happen to your computer/laptop.

Images from: aulibmedia.blogspot.com and http://www.corbisimages.com
http://lifehacker.com/the-most-important-security-settings-to-change-on-your-1573958554

Personal Computer Security

- Have an active anti-virus software automatically scan and update on your computer.
- Have secure internet/wi-fi connection. (More on this later)

http://lifehacker.com/the-most-important-security-settings-to-change-on-your-1573958554

Workstation Computer Security

- Beware of your surrounding work area and report suspicious people and behavior.
- For your own safety, do not try to confront a suspicious person on your own. **Contact the company security desk**.
- Lock your computer screen when you step away from your desk.

Image from http://www.corbisimages.com

Workstation Computer Security

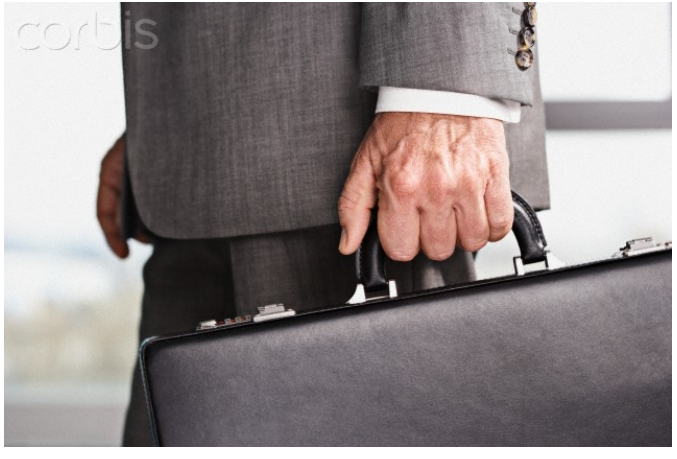
- **Don’t hide passwords under your keyboard or mouse pad.**
- Remember passwords or save them in a **password management program**. (Call [Company] Help Desk and ask them to download KeePass password manager)

Image from http://www.corbisimages.com

Workstation Computer Security

- A real [Company] Help Desk technician can ask for your username BUT will NOT ask you for you password!

PASSWORDS



Passwords: Facts and Tips

- Password Complexity
- Password Length
- Password Hacking/Cracking
- Password Manager Software
- How Passwords Actually Work

Are These Good Passwords?

- abcdefg
- 123456

GIZMODO.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951

Good vs Bad Passwords

OK Password:	Better Password:	Excellent Password:
kitty	1Kitty	**1Ki77y**
susan	Susan53	**.Susan53**
jellyfish	jelly22fish	**jelly22fi$h**
usher	!usher	**!ush3r**
ebay44	ebay.44	**&ebay.44**
deltagamma	deltagamm@	**d3ltagamm@**
ilovemypiano	!LoveMyPiano	**!Lov3MyPiano**
Sterling	SterlingGmail2015	**SterlingGmail20.15**
BankLogin	BankLogin13	**BankLogin!3**
Shelby	ShelbyPass1	**Shelby.Pass1.**
Rolltide	RollTide%	**RollTide%.%**

GIZMODO.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951
http://netforbeginners.about.com/od/antivirusantispyware/fl/What-Strong-Passwords-Look-Like.htm

Password Trivia

DID YOU KNOW…

- The most common password is password
- Followed by 123456

GIZMODO.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951

Secure Passwords

TIPS AND TRICKS

- Use a combination of letters, numbers and symbols in your passwords.
- Use more than 8 characters.
- The longer the password the harder for hackers to crack it.
- Don’t use names of close family members, pets or birth dates.

GIZMODO.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951

Secure Passwords

PASSWORD COMPLEXITY

- Password: insteadofthis
- Password: Ma4eA-P@sxw0RdL*k3Th1s

GIZMODO.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951

Secure Passwords

Password Manager

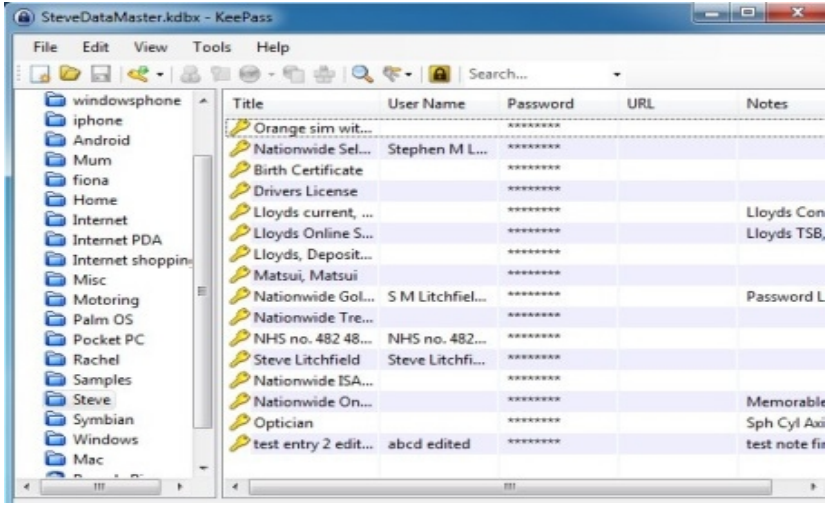
- Use a **password manager** to save all your usernames and passwords.
- This way you can create complex passwords without worrying about forgetting them.

GIZMODO.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951

Secure Passwords

Password manager program examples

- KeePass
- LastPass
- Kaspersky



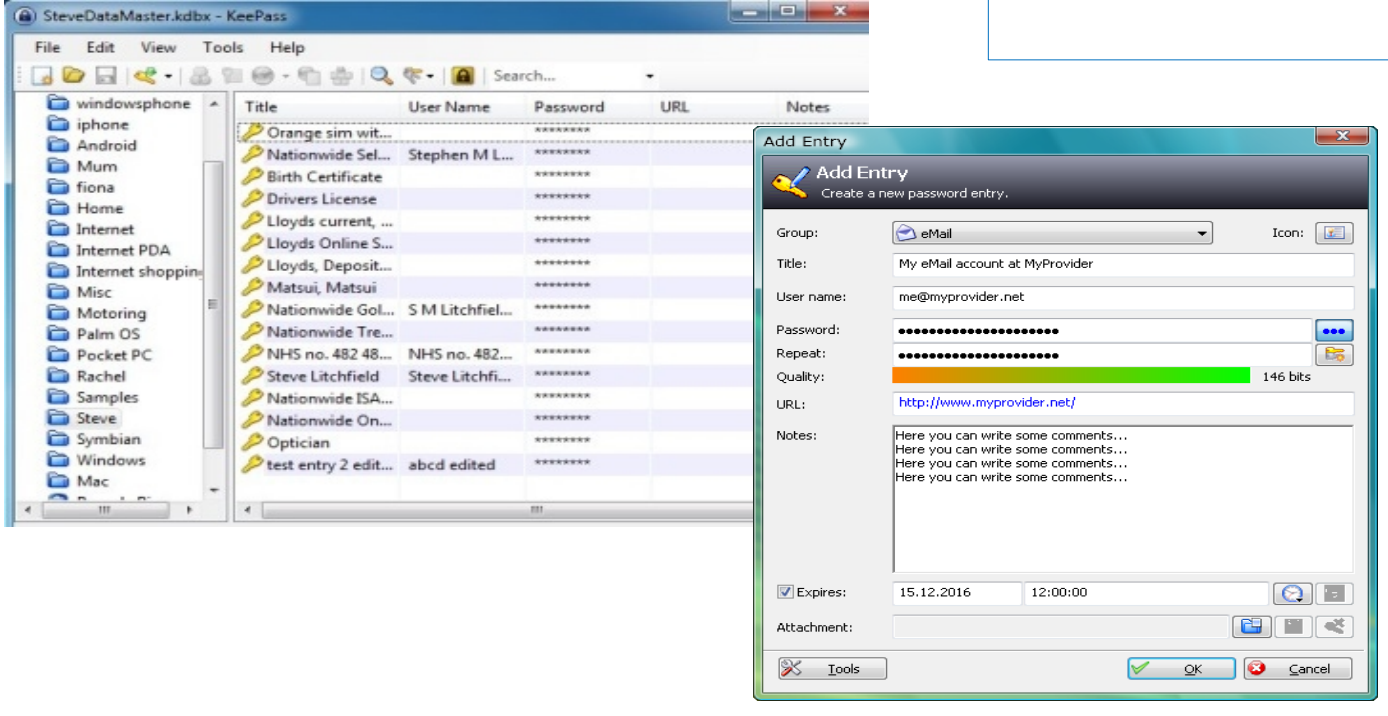
GIZMODO.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951

