

0



1



2



3



4

Passwords

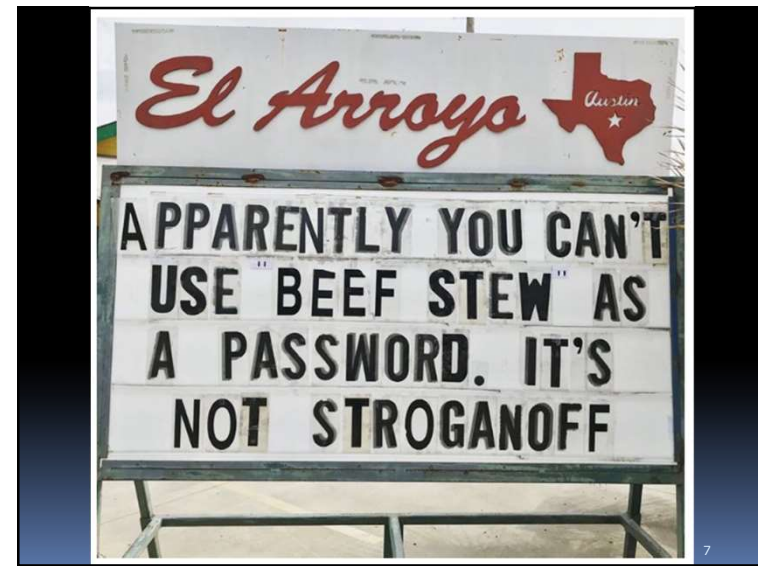
- The most important protection
- Often, the **only** protection

5

Passwords - Agenda

1. How strong is your password?
2. How hackers can guess passwords
3. How hackers can steal passwords
4. How to make a strong password
5. Which accounts need strong passwords
6. How to manage passwords easily

6



7

A Strong Password

- Think of a strong password, easy to remember
- Write it down

8

Is Your Password Strong?

- Password strength tests:
 - www.grc.com/haystack.htm
 - www.PasswordMeter.com

9

9

What Do You Use This for?



Sony PlayStation 3 game console, 2006

10

10



- 200 PlayStation 3's
- Guesses millions of passwords in seconds
- 2008

11

Guess What This Is?



Array of
25
graphics
cards

From: boingboing.net
2012

348 Billion Password Guesses per Second!

12

The Dictionary



Websters: Only **470,000** words

13

What Is a Strong Password?

- Must be long, at least 14 characters
- Include many different characters:
 - Numbers, symbols, capital letters and lowercase letters
- Use random characters
- Avoid common words, dates, names
- ~~Change the password regularly~~

14

14

Can You Remember This Password?

4Sa7ya,ofbfotc

4 Score and **7** years **a**go, **o**ur forefathers
brought forth **o**n **t**his **c**ontinent

15



16

Some Recent Data Breaches

Ashley Madison	2015	32 Million
Uber	2017	57 Million
JP Morgan Chase	2014	76 Million
Equifax	2017	146 Million
Marriott	2018	500 Million
Yahoo!	2013	3 Billion

17

Common Passwords

- Oct. 2013: Adobe.com attacked
- Hackers stole millions of passwords
- ... and posted them!

The 100 Worst Passwords

18

Companies *Will* Be Hacked

- We can't control that
- What does that mean?

