Basic Computer Security

(For the Realistically Insecure)

OPCUG & PATACS

February 16, 2019

Absolutely Secure Computers

Absolutely Secure Computers

HP-35 Scientific Calculator (1972)

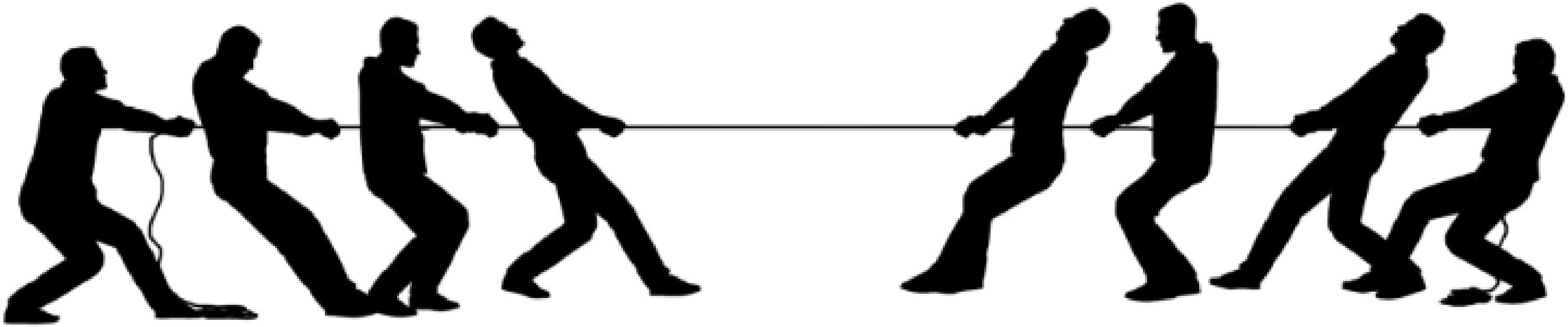
$395—$2,370 in today’s money

Insecure Computers

It’s insecure—if ever attached to the Internet

Computer Security

A never ending tug-of-war



Good Guys / Bad Guys*

Good Guys / Bad Guys*

* Called “hackers” or “black hackers”, i.e., cybercriminals

Good News—Bad News

- **Bad News:** Nothing you can do to make your computer 100% safe
- **Good News:** Reasonable precautions greatly reduce risk of a successful attack
- **More Good News:** Precautions can greatly reduce damage of a successful attack

An Analogy

Fast, savage Cybercriminal

You!

Him

Handout

When Is a Computer Unsafe or Obsolete?

- Computer can’t run essential applications, it’s obsolete
- Computer runs increasingly slow (update to SSD or add RAM?)
- Home computers generally last 5-7 years
- **When the operating system can no longer be updated with security patches—it becomes increasingly unsafe**

Handout

When Is a Computer Obsolete or Unsafe? (cont.)

- Microsoft ⓘ ← External link, click here
  - Windows XP and Vista no longer supported
  - Historically Microsoft has supported Windows for 10 years from date of introduction
  - Windows 10 version 1809 introduced October 2, 2018—end of service April 14, 2020 (2.5 years)
    - Original release caused deletion of files in the Documents folder under some circumstances
    - Version 1809 re-released on November 13, 2018

H
a
n
d
o
u
t

When is a Computer Obsolete or Unsafe? (cont.)

- Apple ⓘ
  - Hardware service ceases for products 5 to 7 years after manufactured
  - Security and serious bug-fix updates provided for about two years after hardware support ceases
  - For details see ⓘ
- **Two years after hardware service stops, you should consider replacing the computer**

Handout

Malware* Bad Guys Distribute

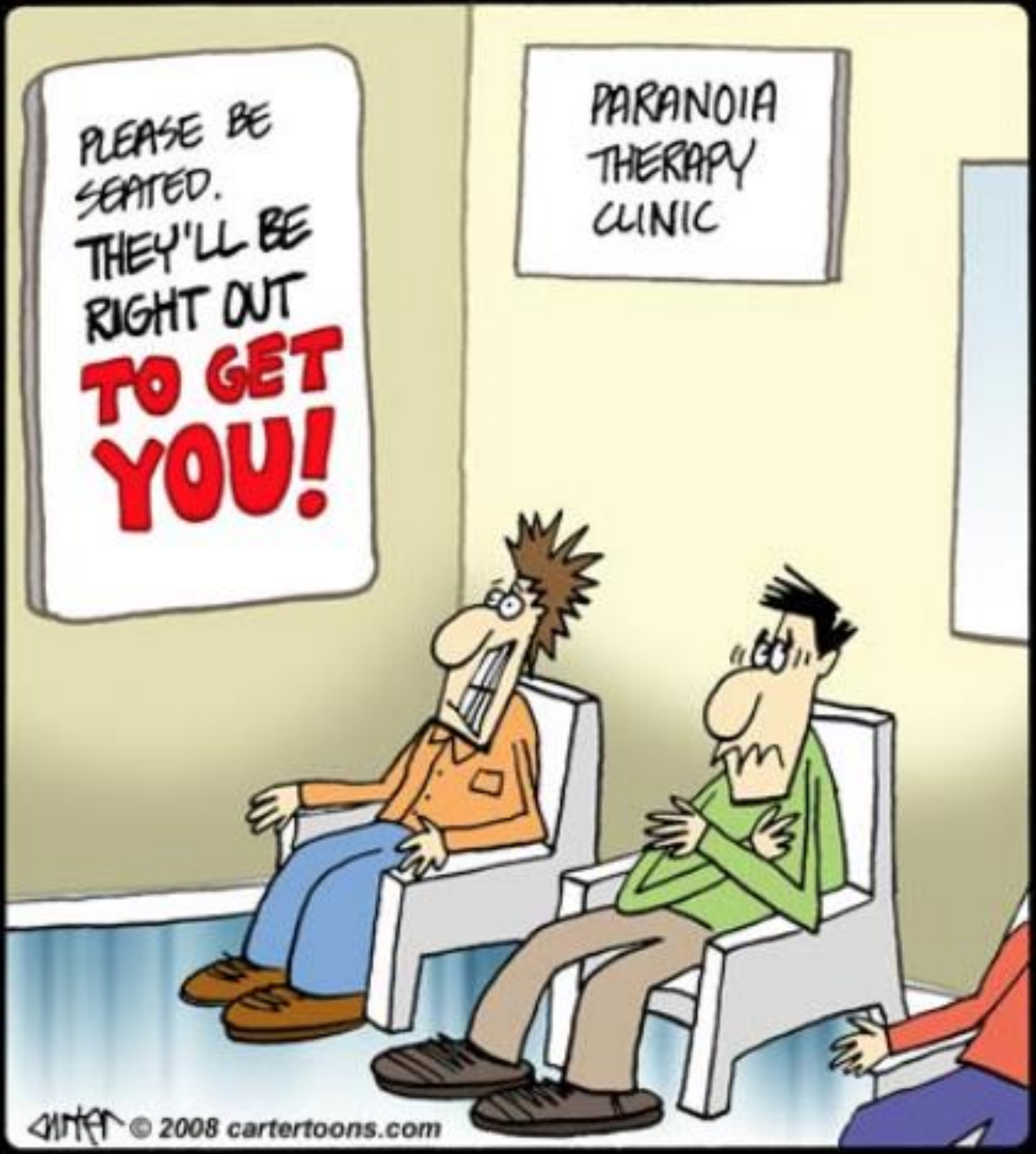
- **Keyloggers (capture IDs/passwords and other data)**
- **Ransomware (encrypt files and demand money)**
- **Store and distribute pornography**
- Viruses (self replicating—corrupt or destroy data)
- Trojan horses (disguised legitimate software)
- Worms (self replicating—spread to other computers)
- Rootkits (gain unauthorized computer access)
- Botnets (network of computers covertly controlled)
- **See the FBI at** ⓘ
- **File a complaint with the FBI at** ⓘ
- **See Krebs-on-Security and Malwarebytes** ⓘ ⓘ

