A presentation by Albert Wang
Systems Administrator Lead
SHASS Dean's Office
02/07/2019

Safe Computing @MIT

What everyone needs to know

SHASS IT

○ This presentation can be found on the SHASS IT website under "IT Documentation" at shassit.mit.edu

○ https://wikis.mit.edu/confluence/display/shassit/SHASS+IT+Documentation+Home

○ Under both "Getting Started" and "Preventative Maintenance and Security" sections

Email

- Important: MIT will *NEVER* ask you for your password, nor will MIT send you email requesting your password or other confidential information.
Please delete all email messages that request such information. They are social engineering scams designed to steal your information.

- These social engineering scams are called "PHISHing".

- The above applies to telephone calls as well. (telemarketing, Nigerian 419, phishing, 809 scam, etc)
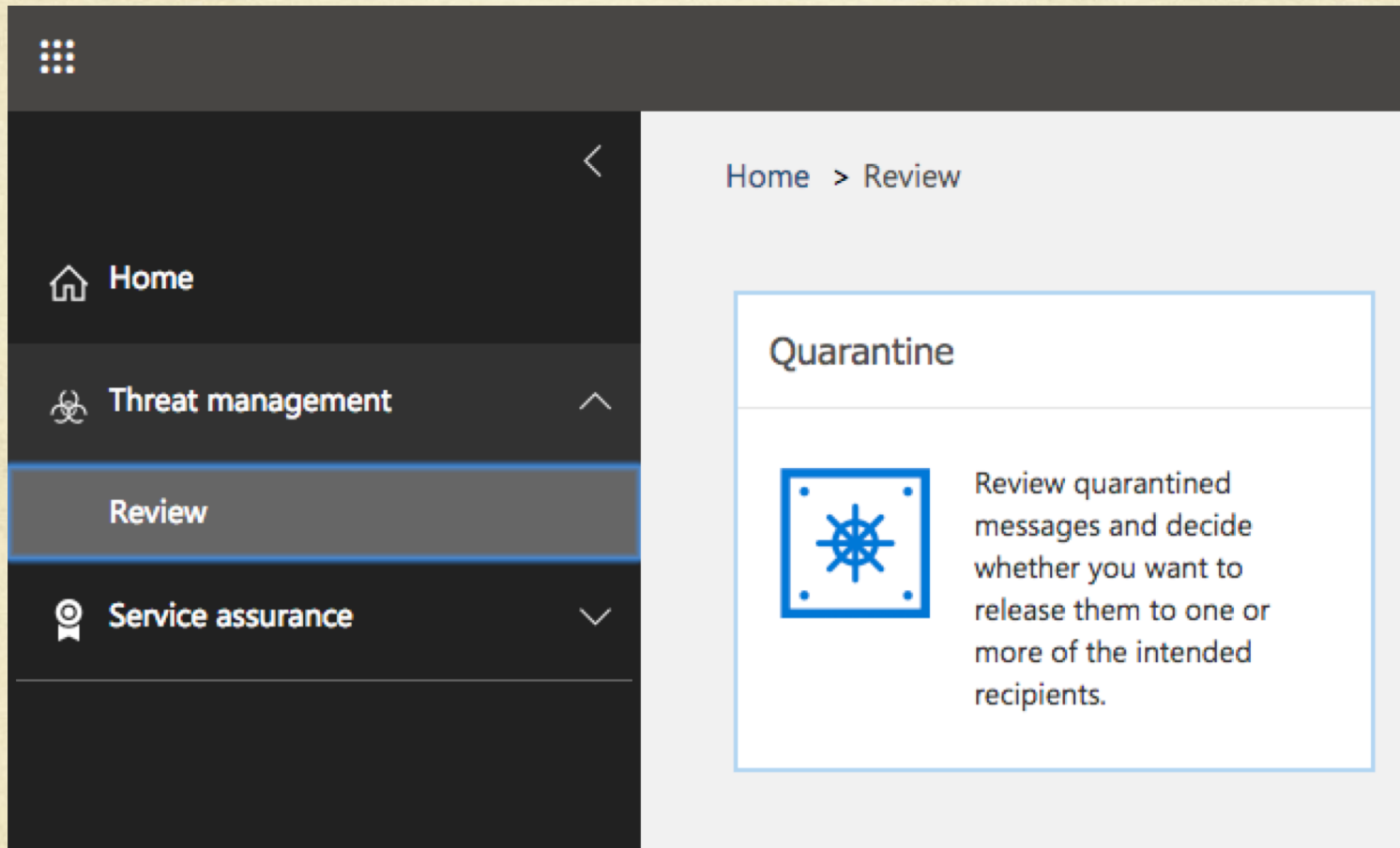
Spam

○ **Spam** is the use of electronic messaging systems to send unsolicited bulk messages, especially advertising, indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media.

○ MIT Anti-Spam Resources: http://ist.mit.edu/spam

○ In January 2019, IS&T Changed the way Spam Quarantine works: https://kb.mit.edu/confluence/pages/viewpage.action?pageId=159393284

Checking Spam Quarantine

- https://protection.office.com/

- If you are not already logged in to MIT's Office 365, you will be prompted to sign in.

- Enter your @mit.edu email address

- Click "Next"

- Click "Work or school account"

- You will be taken to Touchstone@MIT to log in.