Secure Passwords

Password Manager

Go to **keepass.info**

- KeePass Example



Keepass.info
GIZMODO.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951

How Passwords Work

Hashing

- Website saves encrypted password into a random series of letters, numbers and symbols call a **Hash**.
- At login – enter password – its encrypted and compared to the hash value.
- If the hash value and password match the user is authenticated.


```
deb46f052152cfed79e3b96f51e52b82c3d2ee8e
00000dc7cc04ea056cc8162a4cbd65aec3d2f0eb
00000a2c4f4b579fc778e4910518a48ec3d2f111
b3344eaec4585720ca23b338e58449e4c3d2f628
674db9e37ace89b77401fa2bfe456144c3d2f708
37b5b1edf4f84a85d79d04d75fd8f8a1c3d2fbde
00000e56fae33ab04c81e727bf24bedbc3d2fc5a
0000058918701830b2cca174758f7af4c3d30432
000002e09ee4e5a8fcdae7e3082c9d8ec3d304a5
d178cbe8d2a38a1575d3feed73d3f033c3d304d8
00000273b52ee943ab763d2bb3d83f5dc3d30904
4f05e273b52ee943ab763d2bb3d83f5dc3d30904
e417aded63377c45bbb7405edaa53d3cc3d30ba6
0000027bb1ecb0cb067f048d67211cefc3d30c7d
000009c7f74c8061dd374ccbec0565eec3d30e5d
0000008b929083820c449e553aaed98fc3d30e88
000007f5e9c746af19b59420d112a00ac3d30f06
00000cbccc8597dcad1931aa3d642dafc3d311e3
000009be0c87f19bd107ba2a6071c211c3d31450
000004c2694f78f6d51a4c975b027812c3d31716
```

GIZMODO.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951

How Passwords Work

Hashing

- The longer and more complex the password,
  the longer and more complex the Hash value will become,
  Making it harder for hackers to crack your password.

	A	B	C
User Name	Clear-Text Password	LAN Manager-Hashed Password	Minutes & Seconds to Crack
Amy	Jhjklhf	9e1c6fde38d236d0aad3b435b51404ee	3:39
Betty	Giants	4a24a40dfoa37fd3aad3b435b51404ee	3:22
Jenny	Giants	4a24a40dfoa37fd3aad3b435b51404ee	3:22
Karen	rollinriver	fdb30d8b81af25ef6a24d62438290ba9	6:05
Mike	Imhappy	af0e3973994ebb24aad3b435b51404ee	1:17
Nancy	H553f83	f6ed43566b1c84ccaad3b435b51404ee	1:30
Steve	pizzalover63	753c086c08af27e7463ofc68a98b195a	7:53
Tom	Giants	4a24a40dfoa37fd3aad3b435b51404ee	3:22
William	Mypass	92315c8b485693a7aad3b435b51404ee	1:48

GIZMODO.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951
http://www.journalofaccountancy.com/issues/2009/jul/20081305.html

How Hackers Crack Passwords

- Techniques like **Brute Force** and **Dictionary Attack**.
- They often use programs that automatically guess any possible password until the software cracks the password.

GIZMODO.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951

How Hackers Crack Passwords

- Also by **Phishing**. They get people to provide them through social engineering.
- **The more complex your password the harder it is for the hacking program to figure it out and crack your password.**

GIZMODO.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951

Statistics

- People aged **18-24** are the highest group at risk
- **38%** of victims had their debit or credit card number stolen
- **43%** of all identity theft is a result of stolen wallets and paperwork
- **1 in 10** U.S. consumers have already experienced identity theft

Identityhawk.com
https://www.identityhawk.com/identity-theft-risk-statistics-infographic

Millions

Of accounts get hacked every year!

Exact figures are unknown.

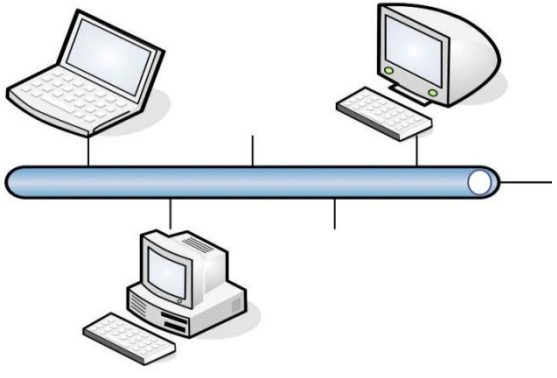
Passwords are like underwear: you don’t let people see it, you should change it very often, and you shouldn’t share it with strangers.

— *Chris Pirillo*
Founder and CEO of LockerGnome, Inc.

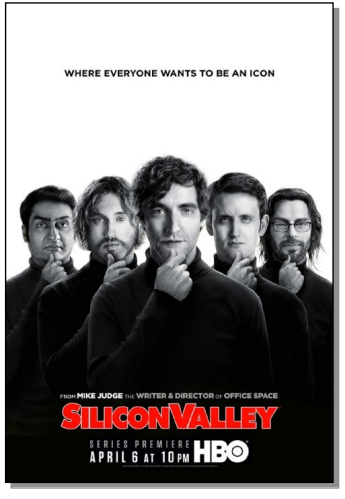
http://www.itscolumn.com/2011/08/top-10-it-security-quotes/

NETWORK SECURITY

(Internet, Intranet and WiFi)