*** Malware is software that damages computers or files, captures private information, and other criminal behavior**

“Agent Tesla” Infestation

- “In the wild” since 2014, probably developed and based in Turkey ⓘ ⓘ ⓘ
- Keylogger—can be imbedded and distributed in images, text, audio and Microsoft Office files
- Can extract information (IDs, passwords, etc.) from
  - Browsers
  - E-mail
  - Sessions with Instagram, Twitter, Gmail, Facebook, etc.
- Microsoft Windows only

Feeling paranoid?


PLEASE BE SEATED. THEY'LL BE RIGHT OUT TO GET YOU!
PARANOIA THERAPY CLINIC
© 2008 cartertoons.com

Symptoms of Malware Infestation

- Strange computer behavior ⓘ ⓘ ⓘ ⓘ
  - Computer slow down
  - Problems connecting to networks
  - Freezing or crashing
  - Lack of storage space
  - Observe modified or deleted files
  - Programs running, turning off, or reconfiguring themselves
  - **Appearance of strange files, programs or desktop icons**
- Many infestations can be asymptomatic

But…what can I do?

There is software that can prevent malware installation—detect & remove

H
a
n
d
o
u
t

Backup—First Line of Defense

- **Badly hacked computers are easiest restored from backup**
- Minimum of two external backup disks
  - One attached to computer for hourly/daily backup
  - One or more <u>not attached</u> and in a safe location
- Learn to use backup software and conduct recovery “fire drills”
- Backup software
  - Windows computers—Backup and Restore function
  - Mac computers—Time Machine
- Numerous third party backup software available

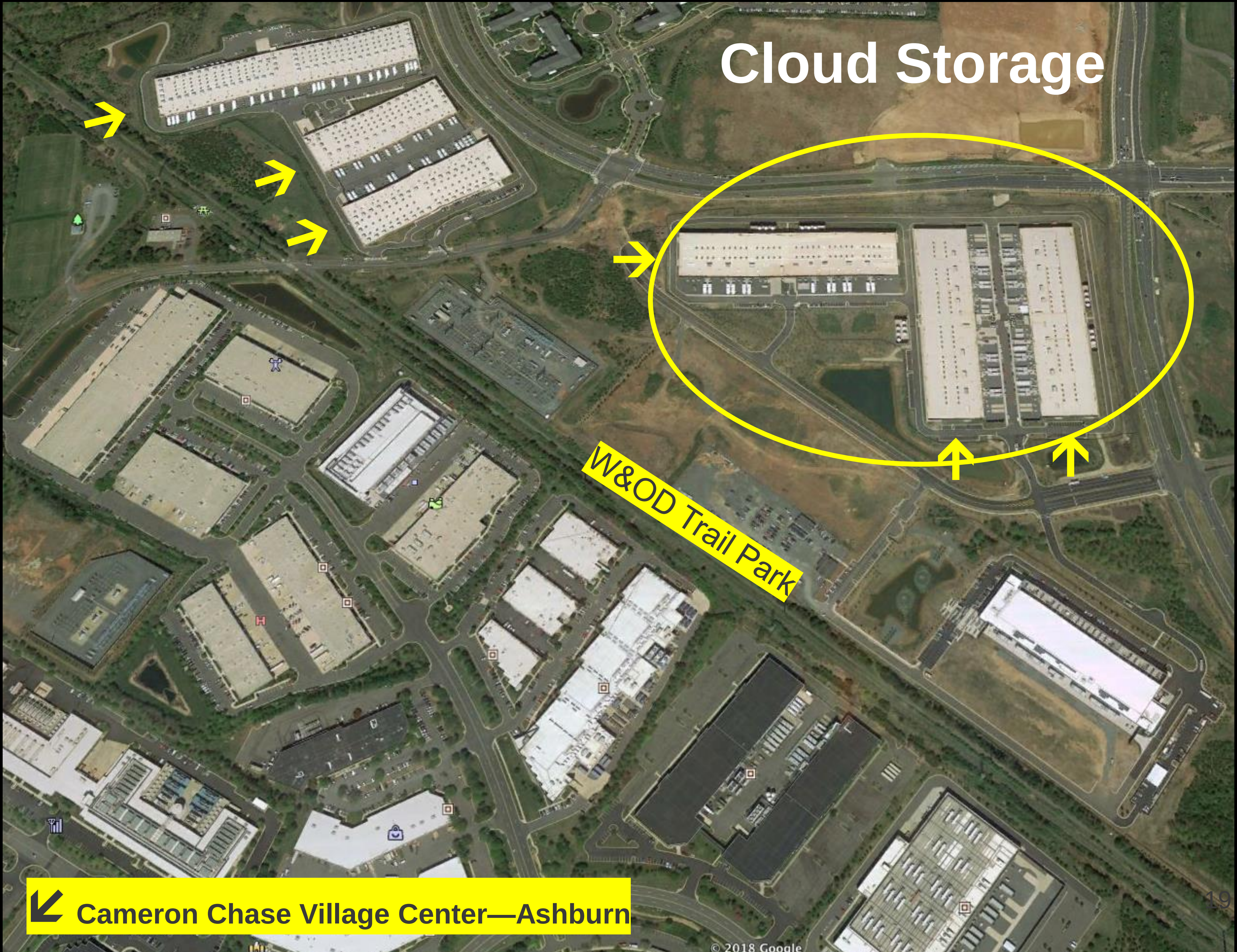
Cloud Backup

- **Cloud Computing:** a network of remote computers (hosted on the Internet) to store, manage, and process data
- **Cloud Backup:** software on your computer to systematically backup files “to the Cloud”
- **Cloud Storage:** acts like a disk drive attached to your computer