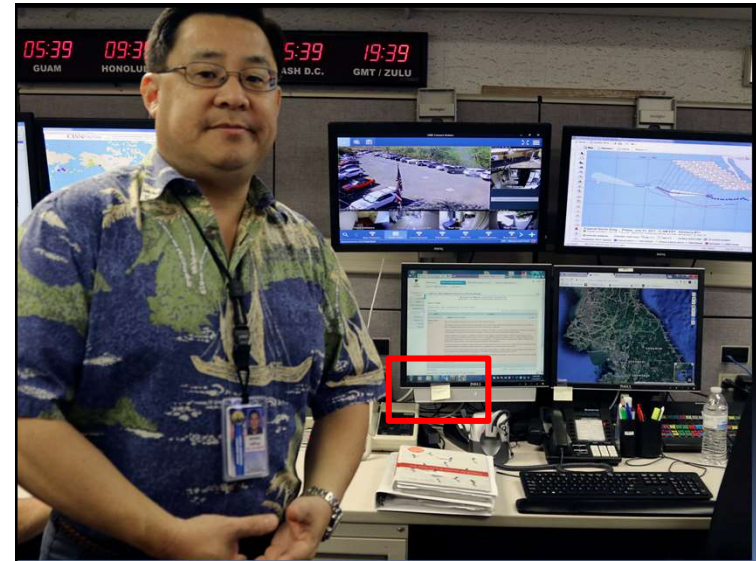
A Different Password for each account

19

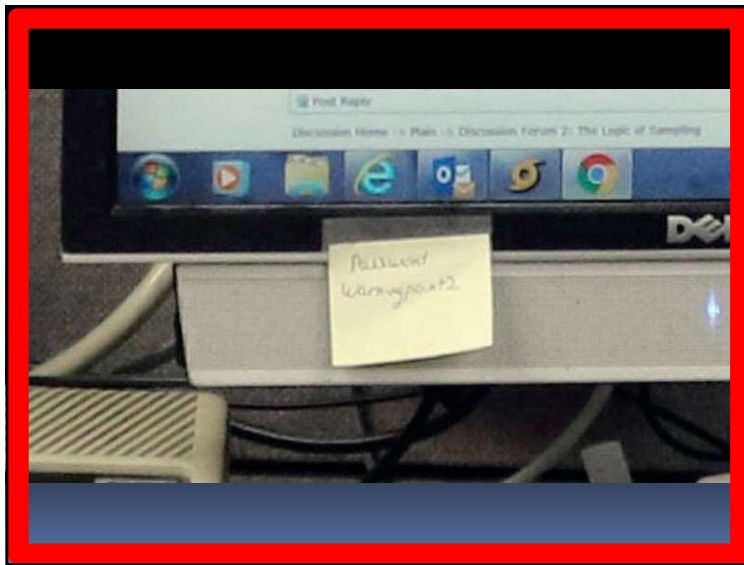
Writing Down Passwords

- Be careful!

20



21



22

2-Factor Authentication

- Proving that you are really you
- Requires Two Things:
 - Something you know: Password
 - Something you have: Phone

23

2-Factor Available on:

- Google Gmail
- Apple
- Facebook
- Instagram
- Twitter

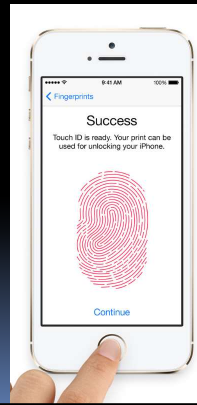
24

Anything Easier than Passwords?

25

Biometric Authentication

- Reads:
 - Fingerprint
 - Patterns in eye
 - Voice authentication
 - Face pattern
- Convenient but secure
- Need password as backup



26

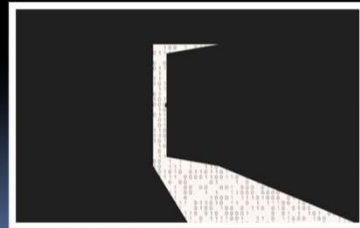
Which Accounts Need Strong Passwords?

- Banking / Finance
- Retailers
- Email

27

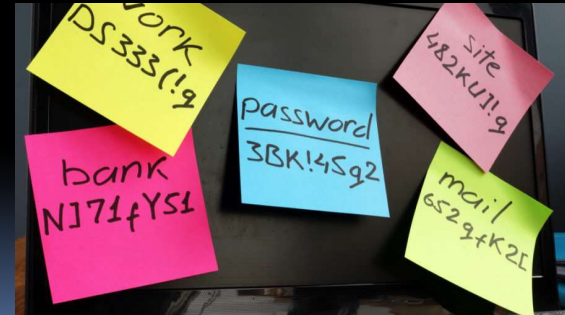
Why Protect Email?

- Email may be a backdoor to your other accounts



28

How can you keep track of all your passwords?