TV Shows about Computers and Technology



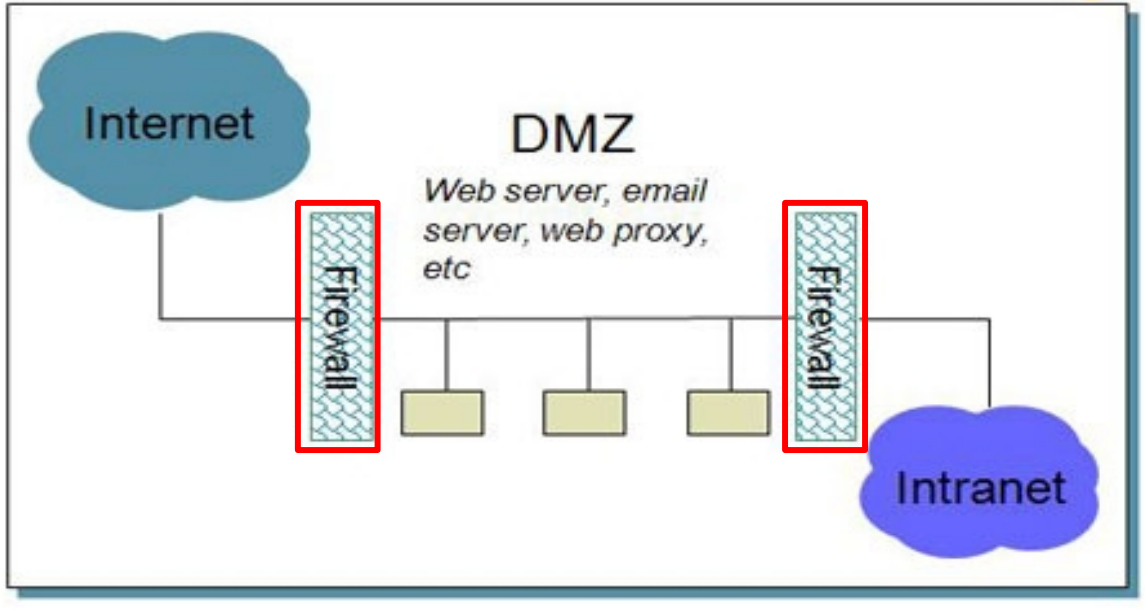
Network Attacks

Firewalls, DMZs and Switches are network defenses against the following attacks:

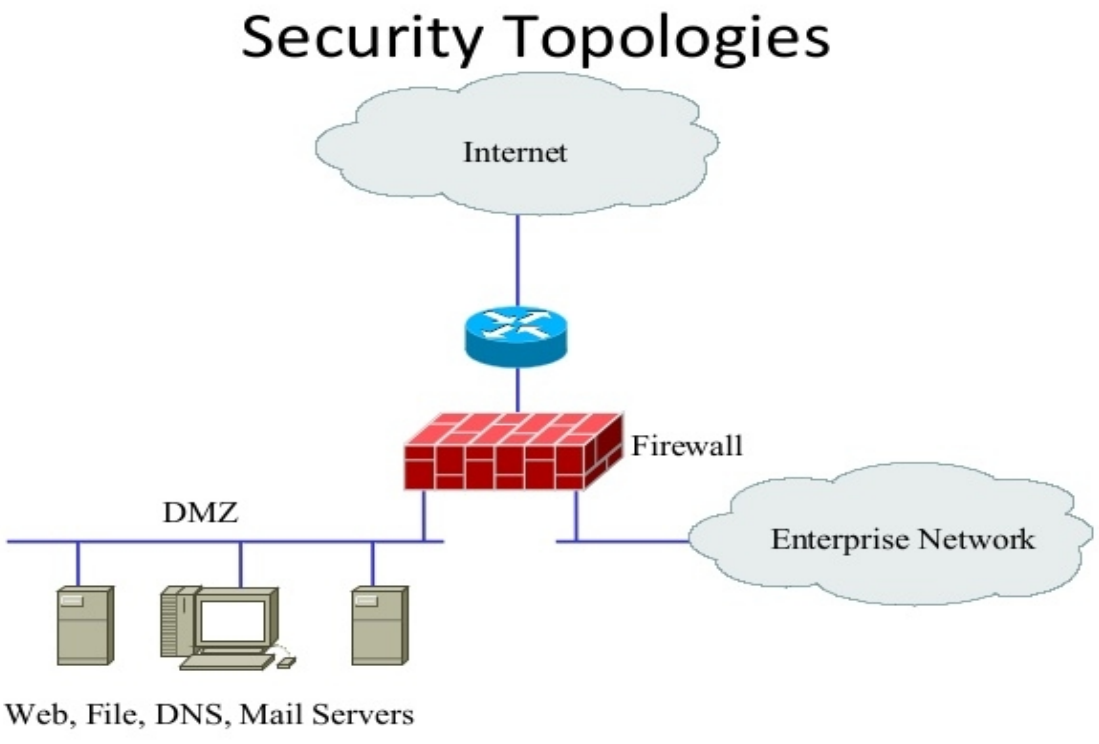
- Brute Forces Attack
- Dictionary Attack
- Denial of Service (DoS)
- Birthday Attack
- Ping Flood Attack
- Man-in-the-Middle
- Packet Sniffing
- War Driving

Network Security

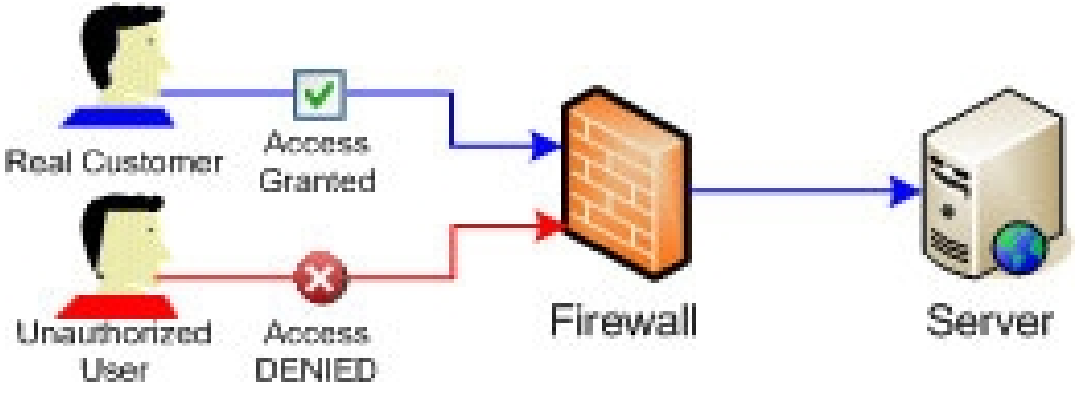
Firewalls



Network Security

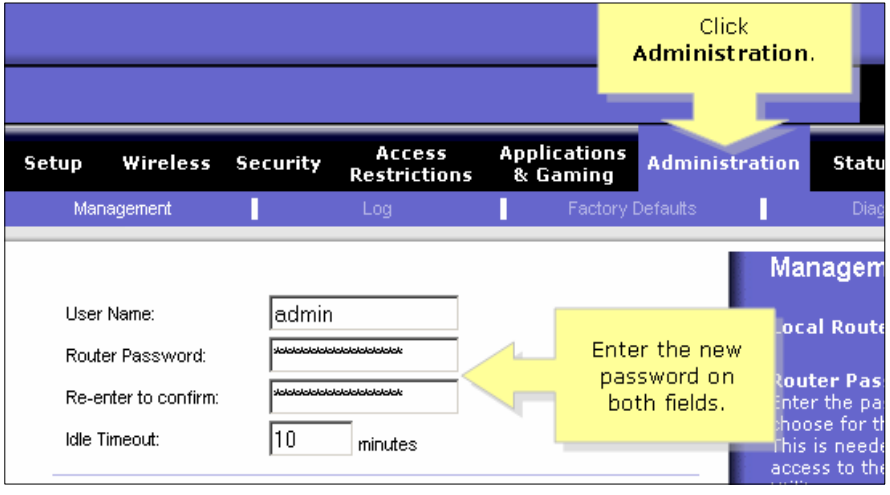


Network Security



Internet and Wireless Network Security

- **Change your default username and password for your wired and wireless internet connection**.
- Anyone can search for default passwords on the internet and use your internet.