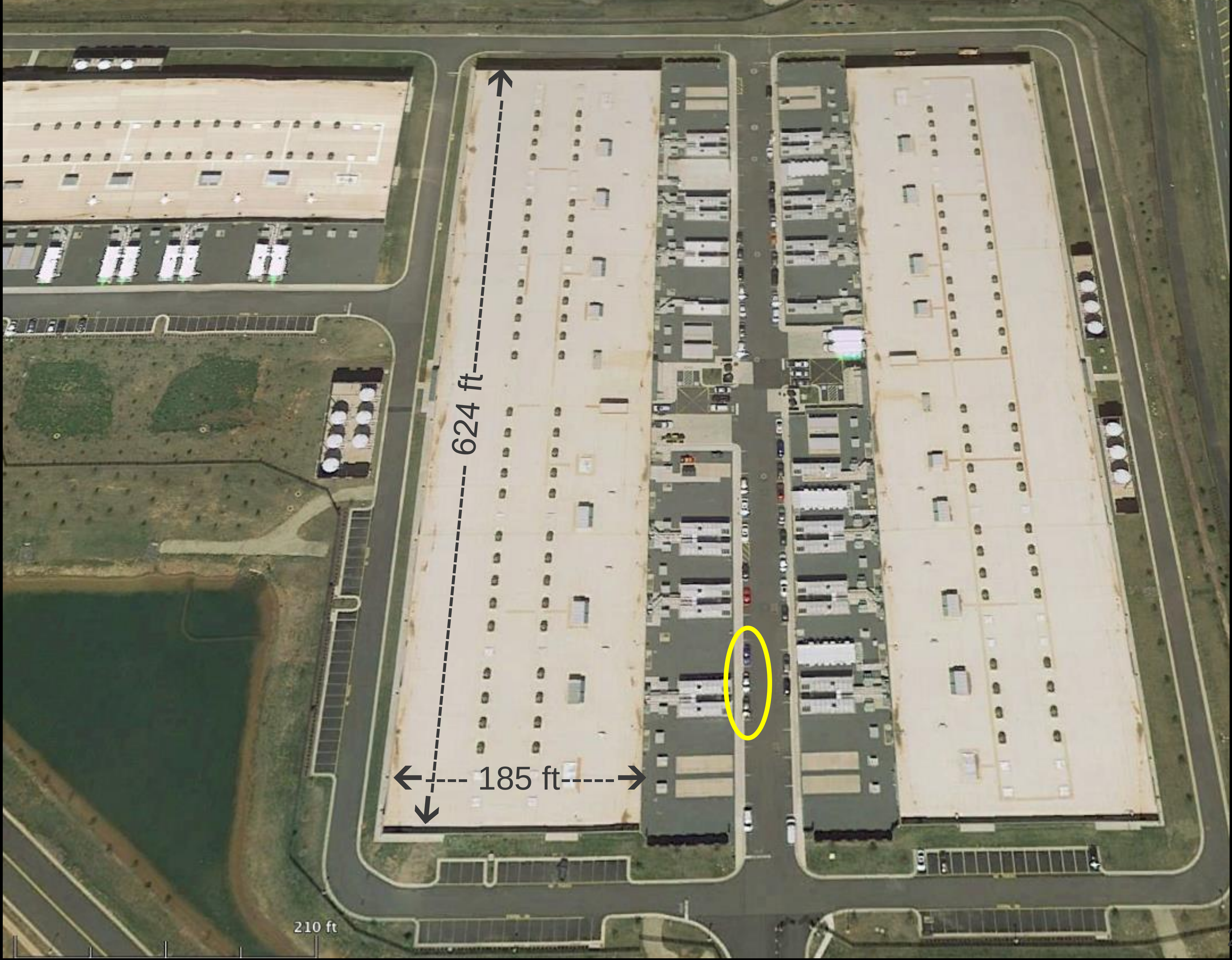
Cloud Storage?