29

29

Password Manager Software

- Remembers passwords for you
- Creates complex passwords
- Enters passwords automatically
- Examples:
 - **LastPass**
 - 1Password
 - Dashlane

30

30

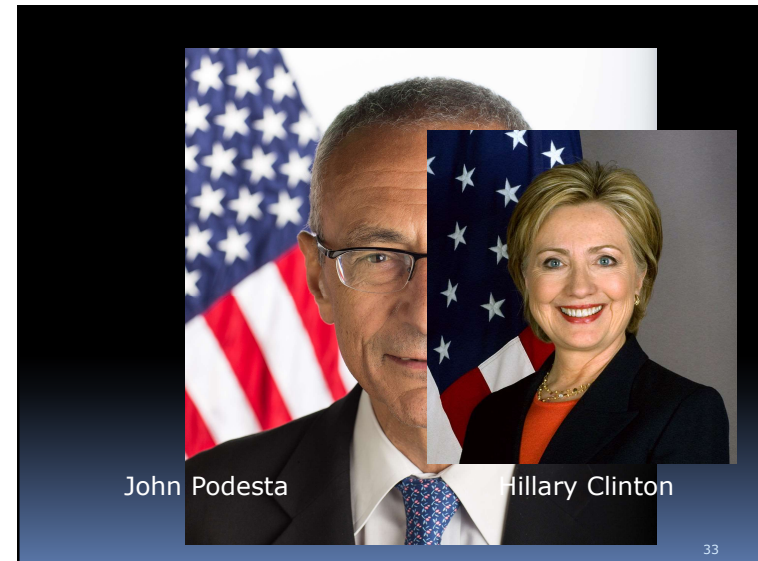
Passwords: Summary

- Use a Strong Password
 - Long
 - Random
 - Unique
- Use a Password Manager
- Use 2-Factor Authentication
- Use a Fingerprint Reader