Images from Messer Studios, LLC, ProfessorMesser.com
community.linksys.com

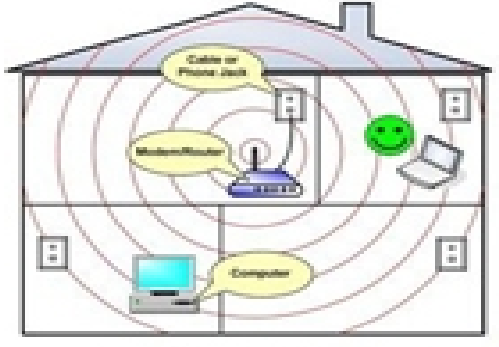
Internet and Wireless Network Security

- Be sure to use secure Wi-Fi settings and connections. **WPA2-AES** is the strongest setting.
- **Do NOT use WPA and WEP settings**. WEP is the weakest setting.

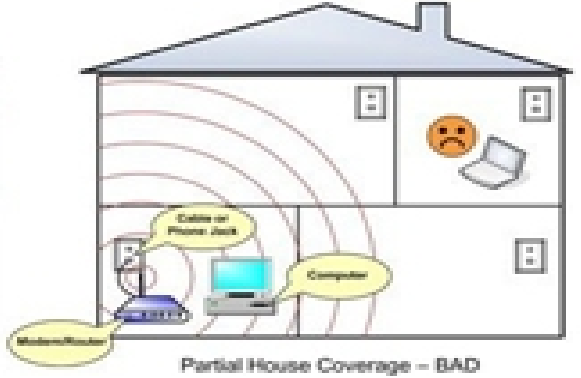
Images from Messer Studios, LLC, ProfessorMesser.com
Verizon.com

Internet and Wireless Network Security

- Place your **wireless access point in the center or top floor** of your home for even wireless distribution.
- Don't have the wireless strength too strong that it extends too far outside your home. You can be victim of **War Driving** attack. This is when someone drives or walk around a neighborhood looking for weak or open internet accounts.



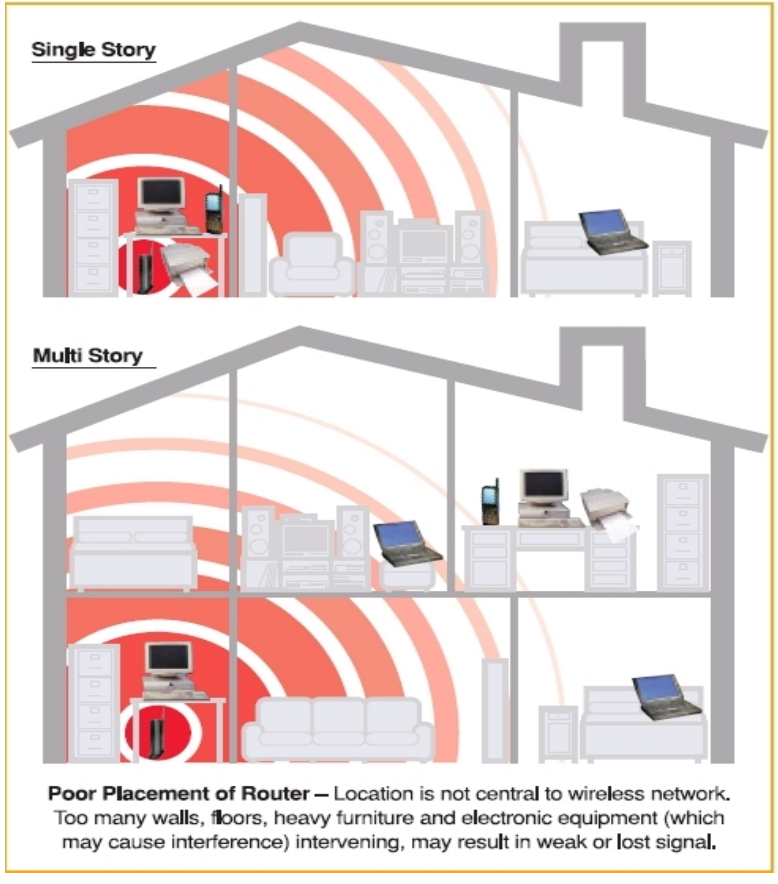
Whole House Coverage – GOOD



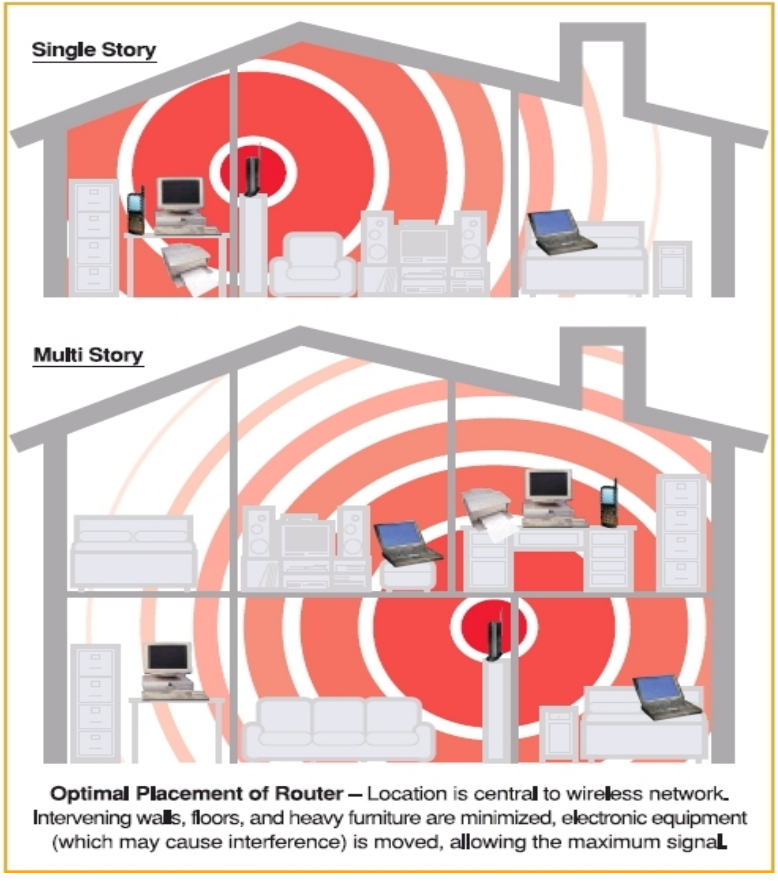
Partial House Coverage – BAD

Images from www.examcollection.com

Internet and Wireless Network Security



Poor Placement of Router – Location is not central to wireless network. Too many walls, floors, heavy furniture and electronic equipment (which may cause interference) intervening, may result in weak or lost signal.