Your files aren’t here

Cloud Storage



↙ **Cameron Chase Village Center—Ashburn**


624 ft
185 ft
210 ft

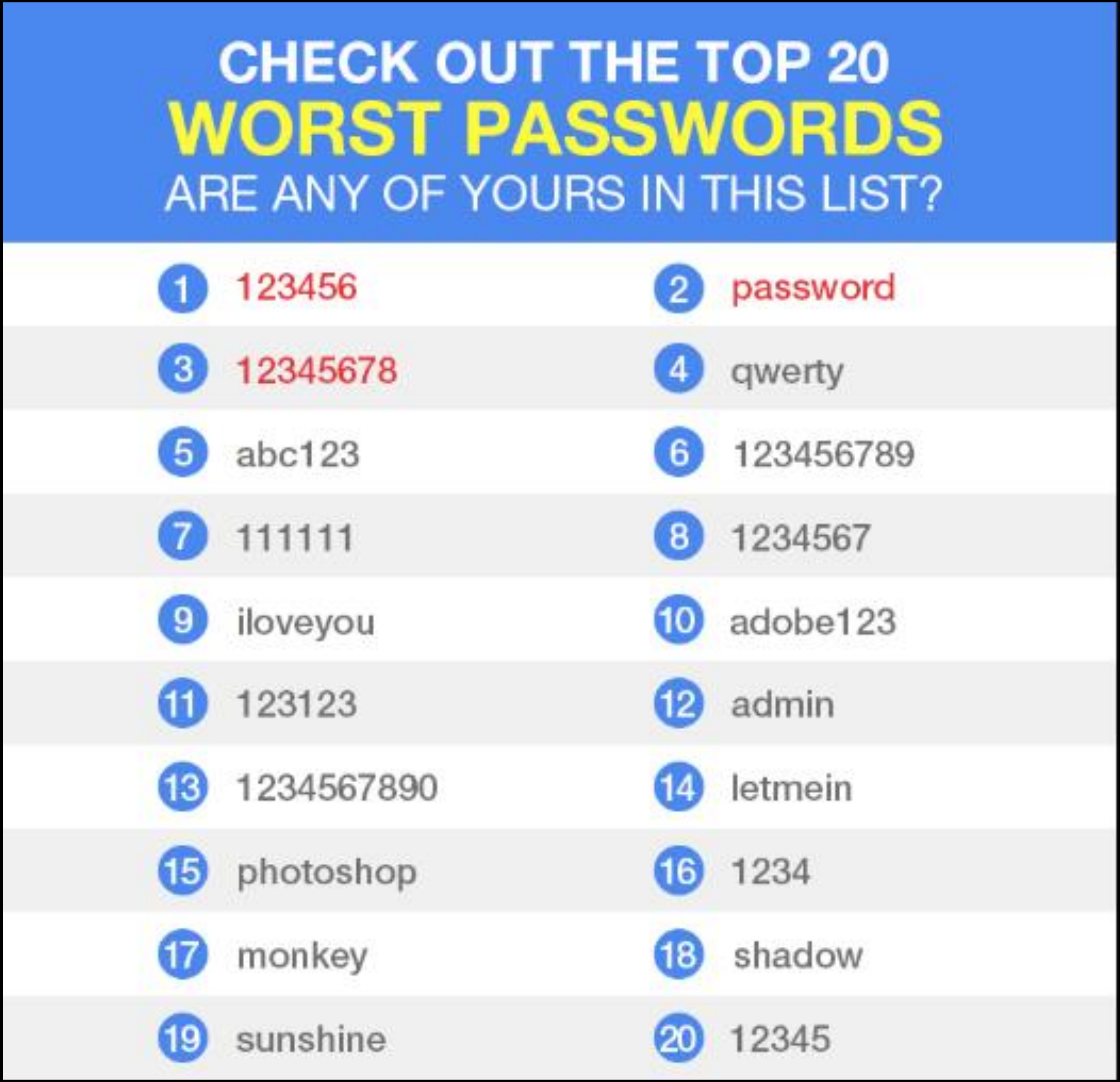
Handout

Cloud Backup—Factors to Consider

- Price
- Your Internet speed
- Cloud storage can be malware contaminated
- Time to recover data
- Security
  - End to end encryption?
  - Stored encrypted?
  - Location of Cloud storage?
- Ease in setting up and using
- Trustworthiness and stability of provider
- Numerous companies offer Cloud backup

A good Learn-in-Thirty Presentation Volunteer?

You still can’t take it with you… but we do offer Cloud storage for your computer



CHECK OUT THE TOP 20 WORST PASSWORDS

ARE ANY OF YOURS IN THIS LIST?

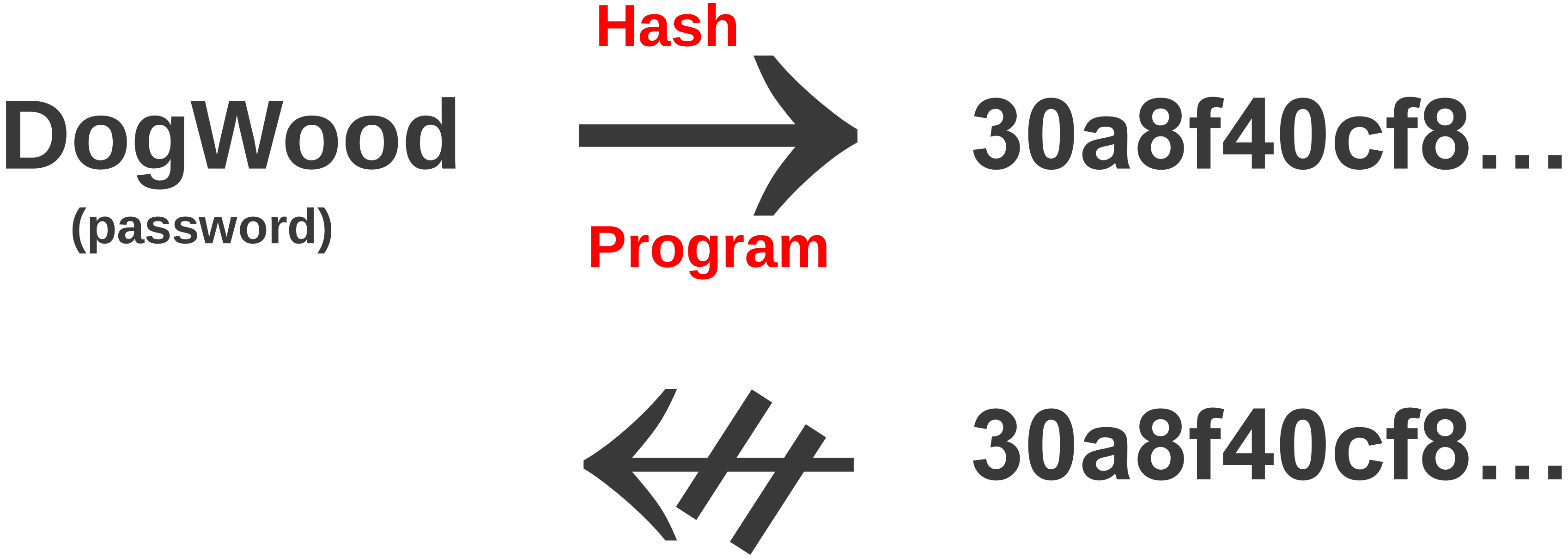
1. 123456
2. password
3. 12345678
4. qwerty
5. abc123
6. 123456789
7. 111111
8. 1234567
9. iloveyou
10. adobe123
11. 123123
12. admin
13. 1234567890
14. letmein
15. photoshop
16. 1234
17. monkey
18. shadow
19. sunshine
20. 12345

Why can’t you use
“Beef Stew” as a password

It isn’t Stroganoff

Hashing

Password Hashing



DogWood

(password)