- Once you're logged in, your filtered messages are found under Threat Management -> Review -> Quarantine

- Please note there are 2 categories present that you will need to review: Spam and Bulk. The email notices you receive only tell you what's in Spam.

Review: Quarantine

Review: Bulk and Spam

Why use Spam Quarantine?

- Spam Quarantine is better than any email client program (Apple Mail or Outlook) spam filtering because it stops the spam BEFORE it gets to your Inbox.

- Emails caught in Spam Quarantine do not count against your email quota.

- If you ever need to use Exchange webmail at owa.mit.edu, all the Spam captured by the new O365 Spam Quarantine applies there as well.

- Spam Quarantine is free and currently running.

- Instructions for how to use it are located on the SHASS IT Website in "SHASS IT Documentation" under "Getting Started" and "Preventative Maintenance and Security".
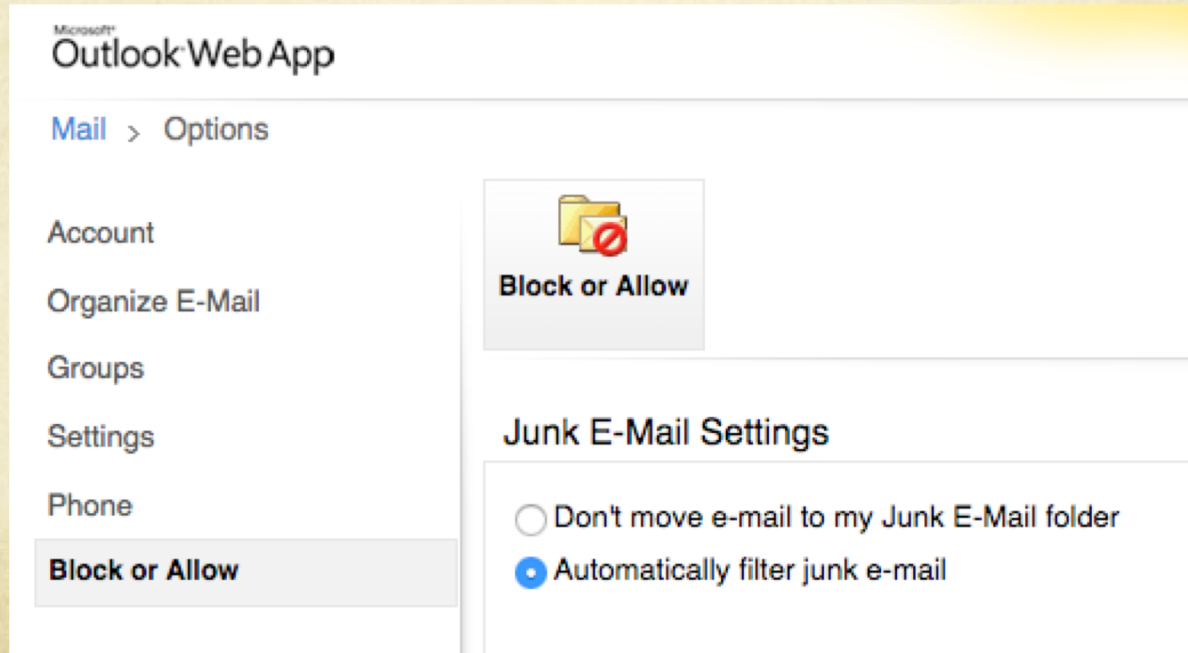
How to create a black/white list

○ You have go to owa.mit.edu

○ "Options" (upper right)-> "See all options"
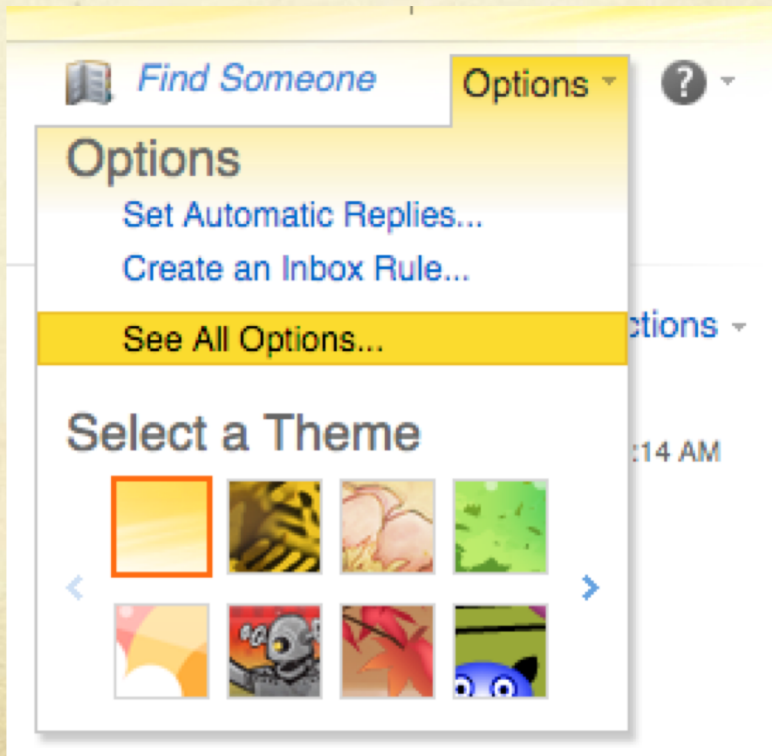
How to create a black/white list

○ "Block or Allow" (left nav bottom)

○ Make sure the Automatically filter junk email radio button is selected

How to create a black/white list

- White listed recipients can be added to "safe senders and recipients," and denied senders added to "blocked senders."