Optimal Placement of Router – Location is central to wireless network. Intervening walls, floors, and heavy furniture are minimized, electronic equipment (which may cause interference) is moved, allowing the maximum signal

Images from blog.roku.com

SOCIAL ENGINEERING

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

— *Bruce Schneier*
American cryptographer, computer security and privacy specialist

http://www.itscolumn.com/2011/08/top-10-it-security-quotes/

Social Engineering

- A non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.

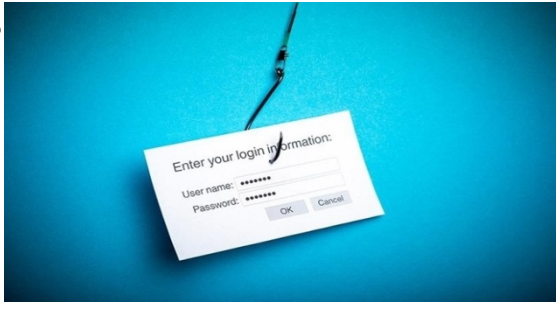
http://searchsecurity.techtarget.com/definition/social-engineering

Social Engineering Techniques

- Phishing
- Whaling
- Dumpster driving
- Tailgating
- Shoulder Surfing

Phishing

- Social engineering with a touch of spoofing
- Often delivered by email spam, IM, etc.
- Don’t be fooled, check the URL
- **Vishing** is done over the phone.
- Fake security checks or bank updates
- Spear Phishing/Whaling



Phishing

- Don’t be fooled, check the URL

I sent you an eCard from AmericanGreetings. Happy Valentine's Day ! - Thunderbird

File Edit View Go Message OpenPGP Tools Help

Get Mail Write Address Book Decrypt Reply Reply All Forward Delete Junk Print Stop

Subject: I sent you an eCard from AmericanGreetings. Happy Valentine's Day !

From: AmericanGreetings <services@americangreetings.com>

Date: 13/02/2007 22:46

To:

Greeting Card Notice with real-looking return address

To view your eCard, choose from the options below.
Click on the following link.
[1]http://www.americangreetings.com/view.pd?i=414303935&m=2157&rr=z&source=a
g999
Or copy and paste the above link ...r's "address" window.
If you have any comments or ques...
[2]http://www.americangreetings...?source=ag999
Thanks for using AmericanGreetin...

The address looks real but the actual link is hidden and leads to malware

References

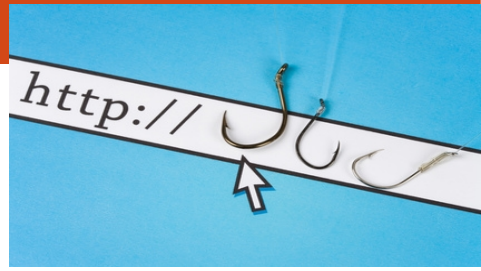
1. http://qgjjdfa.americansgreetings.net/uk/viewcard.html
2. http://qgjjdfa.americansgreetings.net/uk/viewcard.html

http:www.hackspoof-legit-website/92437592478909

Whaling

- A Social engineering technique by sending **fake emails** in an attempt to trick **Management and/CEOs** of a company into disclosing sensitive information about the person or company. (catching the Big Fish!)

Phishing Awareness Training



- Some companies have a Phishing Awareness training campaign.
- If you receive a suspicious email in your Outlook click the Report Phishing button at the top right corner.

Dumpster Diving

Image from http://barfblog.com/wp-content/uploads/2013/03/dumpster-dive-flickr-diegofuego.jpg

Dumpster Diving

- Searching through neighborhood dumpsters and trash cans for sensitive documents that may not be properly discarded.
- Utility bills, social security number, etc.
- **Can you guess other documents they may search for?**
- Bank and credit card statements, medical bills, junk mail with credit card offers, and more
- Shred these documents first!

Use A Paper Shedder

- Use the right type of shredder.

Strip Cut	Cross-Cut	Micro-Cut	High Security
Security Level 2	Security Level 3	Security Level 4	Security Level 6
			
39 -- 7/32" stripsper 8.5" x 11" page	399 particlesper 8.5" x 11" page	3,000 particlesper 8.5" x 11" page	13,000 particlesper 8.5" x 11" page
Ideal for: Non-confidential documents	**Ideal for:** Credit/College Applications, Insurance papers, Junk mail	**Ideal for:** Medical Records, Employee/HR Files, Bank/Financial Statements	**Ideal for:** Top Secret or Classified Government Documents

Not Secure Enough

Aim For One Of These

Even Better!

The shredders in the office are in this range.

http://static.bootic.com/_pictures/9BQIwQL74hGhvrg-jZoiug/600x/_.jpg

Tailgating / Piggy Backing

- An attacker, seeking entry to a restricted area secured by unattended, electronic access control, simply walks in behind a person who has legitimate access.
- Following common courtesy, the legitimate person will usually hold the door open for the attacker.

https://www.petri.com/wp-content/uploads/01-tailgating.png

Shoulder Surfing

- You're in a public setting, (Library, coffee shop) and someone is literally looking over your shoulder at you screen to see your private information like bank account number, credit card number, facebook account, email, password, etc.
- This happens a lot on airplanes and waiting lounges.

Shoulder Surfing Prevention Tips

- Delay logging into sensitive websites like bank accounts until you get home.
- If you must access confidential information when you're in public purchase a **Privacy Filter/Protector** for your laptop so people behind you cannot see the contents of your screen at all.

image from www.alibaba.com

Detecting / Stopping Social Engineering Attacks

- The simplest way to defend against social engineering attacks is to **use common sense**.
- **Someone creating a tremendous sense of urgency.** If you feel like you are under pressure to make a very quick decision, be suspicious.
- **Someone asking for information** they should not have access to or should already know.

http://searchsecurity.techtarget.com/definition/social-engineering
www.securingthehuman.org

Detecting / Stopping Social Engineering Attacks

- **Something too good to be true.** A common example is you are notified you won the lottery, even though you never even entered it.
- **If you suspect someone is trying** to make you the victim of a social engineering attack, do not communicate with the person any more.

http://searchsecurity.techtarget.com/definition/social-engineering
www.securingthehuman.org
techaddictz.wordpress.com

Preventing Future Social Engineering Attacks

- Never Share Passwords
- Don’t Share Too Much Information
- Verify Contacts

www.securingthehuman.org
www.infosecurity-magazine.com

Social Engineering Awareness

- Many companies have **training sessions to teach employees** how to be aware of malicious social engineering.
- Organizations perform **penetration tests** using social engineering techniques to test their employees, security and systems.

http://searchsecurity.techtarget.com/definition/social-engineering

MALWARE

Malware / Viruses

- '**Malware**' is an umbrella term used to refer to a variety of forms of hostile or intrusive software,
- It can take the form of executable code, scripts, active content, and other software.

https://en.wikipedia.org/wiki/**Malware**

Types of Malware

- Computer viruses,
- Worms,
- Trojan horses,
- Ransomware,
- Spyware,
- Adware,
- Scareware,
- and other malicious programs.

https://en.wikipedia.org/wiki/**Malware**

Anti-Malware

- Always have an anti-malware/anti-virus program activated on your computer, laptop, tablet, cell phone, etc.