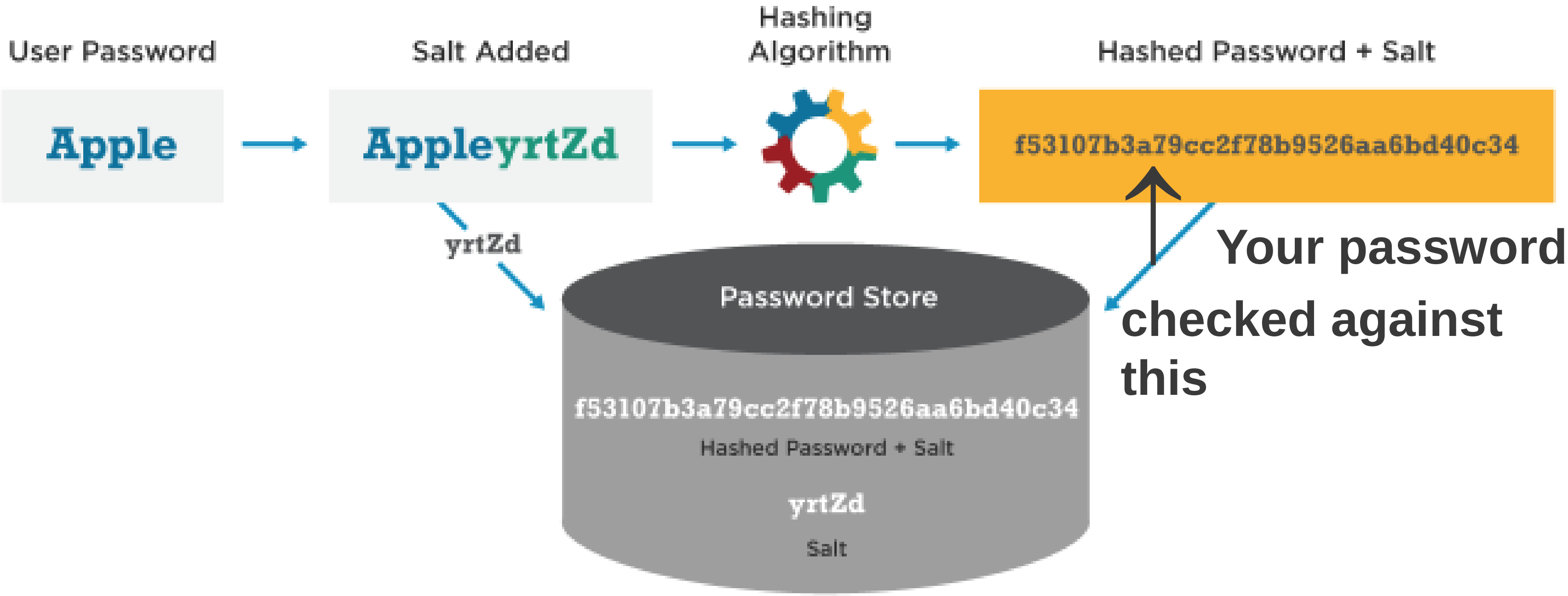
Hash

Program

30a8f40cf8…

30a8f40cf8…

Password Hashing & Storage

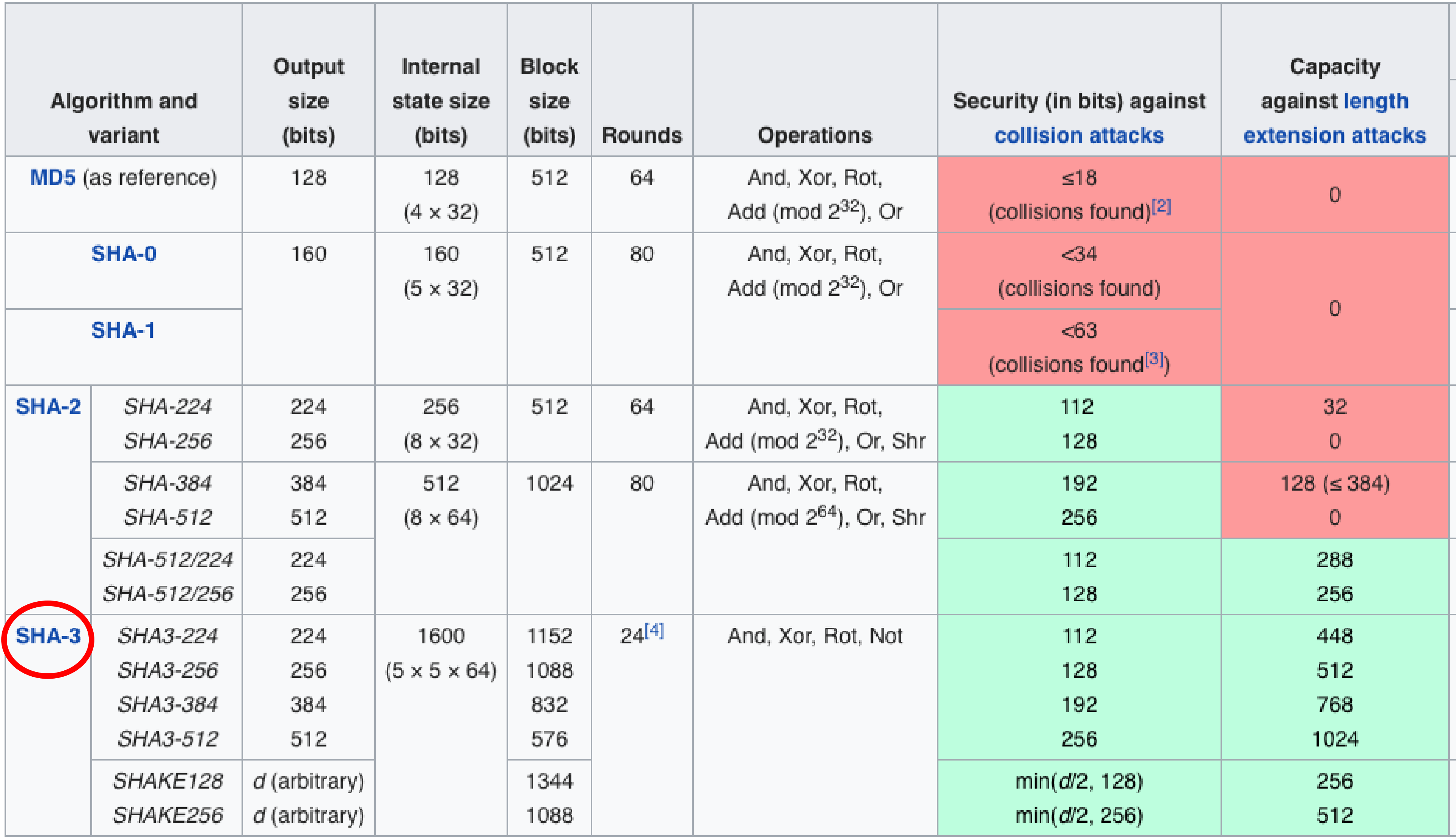


Your password checked against this

Hashing Algorithms ⓘ ⓘ ⓘ ⓘ

- MD5 (insecure and obsolete)
- SHA family (created by NSA)
  - SHA 0 (insecure and obsolete)
  - SHA 1 (insecure and obsolete)
  - SHA 2 (used by Bitcoin)
  - SHA 3 (current and latest)
- bcrypt (encrypting passwords)
- PBKDF2 (encrypting passwords)
- Argon 2
- RIPMD-160
- Whirlpool
- BLAKE 2