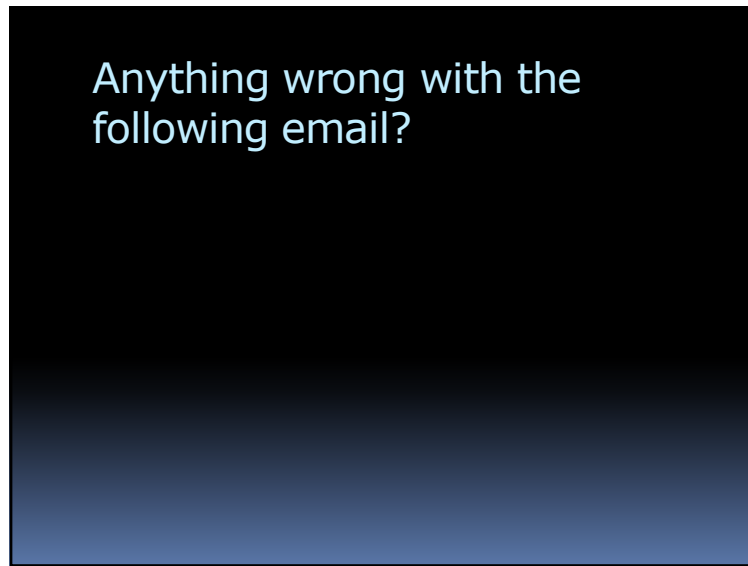
31



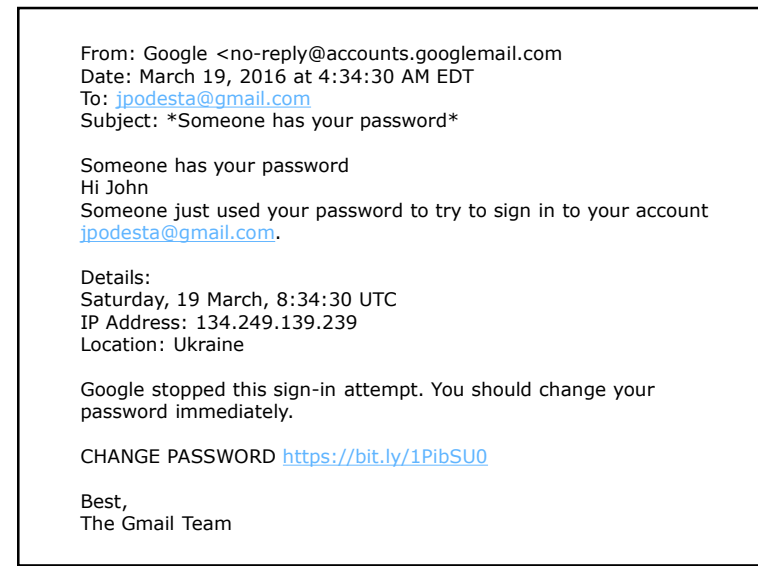
32



33



34



35

Subject: Re: Some has your password

Sara, NOT

This is a legitimate email. John needs to change his password immediately and ensure that two-factor authentication is turned on his account.

He can go to this link: <https://myaccount.goog.e.com/security> to do both. It is absolutely imperative that this is done ASAP.

If you or he has any questions, please reach out to me at 410-562-9762.

36

From: Google <no-reply@accounts.googlemail.com>
 Date: March 19, 2016 at 4:34:30 AM EDT
 To: jpodesta@gmail.com
 Subject: *Someone has your password*

Someone has your password
 Hi John
 Someone just used your password to try to sign in to your account
jpodesta@gmail.com.

Details:
 Saturday, 19 March, 8:34:30 UTC
 IP Address: 134.249.139.239
 Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD <https://bit.ly/1PibSU0>

Best,
 The Gmail Team

37

Phishing

- Fake Email or Web sites
- Tricks Internet users to reveal:
 - Credit card, Social Security numbers, etc.

38

Social Engineering

- Tricks people to reveal information
 - Often doesn't involve computers
 - Often on phone

"What's Your Password," from the Jimmy Kimmel show:
<https://www.youtube.com/watch?v=opRMrEfAIII>

39

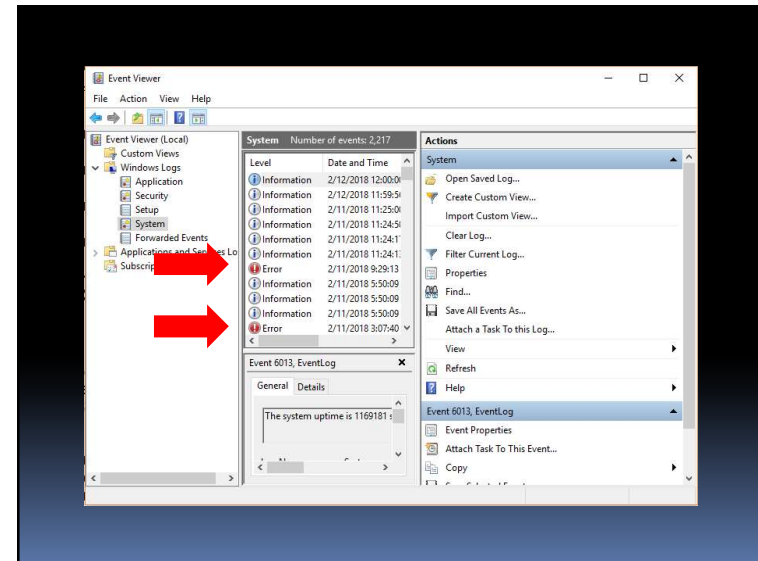
Phishing by Phone

- Tries to get information
- Or access to your computer

An Actual Phone Call:

"Hello, I am calling from Microsoft. We have received an indication that there is a bad virus on your computer..."

40



41

Spear Phishing

- Targeted email
 - Contains confidential customer details
- Can easily trick people to reveal:
 - Credit cards, Social Security numbers, etc.

42

42

Which Is a Phishing Attempt?

- Bank says problem with your account
- FedEx says it cannot deliver package
- Amazon confirms your purchase of a \$500 Apple iPad
- All of the above**

43

What's Wrong with These?

- <http://www.tvvitter.com>
- <http://yahoo.pcrsys.com>
- <http://hrvbt.com/security/support/pc/microsoft.com>

44

Security Questions

- The name of your first pet?
- What was your childhood nickname?
- What day were you born on?

- A Backdoor to your accounts

Many answers are now on websites!