Attachments

○ Never open attachments from people you don't know.

○ Never open attachments from people you do know but weren't expecting an attachment from. Delete the email immediately.

○ Attachments (some examples: pdf, doc, jpg, exe, zip, gzip) are used as Trojan horses by bad people to deliver bad stuff like viruses, malware, and root kits.

○ If in doubt, email the sender to verify the attachment is legit.

Bad Stuff

○ **Viruses**- A computer virus is a computer program that can replicate itself and spread from one computer to another.

○ **Malware**- Short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

○ **Rootkit**- A stealthy type of software, often malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.

Free software

- Everybody loves the idea of free software.

- The only problem is the bad guys know this.

- The guise of free software is another common delivery device for bad stuff (malware, viruses, and rootkits).

- Free software is the most common delivery vehicle for bad stuff. So if your Mac or Windows asks you if you want to open or install any application you aren't sure about, always say NO.

Safe 'free' software

○ Legitimate shareware and freeware do exist, but Google them if you're not familiar to verify their authenticity. See what people are talking about.

○ Anything published directly from official software sites or the IS&T Software Download page is safe.

○ Some very good anti-malware and anti-virus programs are free and safe.

○ When in doubt, ask either Dan or myself.

What once was safe...

○ CNET's downloads.com used to be a safe place to download free software. Unfortunately, the bad guys knew this too.

http://www.howtogeek.com/198622/heres-what-happens-when-you-install-the-top-10-download.com-apps/

Online app stores

○ Apple rigorously vets all of their apps. Sometimes overly so.

○ Microsoft vets nothing. Caveat emptor.

○ Google tries to vet its apps but often fails.
  https://www.wired.com/story/google-play-store-malware/

Anti-Bad Stuff software

- Have one or two that you use. At MIT on work machines, Sophos is the one to use.

- Great free options. (Spybot S&D, Super AntiSpyware, Malwarebytes for Win) (ClamXAV, Avast!, Malwarebytes for Mac)

- Update it. Use it once in a while.

- Everyone at MIT should be using Sophos on their work machines. No one should be running McAfee at this point.
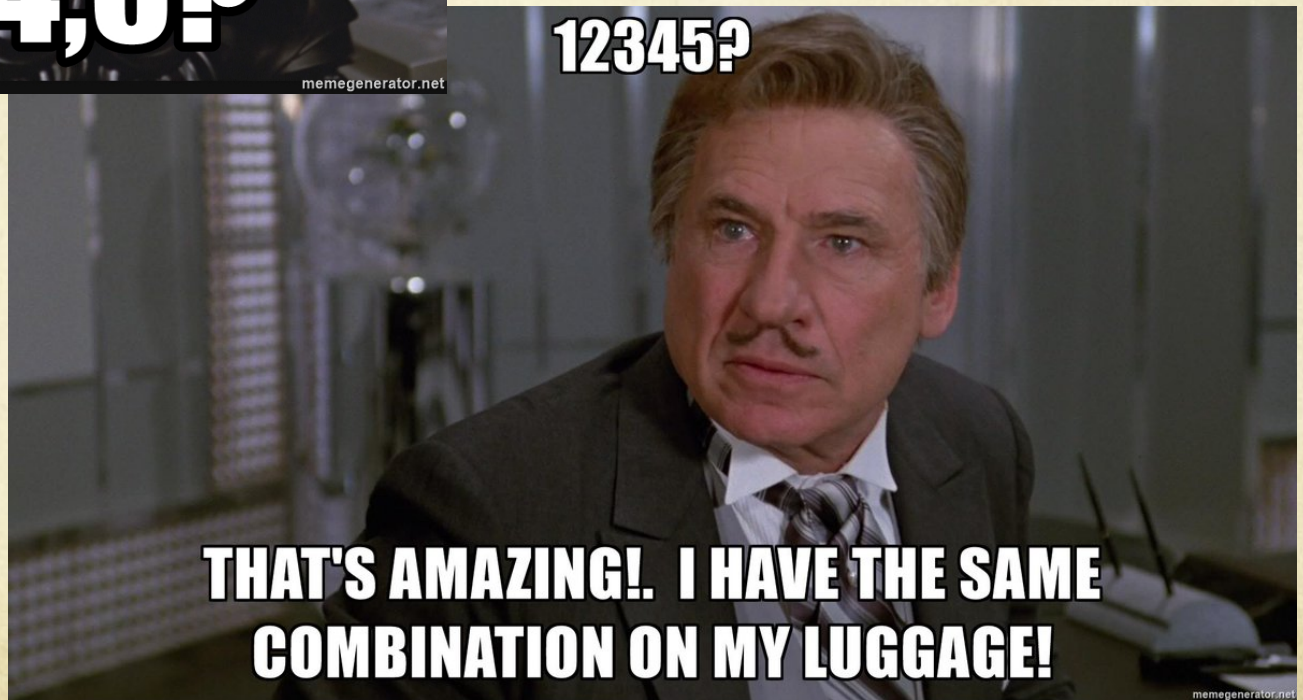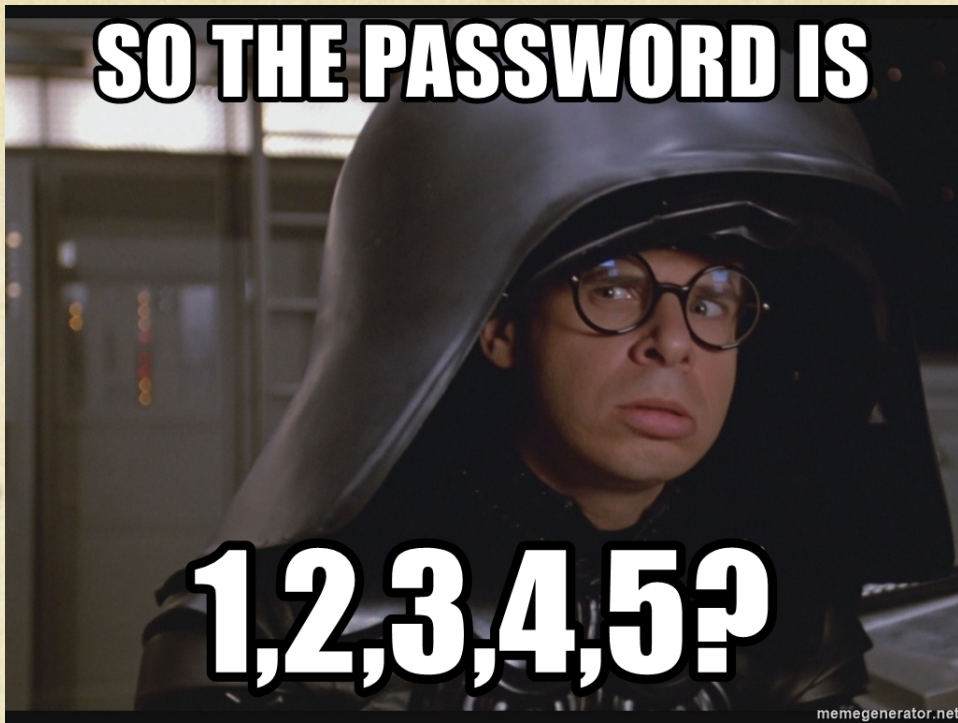
Passwords