Comparison of SHA Functions



Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Rounds	Operations	Security (in bits) against collision attacks	Capacity against length extension attacks
MD5 (as reference)		128	128 (4 × 32)	512	64	And, Xor, Rot, Add (mod 2^{32}), Or	≤18 (collisions found)[2]	0
SHA-0		160	160 (5 × 32)	512	80	And, Xor, Rot, Add (mod 2^{32}), Or	<34 (collisions found)	0
SHA-1							<63 (collisions found[3])	
SHA-2	*SHA-224* *SHA-256*	224 256	256 (8 × 32)	512	64	And, Xor, Rot, Add (mod 2^{32}), Or, Shr	112 128	32 0
	SHA-384 *SHA-512*	384 512	512 (8 × 64)	1024	80	And, Xor, Rot, Add (mod 2^{64}), Or, Shr	192 256	128 (≤ 384) 0
	SHA-512/224 *SHA-512/256*	224 256					112 128	288 256
SHA-3	*SHA3-224* *SHA3-256* *SHA3-384* *SHA3-512*	224 256 384 512	1600 (5 × 5 × 64)	1152 1088 832 576	24[4]	And, Xor, Rot, Not	112 128 192 256	448 512 768 1024

	SHAKE128
	SHAKE256
		d (arbitrary)
		d (arbitrary)
				1344
				1088
							min(*d*/2, 128)
							min(*d*/2, 256)
								256
								512

Where Are Hashed Passwords Stored?

- Windows 10
  - Location: C:\Windows\System32\config\ in folders like ‘SAM’ and ‘SYSTEM’
  - Hash Algorithm*: MD4 ➔ AES128
- macOS
  - Location: /var/db/dslocal/nodes/Default/users/username.plist
  - Hash Algorithm: PBKDF-2 ➔ AES512

Don’t mess with this!

*** MD4 is obsolete and insecure**

Password Best Practices

- Minimum length of 10-12 mixed characters
  - Example #1: #$Animal89Donut
  - Example #2: Lo=ve?Lamp7Avoxtur+Snake
- Passphrases easier to remember
  - Example #3: 011235BuckleMySneaker&&&
- ~aK8=l+bdk:>?$56ZMe]|?719znM (NOT easy to remember)
- Combine mixed languages, English with Latin or Icelandic, Welsh, etc.
- Don’t use a password more than once
- Periodically change passwords (controversial)

Handout

Password Best Practices (cont.)

- Don’t store unencrypted passwords on computer
- **Seriously** consider using a password manager
  - Generates long, random passwords
  - **Essential** to select strong “master” password
- Use two-factor authentication for the most sensitive accounts
- Biometrics soon to replace passwords in many applications (fingerprint, face & iris recognition)
- 10,000 most common passwords ⓘ
- Also see: ⓘ ⓘ ⓘ ⓘ

Anti-malware Software*

H
a
n
d
o
u
t

- Protects against multiple types of attack
- Some companies offer free or trial products
- Removal of anti-malware software can be challenging
  - License software that comes with a removal tool
  - Select a product and stay with it
  - Don't use more than one anti-malware software concurrently
- Numerous companies license anti-malware software (license subscriptions)
  - Kaspersky is a Russian company based in Moscow
  - Windows 10 Defender comes with Windows 10

*** Preventive action and clean up**

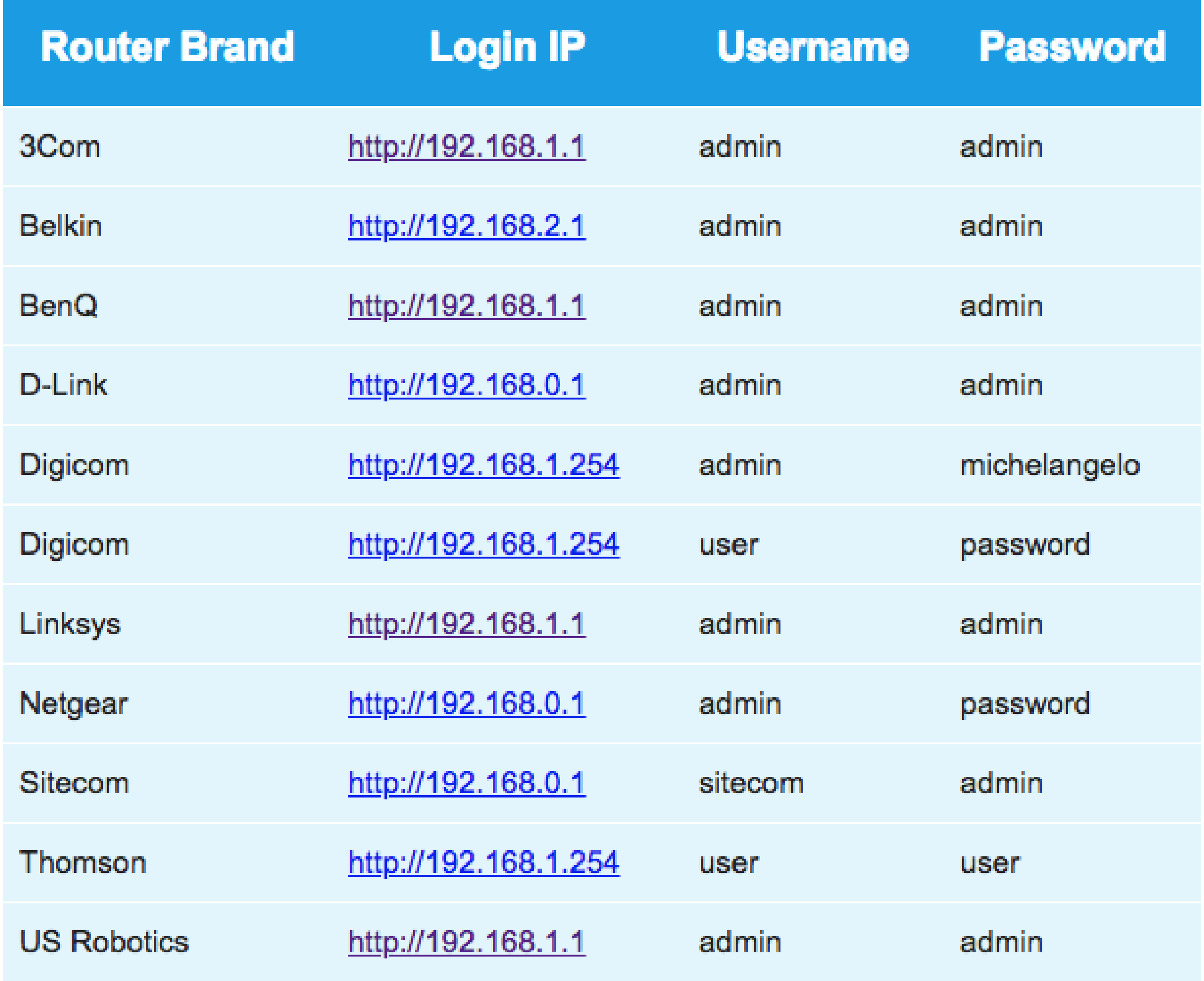
Anti-malware Software (cont.)