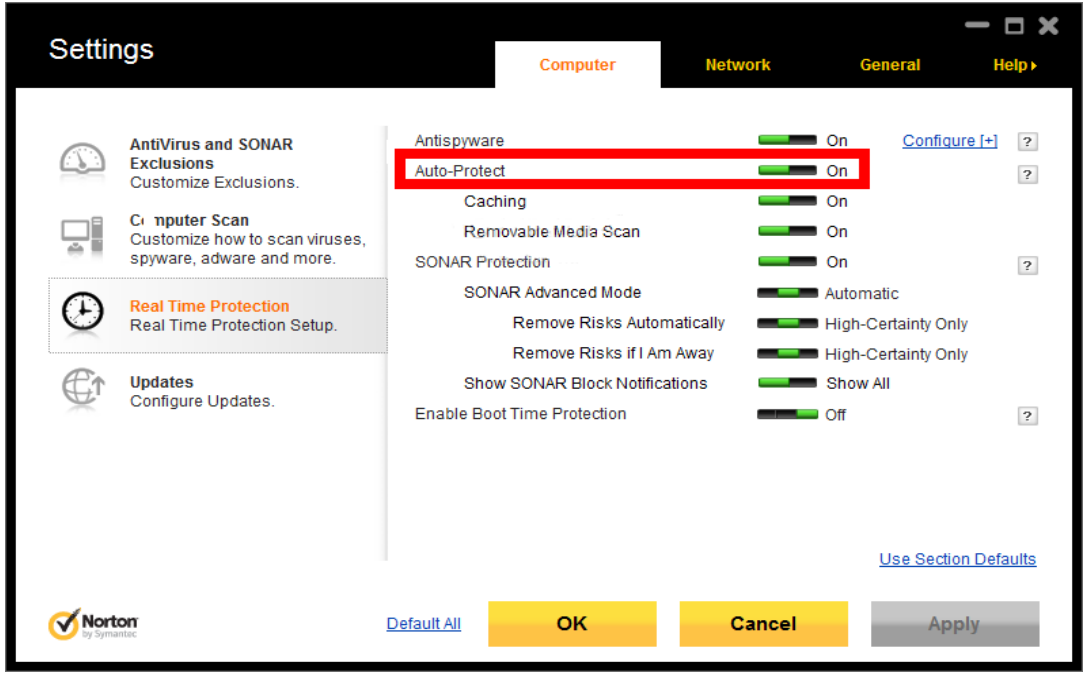


Image from www.ctimls.com
https://en.wikipedia.org/wiki/**Malware**

Anti-Malware

- What's wrong with these settings?

https://en.wikipedia.org/wiki/**Malware**

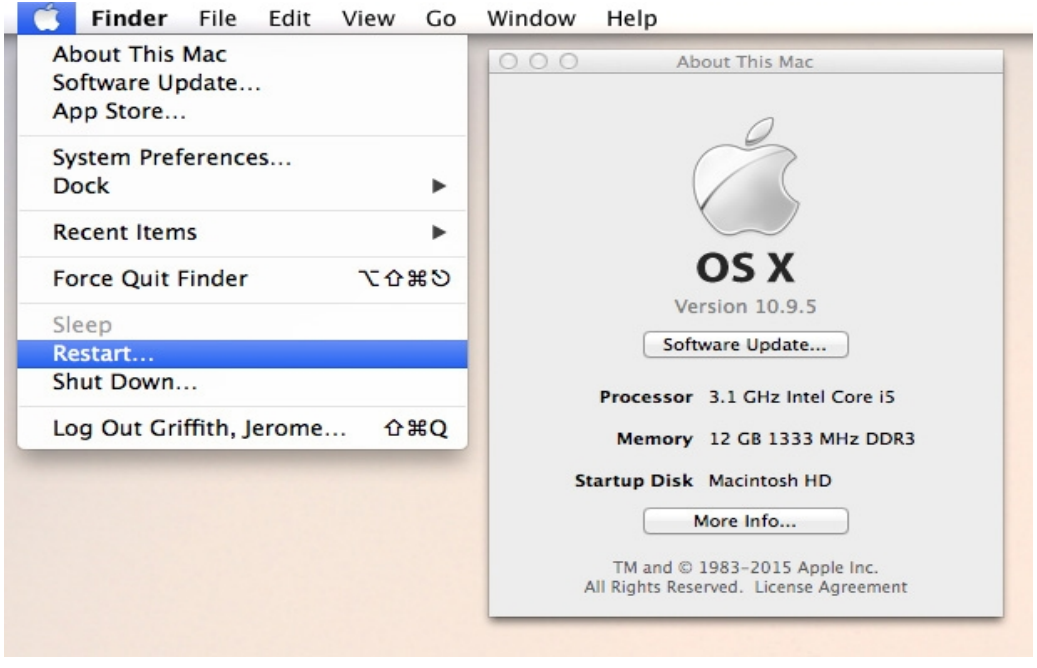
Anti-Malware

- Always update your anti-virus software when it asks you to do so.

https://en.wikipedia.org/wiki/**Malware**

Anti-Malware

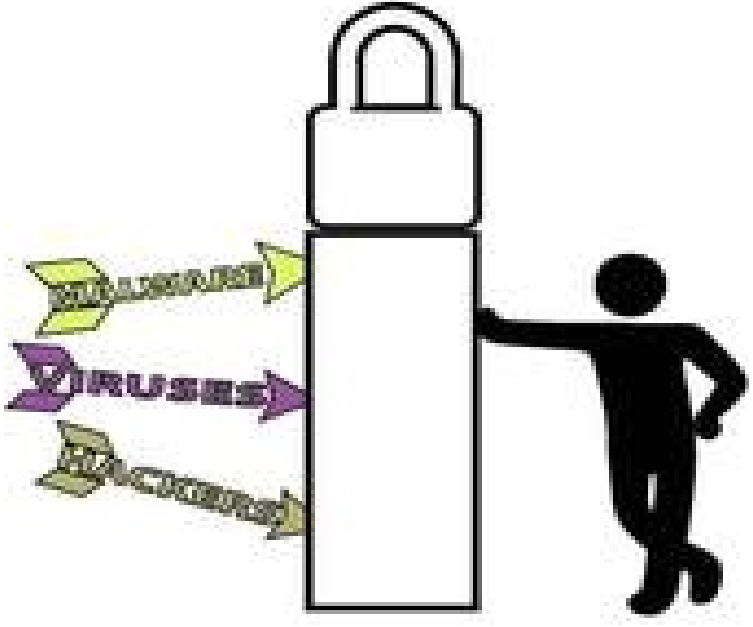
- Workplace computers are automatically updated, so reboot at the end of each day.