- According to the password management company SplashData, here are the 25 most common stolen passwords of 2013, along with the change in rank from last year.

- **1 123456** (*Up 1*), **2 password** (*Down 1*), **3 12345678** (*Unchanged*), **4 qwerty** (*Up 1*), **5 abc123** (*Down 1*), **6 123456789** (*New*), **7 111111** (*Up 2*), **8 1234567** (*Up 5*), **9 iloveyou** (*Up 2*), **10 adobe123** (*New*), **11 123123** (*Up 5*), **12 admin** (*New*), **13 1234567890** (*New*), **14 letmein** (*Down 7*), **15 photoshop** (*New*), **16 1234** (*New*), **17 monkey** (*Down 11*), **18 shadow** (*Unchanged*), **19 sunshine** (*Down 5*), **20 12345** (*New*), **21 password1** (*Up 4*), **22 princess** (*New*), **23 azerty** (*New*), **24 trustno1** (*Down 12*), **25 000000** (*New*)
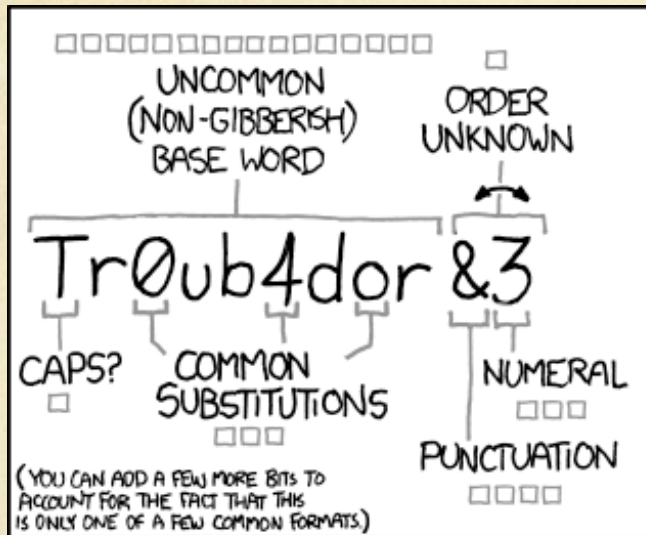
Passwords

○ For 2018, the 25 most stolen passwords:

1. 123456 (Unchanged) **2. password** (Unchanged) **3. 12345678** (Up 1) **4. qwerty** (Up 1) **5. 12345** (Down 2) **6. 123456789** (Unchanged) **7. football** (Up 3) **8. 1234** (Down 1) **9. 1234567** (Up 2) **10. baseball** (Down 2) **11. welcome** (New) **12. 1234567890** (New) **13. abc123** (Up 1) **14. 111111** (Up 1) **15. 1qaz2wsx** (New) **16. dragon** (Down 7) **17. master** (Up 2) **18. monkey** (Down 6) **19. letmein** (Down 6) **20. login** (New) **21. princess** (New) **22. qwertyuiop** (New) **23. solo** (New) **24. passw0rd** (New) **25. starwars** (New)

What is a good password?