45

Facebook Phishing

- Fake surveys and contests
- Games
 - "What's your stripper name?"

46

What to Do?

- Be wary of *ANY* inbound message:
 - Email
 - Pop-up
 - Phone call

47

47

Summary – Phishing

- Phishing tricks you into revealing secret information
- Impersonates banks, government, Internet companies, etc.
- Be wary of any inbound communication

48

3. Malware

“Malicious Software”
Viruses, Worms, Trojan Horses, etc.



49

Types of **Malware**

- Viruses
- Worms
- Trojan Horses
- Ransomware
- Spyware

50

Viruses can spread without human interaction.

1. True

2. False

51

Computer **Viruses**

- A program attached to a data file
- Spread when files are exchanged
 - Email
 - Downloaded songs and videos
 - USB Flash Drives
- Requires user action to come alive

52

52

Viruses

- Usually arrive as attachments
 - May be disguised as Web [hyperlinks](#)
- Often come from **friends**
 - Via your friend's Address Book

53

Worms

- Spread by themselves
- Through networks
- **Without human interaction**

From: www.freecompostingworms.com

54

Trojan Horses

- Appears to be useful
 - E.g., Removes viruses
- But does something bad



55

55

USB Flash Drives



- Be wary of USB drives you "find"

56

The Register
Biting the hand that feeds IT

DATA CENTER SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SCIENCE EMERGENT TECH BOOTHNOTES LECTURES

What is your first layer of defense?
5 Things to Know
Network Segmentation

Security

Half of people plug in USB drives they find in the parking lot

Why do we even bother with security software?

By Shaun Nichols in San Francisco 11 Apr 2016 at 21:09 115 SHARE

A new study has found that almost half the people who pick up a USB stick they happen across in a parking lot plug said drives into their PCs.

Researchers from Google, the University of Illinois Urbana-Champaign, and the University of Michigan, spread 297 USB drives around the Urbana-Champaign campus. They found that 48 percent of the drives were picked up and plugged into a computer, some within minutes of being dropped.

"The security community has long held the belief that users can be socially engineered into picking up and plugging in seemingly lost USB flash drives they find," the researchers reported this month.

Ad closed by Google
Stop seeing this ad
AdChoices

57

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FBI

BIZ & IT

Two US power plants infected with malware spread via USB drive

Investigators find no up-to-date antivirus, system backups for control systems.

DAN GOODIN - 1/15/2013, 3:30 PM

<https://arstechnica.com/information-technology/2013/01/two-us-power-plants-infected-with-malware-spread-via-usb-drive/>

58

What Does Malware Do

- Main purpose
 - Spread to other computers
- Secondary objectives
 - Slow down networks
 - Display annoying messages
 - Gain control of computers
 - Destroy files or hold files for ransom

59

Bots and Botnets

- Malware turns PCs into “bots”
 - Controlled by a hacker
- Hackers can have “botnets”
 - Armies of thousands of bots
- Can be used to “attack” websites

60

Which Is a Sign of an Infected PC?

- A. Odd messages or pop-ups appear
- B. Program icons suddenly are gone
- C. Browser takes you to strange places
- D. Computer is unusually slow
- E. Computer fan is very loud
- F. Antivirus programs stop working
- G. All of the above

61

61

Oh, No!

Cryptolocker 2.0

Your personal files are encrypted

Your files will be lost without payment on:
11/24/2013 3:16:34 PM

Info
Your **important files were encrypted** on this computer: photos, videos, documents, etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key **RSA-4096** generated for this computer. To decrypt files, you need to obtain **private key**.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet, **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

See files << Back Proceed to payment >>

62

Ransomware

- The worst type of malware
- Encrypts your documents, pictures
- You have to pay ransom to decrypt
- E.g., “CryptoLocker”

63

Cryptolocker Strikes Again

Illinois Cops Pay Hackers \$500 Ransom to Unlock a Computer

An e-mailed virus disabled computers until cops paid \$500 in Bitcoins

Don't Miss Out — Follow us on: f t i y

by Matt Stroud

A suburban Chicago police department paid hackers \$500 in Bitcoins to unlock a computer they had remotely disabled, according to a report.