Screen shot by Jerome Griffith

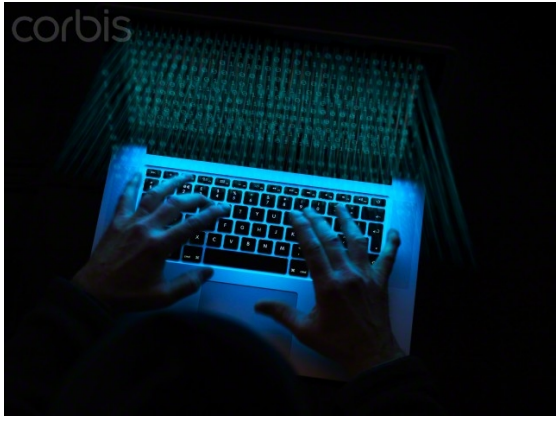
Anti-Malware Recommendations

- Norton AntiVirus
- McAfee
- MalwareBytes
- Bitdefender
- AVG



https://en.wikipedia.org/wiki/**Malware**
http://www.top10antivirussoftware.com
http://top5antivirussoftware.com/

HACKING



Hacking Software and Codes

- Hackers either **download software** from the internet or **develop their own programs** to infiltrate networks and computers.

Image from http://www.corbisimages.com

Hacking Software and Codes

- Some **write codes or scripts to infiltrate/hack** passwords, email, databases, computers, etc.

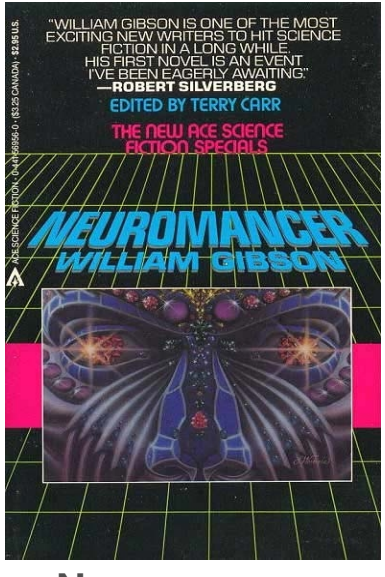
Image from http://www.corbisimages.com

If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked.

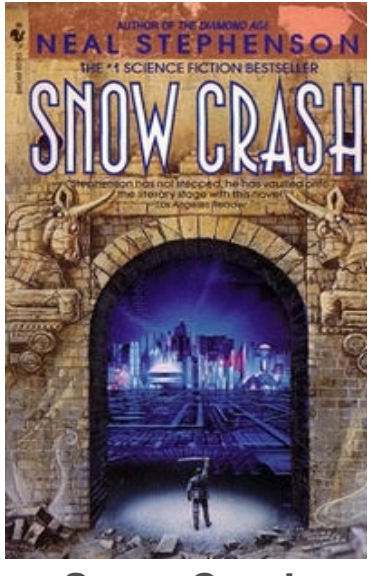
— *Richard Clarke*
Former National Coordinator for Security,
Infrastructure Protection,
and Counter-terrorism for the United States.

http://www.itscolumn.com/2011/08/top-10-it-security-quotes/

Novels about Computers and Technology

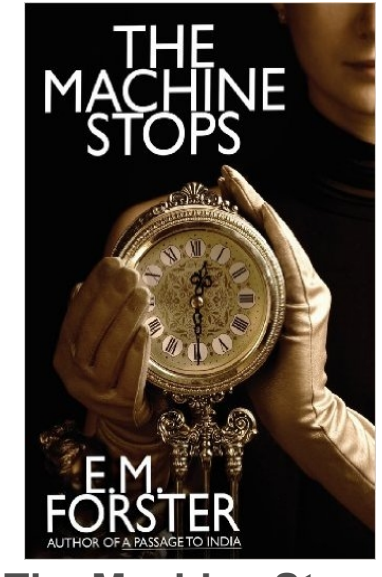


Neuromancer
William Gibson (1984)



Snow Crash
Neal Stephenson, 1992

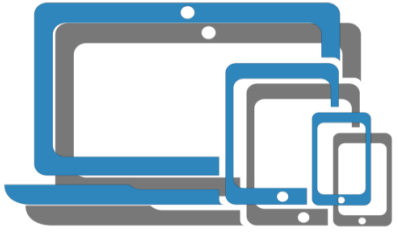
Ghost in the Shell
Masamune Shirow (1989)



The Machine Stops
E. M. Forster (1909)

Images from https://en.wikipedia.org

MOBILE DEVICES



http://mi-backup.co.uk/mi-briefcase/

Whats Wrong with this picture?

What do you see in this picture?

Mobile Device Security Tips

- **Setup a passcode or swipe pattern for your smart phone and tablet.**
- **Location Apps:** Find your device if lost by making a sound or display message.
  E.g. *Device Manager* app.
- **Remote Wipe:** Delete all info and data from device if lost for good.
- **Remote Backup:** Backup everything automatically to cloud storage. Example: Google Apps for Android devices.

Device Manager

http://www.ProfessorMesser.com

Mobile Device Security Tips

- Only download apps from trusted sources like **Apple App Store** and **Google Play**.
- Make sure your **apps are up to date** for security patches from the app developers.
- Uninstall apps you are not using.
- Install and activate an **Anti-Virus software** on you mobile device.

Mobile Device Security Facts

- **Travel** is the number one way mobile devices are lost.
- Most are lost at **security check points**.
- **Authorized Apps** on company tablets.
- About **50 company devices are lost per year**. That's almost one device per week.