○ Back ten years ago, eight characters or longer was pretty good. Today, 16 or longer is best.

○ Mixed case (lower and upper case letters), with a number, and a symbol to maximize the amount of time cracking programs will take to figure out the password.

○ Something you'll easily remember.

○ Eg. Whyisevery1Iknowwatchinggameofthrones? Inanthroareyoumysteryorsciencefiction? Fortunethehappydogsmilesatme2day! Makewayforskippypeanutbutterducklingsinboston! correcthorsebatterystaple

○ If you have to write it down, it's not a good password.

What's easy to remember and hard to hack?
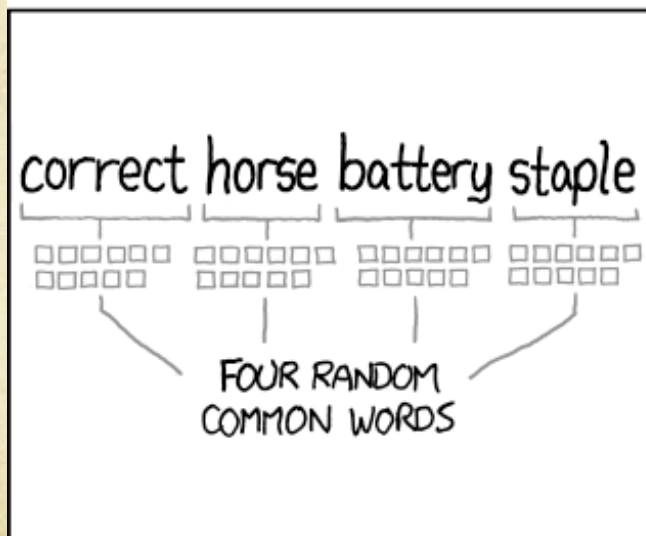
How fast can a password be cracked?

- In 2013, Hackers cracked 16-character passwords in less than an HOUR

- During an experiment for Ars Technica one hacker managed to crack 90% of 16,449 hashed passwords

- Six passwords were cracked each minute including 16-character versions such as 'qeadzcwrsfxv1331'

- http://www.dailymail.co.uk/sciencetech/article-2331984/Think-strong-password-Hackers-crack-16-character-passwords-hour.html

Time to crack a password vs technology type
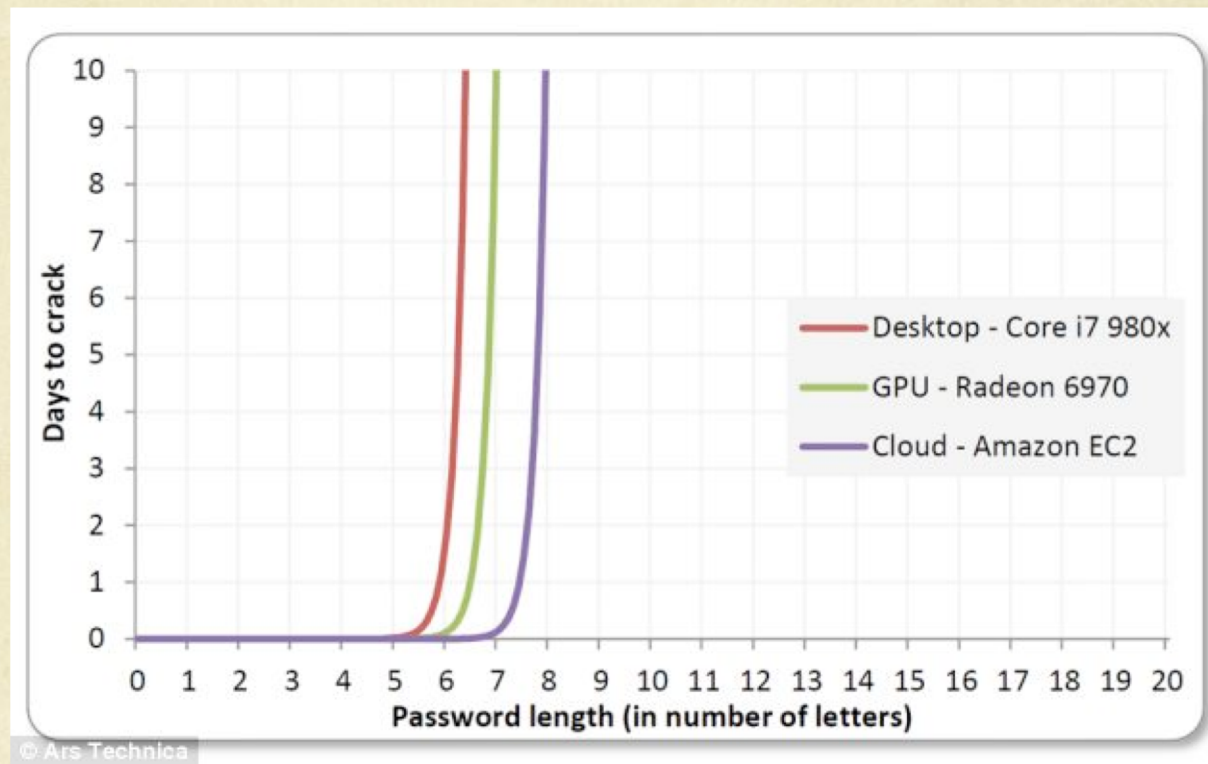
This graph shows how long in days it took the Ars Technica hackers to crack the list of 16,449 hashed passwords based on the method used. It also shows how long it took to crack passwords based on how long they were. Each hacker used a combination of wordlists, brute-force attacks and Markov chains to crack the list. One hacker managed to crack 90% of the list.