4:00 PM EST
February 23, 2019

The *Chicago Tribune* reported that the Midlothian Police Department was the latest government department to be

64

Your Other Computers:

Routers & Cable Modems

- These devices are tiny computers
- Often targets for hackers
- Avoid cheap routers
- Be sure to keep them updated

65

REUTERS World Business Markets Politics TV

Brexit Imprisoned in Myanmar Sectors Up Close Breakingviews Investing Future of Money World At Work

CYBER RISK MAY 25, 2018 / 11:54 AM / 6 MONTHS AGO

FBI warns Russians hacked hundreds of thousands of routers

Joseph Menn, Sarah N. Lynch 3 MIN READ t f

(Reuters) - The FBI warned on Friday that Russian computer hackers had compromised hundreds of thousands of home and office routers and could collect user information or shut down network traffic.

66

The Best Way to Get Infected?

- A. Download free songs or videos
- B. Open strange email attachments
- C. Download free programs
- D. Share a USB Flash drive
- E. Don't update your software
- F. Go to porn sites
- G. All of the above

67

Summary

- Many types of malware
 - Viruses, worms, Trojan Horses, etc.
- Can cause many types of problems
- Several ways to avoid them

68

4. Privacy & WiFi



69



Gen. David Petraeus


- 4-Star General
- Director of the Central Intelligence Agency (CIA)

70



General & Mrs. Petraeus

71



General & Paula Broadwell

- The General's Biographer
- *And Mistress*

A photograph of General Stanley A. McChrystal III (Petraeus) in military uniform standing next to Paula Broadwell. They are both smiling and have their hands clasped in front of them. The background features the American flag and a red banner with Arabic calligraphy.

72

If the **Director of the CIA** has no privacy ...

How can **you** expect to have any?

73

Remember:
EMAIL IS NEVER PRIVATE

74

Q: Can employers spy on their employees' computers?

75

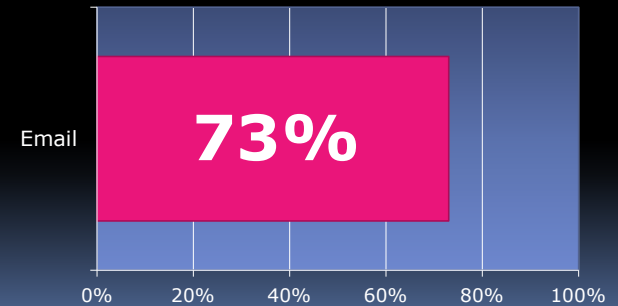
How Many Employers Spy on Their Employees?

Survey by:

- The American Management Association
- The ePolicy Institute

76

Employers Who Monitor Email



77

Spyware

- Transmits information about you
- **Keylogger**
 - Records keystrokes:
 - Passwords, Login IDs, Credit cards

78

78

Who Uses Spyware?

- Bosses
- Hackers
- Parents
- Spouses
- Ex-Spouses

79

WiFi

- Wireless network in homes and companies
- Very convenient
- Not very secure

80

Have you ever accessed your bank account while using WiFi?

1. Yes
2. No

81

"Pineapples"