Enterprise Security: Rob Hoehn
Image from corbisimages.com

BYOD Policies

Bring Your Own Device Policies

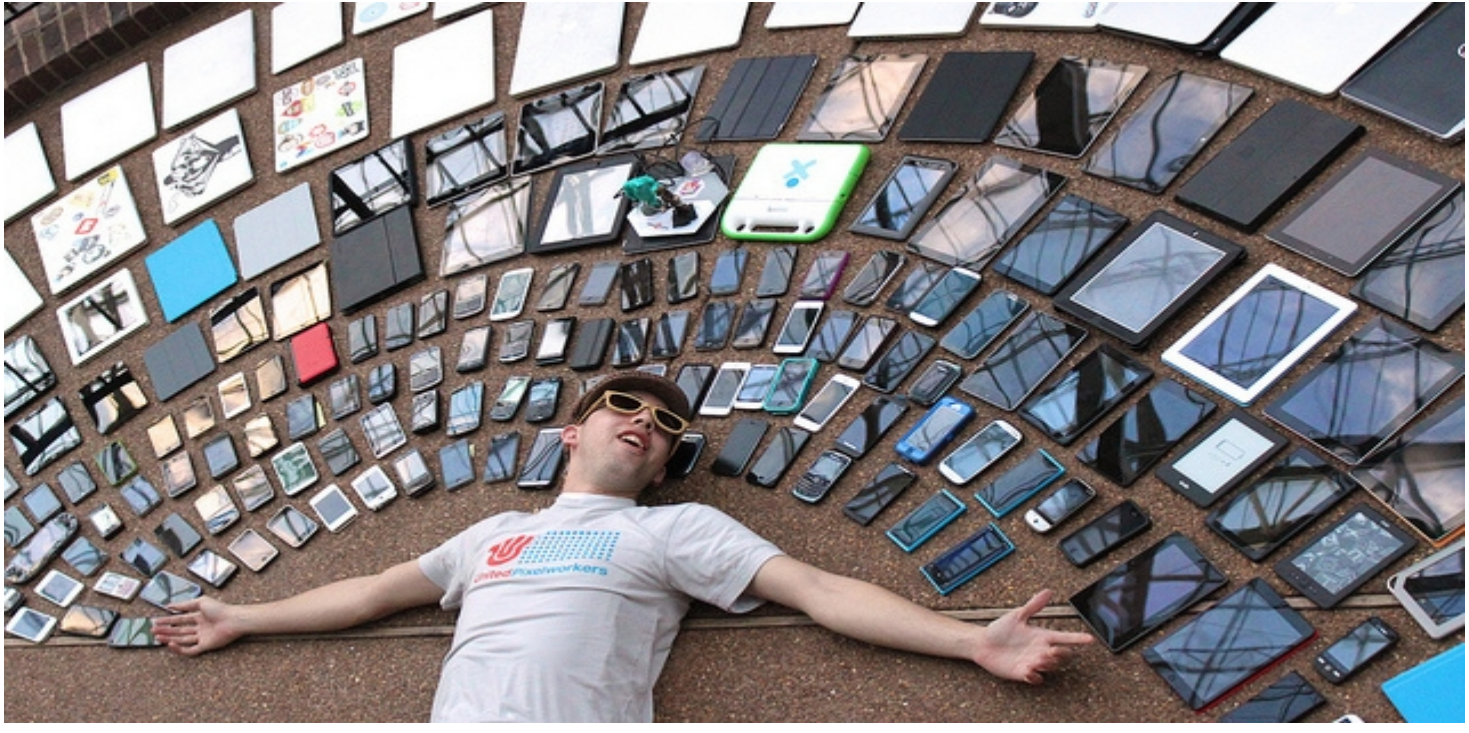
- Acceptable use of personal mobile devices – smartphones, tablet devices, laptops, PDAs, flash drives – in the workplace.
- Rules and Restrictions
- Security concerns

Mobile Devices and Access; Version 3.2; April 6, 2015; Prepared by: Jeff Snyder
Image from corbisimages.com

BYOD Policies

- Personal devices should not be used to perform work related tasks unless authorized (except when using Citrix to remote into your work stations).
- Work related files should not be downloaded to you device.
- Employees may connect their personal devices to the **company's WiFi** network to access the internet.
- Employees can use an **Entrust token** for authentication login to their MS Outlook/work email and Workstations from there laptop or other mobile device.

Mobile Devices and Access; Version 3.2; April 6, 2015; Prepared by: Jeff Snyder
GMM: Good Mobile Messaging application. Used for access to corporate email on a personal device .
Image from T. Rowe Price MediaBeacon DAL.



http://sproutsocial.com/insights/trends-2014-social-mobile-synonymous-now-heres/

Cyberpunk

- A genre of science fiction set in a lawless subculture of an oppressive society dominated by computer technology.

Science Fiction

Is becoming

Science Fact.

Positive Impact of Technology

Virtual classrooms, bionic prosthetic arms and legs for humans and animals, GPA devices and more!

Images from various sources.

WHAT WAS THE FIRST MOVIE TO FEATURE COMPUTER HACKING?

First Movies About Computer Hacking?

1

Hot Millions (1968)

- Starring Peter Ustinov as the hacker.
- A Cockney con-artist just out of prison replaces an insurance company's computer programmer and sends claim checks to himself in various guises at addresses all over Europe.

2

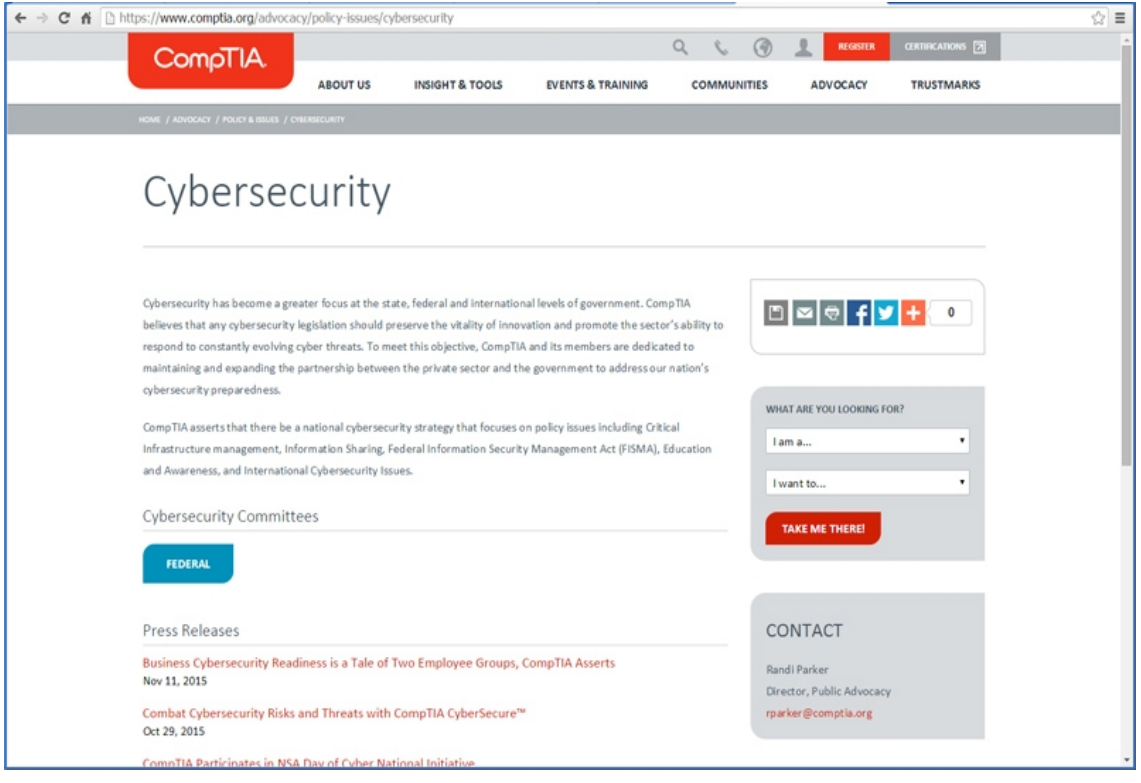
The Italian Job (1969)

- Starring Michael Caine.
- Comic caper movie about a plan to steal a gold shipment from the streets of Turin by creating a traffic jam.

The Italian Job : https://youtu.be/Z0uN32GV1_c
Hot Millions : https://youtu.be/7pnsxmU1Amw
http://www.paranoidprose.com/2011/12/31/the-worlds-first-hacker-movie/

RESOURCES

comptia.org/advocacy/policy-issues/cybersecurity



cnet.com/topics/security/

cyberark.com/blog/

www.infosecnews.org/

lifehacker.com/

COMPTIA SECURITY+ CERTIFICATION

http://certification.comptia.org/certifications/security

http://certification.comptia.org/certifications/security

THANK YOU