Storing passwords

○ Never send or store passwords in email.

○ Many of us can end up with as many as 10 or more passwords for different accounts in our daily lives. Keeping track of which password goes where can be a challenge.

○ If you have a lot of passwords, you can store the passwords in an encrypted (password protected) file or use a management system like LastPass, 1Password, KeePass.

○ Don't keep passwords under your keyboard or written down on a piece of paper in your office.

What happens if I lose that password?

SOFTPEDIA® DESKTOP ▾ MOBILE ▾ WEB ▾ **NEWS**

☰ Softpedia › News › Security

FLASH SALE: **System Mechanic Professional** ⚠ **60% OFF!**

Email Accounts from Top Universities on Sale on China's Taobao

Start searching now... ▸

Accounts offer discount benefits from retailers and access to educational content

By *Ionut Ilascu* 🐦 g+ 5 Sep 2014, 00:13 GMT

Individuals engaged in e-commerce activity on Chinese online shopping platform Taobao offer for sale stolen email accounts belonging to top universities across the world.

The accounts offer various benefits, which include registration to software developer programs, discounts from certain retailers, as well as access to academic databases.

Provider of network security solutions Palo Alto Networks found the information available for sale after searching the listings on Taobao for "edu mailbox." The result returned 99 entries of email addresses and passwords for 42 top universities from ten countries.

19 educational institutions in the US were robbed of the accounts, among the owners being MIT, Stanford, Yale, Princeton, Harvard, Purdue, Columbia, Cornell, University of Chicago, and New York University.

🔍 Email account sold on Taobao offers access t...

We work hard every day to bring you the latest software & games, tech

MIT credentials on sale on Alibaba's Taobao

MIT credentials on sale on Alibaba's Taobao

A gas can full of snake bile, breast-milk soap, the head of Tom Cruise —those are just some of the odd things you can buy on Alibaba's Taobao, China's biggest consumer-to-consumer online marketplace. Add to that a fake or stolen university email addresses. In an investigation last week, IT security company Palo Alto Networks found email accounts from 42 universities for sale on Taobao, ranging from 0.98 yuan to 2,400 yuan ($0.16 to $390).

What ".edu" accounts were up for grabs? The 19 US universities included many Ivy League colleges, Massachusetts Institute of Technology, Duke, Stanford, as well as some less obvious choices to claim as one's fake alma mater (e.g. University of California, Merced).
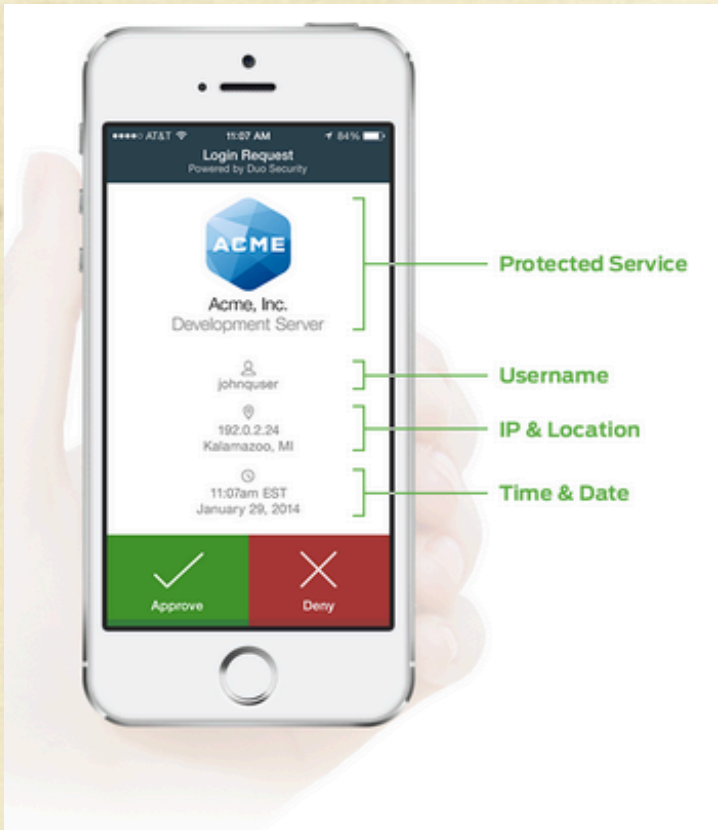
What if they also got your MIT ID number?

○ They can go to IS&T's website and get your certificates installed on their computer.

○ Prior to Duo Authentication, Certificates allow a malicious user universal access to private data in your Atlas, retirement information, access to the MIT library resources, authorized access into MIT academic systems, and even allow the user to change your MIT password.

○ Certificates DO NOT EXPIRE until the end of July.