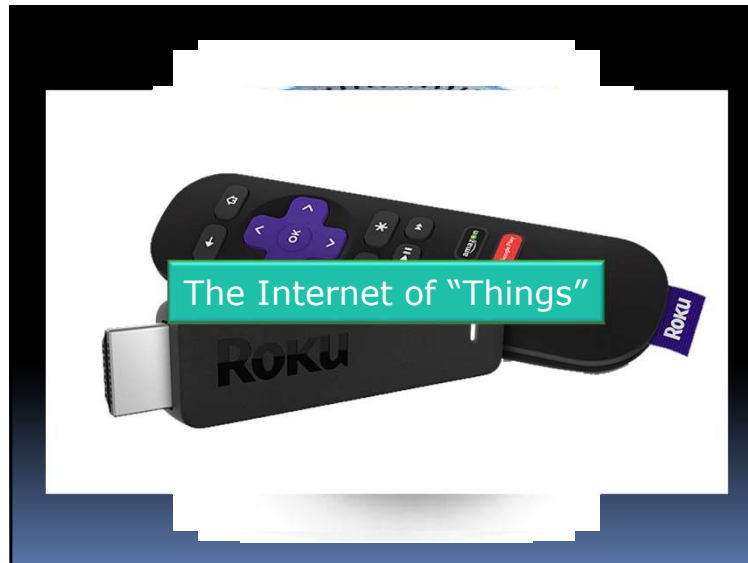
82

Wireless Eavesdropping

- Beware public places (Starbucks)
- Someone can "sniff" your connection

- Use https
- Use a VPN

83



84

The Internet of Things (IOT)

- Growing number of devices
- Minimal security
- Can spy on us
- Or can be turned into bots

85

Eavesdropping



- Baby monitors have little security
— Ars Technica, 9/02/2015

86

Your Phone Is a Tracking Device

- Google apps: Timeline
 - Record everywhere you have been
- iPhones
 - Record "Significant Locations"



87

A "Slave"



From: arstechnica.com

- A woman unknowingly captured by her own webcam

88

"Slaves" on the Internet

From: arstechnica.com

- Pictures of women posted on the web
- Taken without their knowledge

89

Ratters

- Hackers who spy on women
- Use: Remote Administration Tools
 - RAT
- Takes control of a woman's PC
- Watches camera
- Takes pictures; Posts on Web
- **Cure: Put tape on the webcam**

90

Cover That Camera

<https://www.youtube.com/watch?v=1MV3ZlazAIA>

91

Review: True or False

- Email provides ~~secure~~ communication
- WiFi is ~~always safe~~
- Hackers can see laptop users ✓
- Anything connected to the Internet could be a security problem ✓

92

5. Protection



93

Antivirus Software

- Programs you can buy:
 - Norton
 - McAfee
 - ~~Kaspersky~~

94

94

Antivirus Software

- Free programs
 - AVG
 - Avast
 - Microsoft Security Essentials
 - Microsoft Windows Defender

95

95

Microsoft Windows 10

- Includes Windows Defender
- Finally a good antivirus app
- Additional antivirus not needed
 - Can actually reduce security

96

How Antivirus Software Works

- Looks for **virus signatures**
- Prevention
 - Scans incoming email
- Cures
 - Scans whole PC periodically
- **Quarantines** possible malware
 - Moves virus to secure area on HD

97

82,000

- New viruses every day, worldwide
 - Source: pcworld.com, 3/18/14

11,000

- New babies in US every day
 - Source: babycenter.com

98

"Zero Day" Virus

- Brand new virus
- Antivirus s/w can't spot it

99

Update Your Antivirus S/W

- New viruses arrive every day
- Antivirus cannot protect you if...
 - It does not know about new viruses
- Be sure software updates *automatically*

100

Malwarebytes Free

- "Virus first aid"
- Quickly scans your PC
- Finds and removes malware
- Free, from malwarebytes.org

101

If Your PC Is Infected ...

- Scan with your Antivirus Program
- Scan with Malwarebytes
- Worst case:
 - Reinstall your operating system and programs and backed-up data

102

Keep All Programs Up to Date

- No program is perfect
 - Can have vulnerabilities
 - Discovered by hackers
- Programmers come up with patches
- Be sure all programs are up to date
 - *Automatically*

103

103

Attention!

**Your current version of Adobe Flash Player is outdated!
Your computer is vulnerable to malware now.
Update your Adobe Flash player now.**

[Click Here](#)

Don't fall for this!

104

Go to the Source

- Update **only** at publisher's site:
 - microsoft.com
 - adobe.com
 - java.com
 - etc.

105

Firewalls

- Program or Device
- Protects computers from outside threats
 - E.g., hackers and worms
- Already included in Windows 7+

106

Is Your Firewall Working?

- Websites that test a PC's vulnerability
 - Gibson Research Corp. (www.grc.com)
 - ShieldsUP
 - LeakTest

107

Don't Give Yourself Too Much Power

108

Who Can Do More Damage?