- **Anti-malware software is essential for computers using Microsoft Windows**
- Many (most?) users of Apple computers do not install anti-malware software

H
a
n
d
o
u
t

Internet Discipline

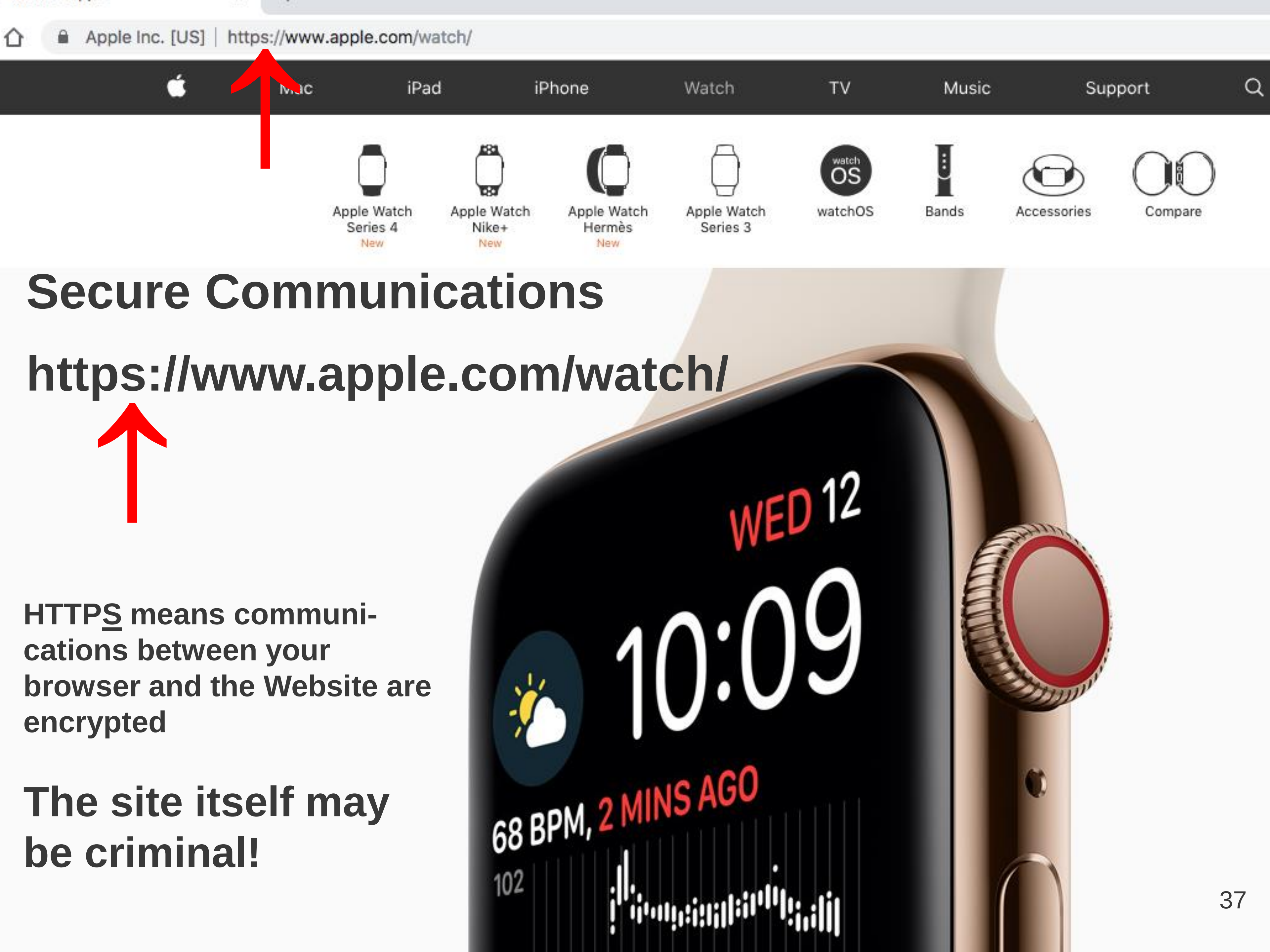
- **Change the admin password on your router or modem**
- Use only secure communications when sending or seeking sensitive information on the Web
- Be wary of using public Wi-Fi
  - At public libraries, restaurants, airports, etc.
- **Do not use public Wi-Fi for banking, purchasing, sensitive communications, etc.**
- Public Wi-Fi can be safe with Virtual Private Networking (VPN)



Router Brand	Login IP	Username	Password
3Com	http://192.168.1.1	admin	admin
Belkin	http://192.168.2.1	admin	admin
BenQ	http://192.168.1.1	admin	admin
D-Link	http://192.168.0.1	admin	admin
Digicom	http://192.168.1.254	admin	michelangelo
Digicom	http://192.168.1.254	user	password
Linksys	http://192.168.1.1	admin	admin
Netgear	http://192.168.0.1	admin	password
Sitecom	http://192.168.0.1	sitecom	admin
Thomson	http://192.168.1.254	user	user
US Robotics	http://192.168.1.1	admin	admin

Verizon uses ActionTec routers
Cox uses Netgear routers

Handout



Secure Communications

https://www.apple.com/watch/

HTTPS means communications between your browser and the Website are encrypted

The site itself may be criminal!

User Account Best Practices

- Windows 10—user accounts
  - Administrator (a single account)
  - **Standard** (each user)
  - Guest (earlier versions of Windows)
- Apple macOS—user accounts
  - Admin (a single account)
  - **Standard** (each user)
  - Guest User (set to off)

Handout

Firewalls—Turn Them On!

- **Router or modem firewall**
- Windows 10 computer
  - Control Panel ➔ System and Security ➔ Windows Firewall ➔ [select] Turn Windows Firewall **ON**
- Apple macOS computer
  - System Preferences ➔ Security and Privacy ➔ Firewall [set to **ON**)

Can I interest you in a Firewall for your toaster?

H
a
n
d
o
u
t

E-Mail Best Practices

- E-mail messages—on a huge party-line
- E-mail—equivalent to a written document
- Don’t click on links in e-mail messages unless you know the sender; even then be cautious
- Be wary of short or abnormal looking e-mail messages prompting you to “click here” or ask you to respond
- Banks, Microsoft, Apple and most legitimate merchants will not ask for personal information via e-mail

Handout

E-Mail Best Practices (cont.)