○ Fortunately for Duo-Authentication, now the bad guys can't get to sensitive stuff if they hacked your password because you still need to OK it via DUO.

Two Factor Authentication

This is an example of DUO's app in use. It can accept both push notifications like seen above (Accept/Deny) or give you a rolling numerical password.

Two Factor Authentication

○ In addition to certificates and the traditional username and password, a second factor authentication device provides a rolling numerical password that changes over time (like every 60 seconds).

○ Why is this good?

○ Because now even if bad guys have stolen your username, password, and ID number and have your Certificates installed on their machine, it's all completely useless without the device to tell them what the current rolling numerical password is.

Two Factor Authentication

- The rolling second password can be sent either to:
  - A cellphone in the form of an SMS text message
  - A landline telephone
  - A cell phone app with a Accept/Deny button
  - A cell phone app that displays the rolling numerical password
  - A USB Yubikey
  - A DUO D100 hardware token that displays the numerical password

Two Factor Authentication

- The DUO cellphone app and landline telephones are the easiest to use once they're set up.

- The DUO cellphone app can receive a push notification that allows the user to accept or decline access.

- The landline telephone will ring the user who then picks up the receiver and presses any random telephone keys to approve authorization.

Two Factor Authentication

○ The USB Yubikey needs to be set up by your IT person via a special Yubico setup app and then handed to you.

○ The Yubikey must then be connected via a USB port.

○ Move your mouse to the Passcode line where the second password is prompted, then press the Yubikey button to automatically paste the password into the second password box.

○ Yubikeys don't work well with iMacs unless you have a USB extension cable.

Two Factor Authentication

Plug Yubikey into the computer's USB port
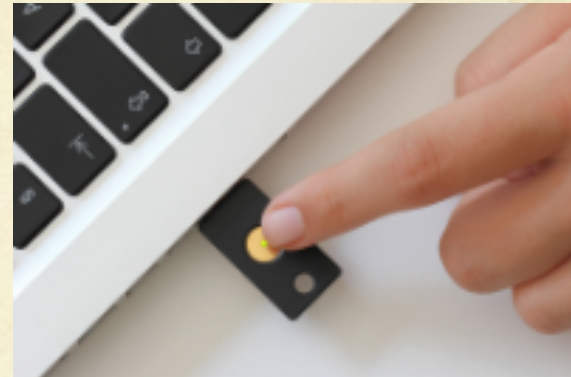
Press Yubikey button to paste code into the second password line on the browser

Yubikeys are USB tokens that are manufactured by a company called Yubico. This key needs to be set up with Yubico's software by your IT guy and then requires you to plug it into one of your computer's USB ports to function.

Two Factor Authentication

This is Tom holding the DUO D100 Hardware Token. This hardware token clips to your key chain and works anywhere in the world!

Two Factor Authentication

○ Once you decide on and/or get your DUO authentication device, you must register it with the same browser your certificates are on at http://duo.mit.edu

○ IS&T recommends that all users register **TWO devices** to be used for two factor authentication. This can be 2 different (eg. cell phone and USB Yubikey, landline phone and D100 hardware token, etc) or the same type of device (eg. 2 D100 hardware tokens).

○ To make the request for hardware tokens or USB Yubikeys, call the IS&T Help Desk at 3-1101. The devices are free and they will deliver them to your main office areas.

Software Updates
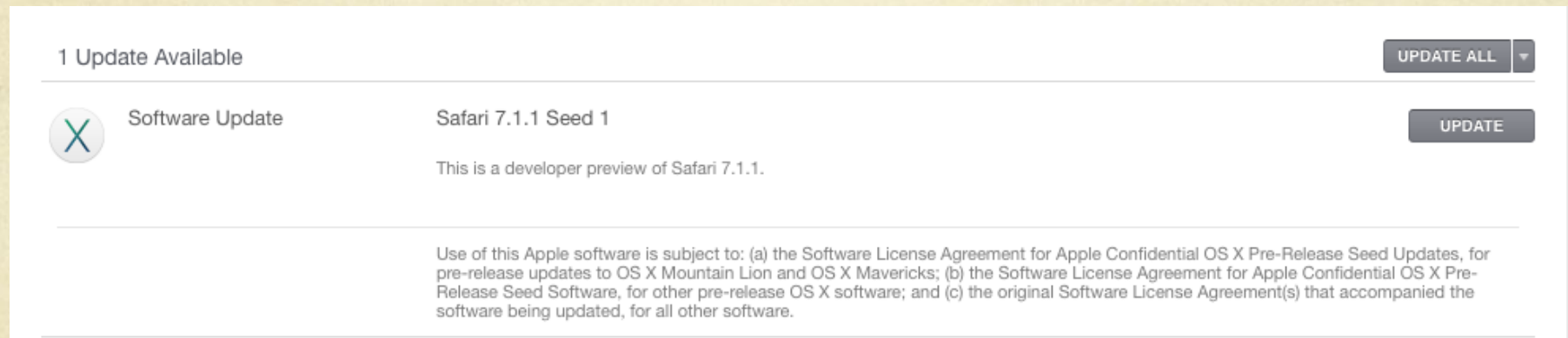
○ General rule is to do your Windows or Mac OS X operating system updates a week or two AFTER they come out. This gives the company time to work out any bugs.