If an enemy agent impersonated a general, he could do much more damage

109

Two Types of User Accounts

- Administrator
- Standard User

- Only Administrator can install software

110

Set up Two Accounts on Your PC

- An Administrator account
 - Use only when installing software
- A Standard User account
 - Use this account at all other times

Then...

- If a virus attacks your PC
- It cannot install itself!

111

Don't Be an Administrator

- Use a Standard User account
- Will protect you from many viruses

112

WiFi: Use a VPN

- VPN: Virtual Private Network
- Encrypts data point to point



113

Review: Protection

- Antivirus software now not needed
- Firewalls already included in Windows
- Keep programs up to date
- Use a Standard User account
 - Not an Administrator account
- Use a VPN for WiFi

114

6. How to Backup Your Data



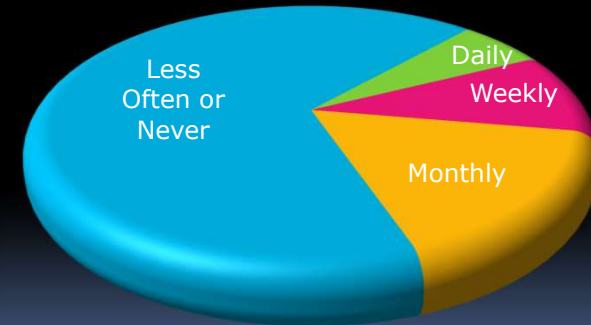
115

I regularly back up my data.

1. True
2. False

116

How Many People Backup?



117

What Is a Backup?

- Copies of your files
- Can be used to replace the originals
 - If the originals are lost or damaged

118

118

Which Files Should I Backup?

- Data files
 - Files you've created or purchased
- Program files

119

119

Where to Back Up Your Data

- External hard drives
 - Connected directly to your PC
- Online (in the "cloud")

120

120

How Often Should You Backup?

- As often as possible
- Must be **Automatic**

121

Backup Software

- PC
 - Assortment of programs
- Mac
 - Time Machine
 - Super Duper
 - Carbon Copy Cloner

122

Check Your Backups

- Try to restore a random file
- At least twice a year
 - When you change your clocks

123

The Best Backup - Summary

- Back up your data – Right now!
- Back up your data automatically
- Check your backups twice a year

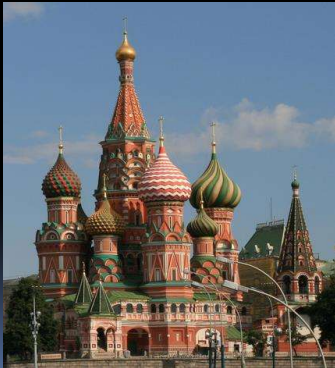
124

7. Simple Solutions



125

The Kremlin in Moscow



Now Using
Typewriters!



126

Are Tablets Immune?

- Mostly, yes
- Protected "ecosystems"
 - Apple's App Store
- But, hackers may eventually invade

127

What about Phones?

- Generally safe
- But major privacy issue:
 - Location monitoring:
 - Google Maps Timeline
 - Apple: Location Services, Significant Locations

128

Is Your Phone Hacked?

- YouTube: [15 Clear Signs Your Phone Was Hacked](#)



129

Chromebooks

- Inexpensive
- Well protected
- Easy to reset



HP Chromebook
14, \$220

130

130

Are Macs Immune?

- Fairly safe, but not perfectly so
- A few attacks so far
- Cross-platform apps vulnerable
 - Adobe Reader & Flash
 - Java
- More viruses to come



131

Mac Users Still Need:

- Good passwords
- Be wary of Phishing attempts
- Data backup



132

Summary



133

Summary – Key Points

- Careless design has made our PCs vulnerable
- **Convenient** is the opposite of **Secure**
- We can access the world
 - But the world can access us
- Arms Race: Hackers only get smarter
- We have to be wary always

134

What To Do:

1. Be wary of any incoming message
2. Use good passwords
3. Update programs
4. Backup important files
5. Be wary of WiFi networks
6. Use: iPad, Chromebook, Mac

135

Security:
As Simple as ABC

Always Be Careful

Rich Malloy
Tech Help Today
Greenwich, CT
203-862-9411
malloy@techhelptoday.com

136