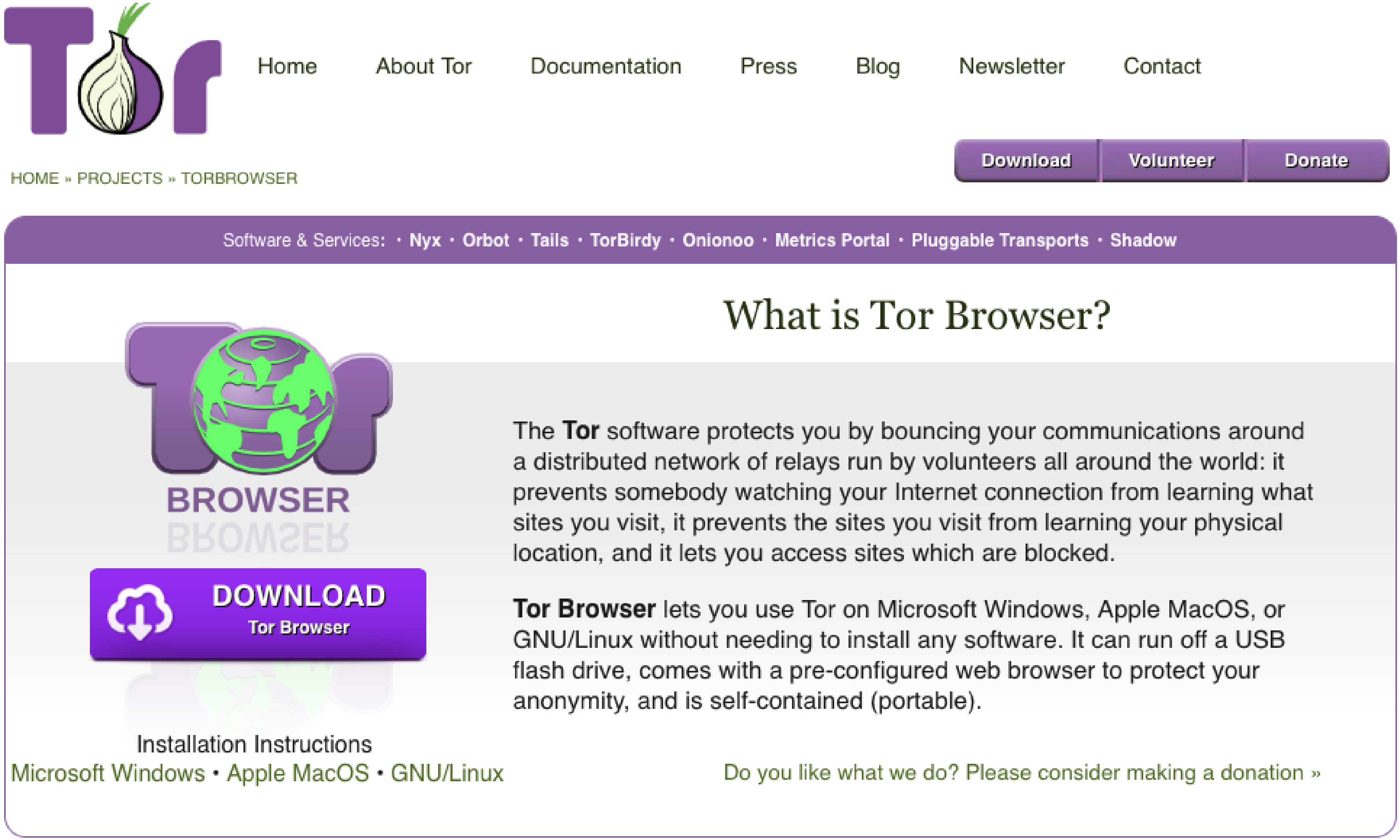
- When sending a message to groups, use BCC field rather than TO or CC fields
  - Some individuals may not wish to share their e-mail address with the group
  - Including e-mail addresses in TO and CC fields increases risk of capture of these addresses
  - In replying to group messages, reply to ALL sparingly—replying only to the sender is best
- Establish a throw-away e-mail address
- Use 10MinuteMail (https://10minutemail.com) ⓘ
- Secure e-mail systems are available, but generally complex to install and use

Browser Discipline

- Most common Web browsers:
  - Firefox
  - Google Chrome
  - Microsoft Edge
  - Safari
- Have two or more browsers
- Do not have browsers remember passwords*
- When accessing a questionable site, use “private” mode (incognito or InPrivate)
- If you access a site that looks fishy, **STOP and “kill” the browser session**

*** Passwords saved in browsers are insecure**

Get the Tor browser here → ⓘ


Home
About Tor
Documentation
Press
Blog
Newsletter
Contact
Download
Volunteer
Donate
HOME » PROJECTS » TORBROWSER
Software & Services: · Nyx · Orbot · Tails · TorBirdy · Onionoo · Metrics Portal · Pluggable Transports · Shadow
BROWSER
DOWNLOAD
Tor Browser

What is Tor Browser?

The **Tor** software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.

Tor Browser lets you use Tor on Microsoft Windows, Apple MacOS, or GNU/Linux without needing to install any software. It can run off a USB flash drive, comes with a pre-configured web browser to protect your anonymity, and is self-contained (portable).

Installation Instructions
Microsoft Windows • Apple MacOS • GNU/Linux

Do you like what we do? Please consider making a donation »

Search Services & Privacy

Handout

- Google (87.28% market share in U.S.)
- Bing (6.91%)
- Yahoo (4.65%)
- DuckDuckGo* (0.59%)
- Others (0.57%)

*** Mindful of privacy**

Periodic Computer Maintenance

- Perform *weekly* or biweekly (5-10 minutes)
- Check for operating system updates and security patches (Windows or macOS)
  - If possible delay OS installations 2-4 weeks
- Check for updates for your applications
  - Microsoft Office
  - Browsers
  - Anti-malware software
  - Flash
  - Programs/apps commonly used
- Perform a manual backup
- Exchange backup disks—then perform manual backup

H
a
n
d
o
u
t

Where to Get Help & Computer Repair

- Grandchildren or children
- Apple/Microsoft Stores
- Apple itself
- Advanced 2000
- Computer Repair Fairfax
- Fairfax Computer Repair
- Geek Squad (Best Buy)
- iFixIt (help for do-it-yourself)
- Keystone Computer
- Micro Center (PCs and Macs)
- TCS Computer
- uBreakiFix

User Groups' Clinics

No endorsement given or implied

Fixed it!

Thanks for listening!

A Video: Password Cracking

- Dr. Mike Pound, Assistant Professor, University of Nottingham ⓘ
- 40 billion hashed passwords checked per second
- 60-70% of 6,500 passwords revealed while making the video
- Using a program called CudaHashCat on a Linux-based computer that costs ~$5,000
- Going to 2.5 year-old video… ⓘ