○ Always wait for us to give you the all clear for any iOS or OS X Upgrades (eg. iOS 7 to iOS 8 or Mac OS 10.8 to 10.9, etc.)

○ Office Updates are generally always safe. It's ok to do those when they come out.

○ Always do Flash and Adobe Reader PDF updates.

Don't do the free upgrade right away

○ There are always bugs with the new UPGRADES.

○ Your normal system UPDATES that appear underneath the upgrade banner are safe to do.

Normal System Updates OK

> Your normal system UPDATES that appear underneath the upgrade banner in the white boxes are safe to do.

New OSes Have Bugs

○ Software incompatibility with MIT applications as well as pre-existing software you may need. This often results in features not working or random crashes.

○ Slow unacceptable hardware performance.

○ Slow or buggy web browsing. Often the browser companies need to update their software to make it work correctly.

○ Nuance products (Dragon) are usually inherently incompatible with new OS versions. They need time to work out the bugs.

NUANCE
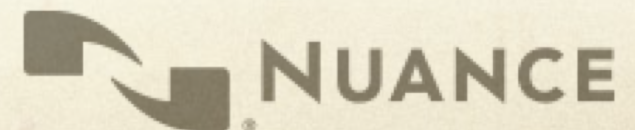
New Hardware can have bugs

(Circa August 2015)

It turns out, Kinesis Advantage keyboards (which have been around a while) won't work with Windows 7 (which has also been around a while) AND new computer hardware that has USB 3 ports.

Kinesis verified the problem

"It is highly likely that the Intel USB controller you have is the one that won't support our Advantage keyboard. **It is a problem with the Win7 drivers because the Intel USB chipsets and keyboard work together with Window 8, Linux, and Mac OS X. We've tried to work with Intel to get them to fix it but have not had success getting them to do so.** Normally a powered hub should be able to accept the Advantage keyboard, even though it has its own hub, but in spite of testing many powered hubs, we haven't found one that will mask and solve this problem.

If you had an existing keyboard and a new computer that wasn't compatible, we would suggest converting your keyboard to PS/2 (we could sell you a cable) and then use a PS/2 to USB adapter. This is a clunky solution and you would lose the USB port on the back of the keyboard, so we would never suggest doing this with a new keyboard.

We are working on a new electronic design that will solve this problem, but we don't know when it will be available (but hopefully this year). Anyway, if you would need to use your new Advantage keyboard on a computer that only has USB 3.0 and Win7, I suggest waiting for the new version or considering an upgrade to Win8.1 when it comes out (assuming Microsoft does a decent job fixing the disaster they created for keyboard/mouse users with Win 8.0)."

Hackers and Security Research

- Hackers have been around as long as there's been computers.

- For many young hackers, the movie Wargames was a popular cultural crucible of inspiration.

- Many hackers got their start taking things apart to see how they work.

- White hat hackers who work in security research disclose their findings to the companies and then the general public.

- Their findings spur improvements in security and design changes to keep us safe.

Hackers and Security Research

"For over two decades DEF CON has been an open nexus of hacker culture, a place where seasoned pros, hackers, academics, and feds can meet, share ideas and party on neutral territory."

"Our community operates in the spirit of openness, verified trust, and mutual respect."

NEWS / OPINIONS / FEATURES / DEALS / HOW-TO / BUSINESS / VIDEO / SUBSCRIBE

ALL REVIEWS ⌄   LAPTOPS / TABLETS / PHONES / APPS / SOFTWARE / SECURITY /

Home / Reviews / Software / Security / Defcon Hackers to Feds: We Need Some Time Apart

Defcon Hackers to Feds: We Need Some Time Apart

BY CHLOE ALBANESIUS   JULY 11, 2013 03:35PM EST   💬 7 COMMENTS

The controversy over leaked National Security Agency (NSA) documents has prompted the organizers of the Defcon conference to rescind their invitation to federal authorities.

13 g+ f 🐦 +
SHARES

The controversy over leaked National Security Agency (NSA) documents has prompted the organizers of the Defcon conference to rescind their invitation to federal authorities.

For years, government officials have been among the hackers and security experts on the Defcon agenda. NSA chief Keith Alexander made an appearance at last year's event, while in 2009, Defcon founder Jeff Moss was among the 16 individuals named to the Homeland Security Advisory Council (HSAC).

"For over two decades DEF CON has been an open nexus of hacker culture, a place where seasoned pros, hackers, academics, and feds can meet, share ideas and party on neutral territory," Defcon organizers said on their website. "Our community operates in the spirit of openness, verified trust, and mutual respect."

But amidst reports of widespread surveillance at the hands of the government, the hackers at Defcon aren't exactly enthusiastic about breaking bread with their federal counterparts this year.

Active hardware vulnerabilities

○ Thunderbolt adapters (all) through the Option ROMs

Exploit code can be passed through the Option ROM of any TB Adapter to a Mac which (now infected) can then pass the infection on to the Option ROM in another TB adapter.

Active hardware vulnerabilities

USB Ports (Aug 2014)

"Connecting devices to computers using a USB port could lead to security breaches.

USB technology has been called "critically flawed" by Berlin-based security researchers Karsten Nohl and Jakob Lell.

According to the BBC, the researchers said there is no way to defend against cyber vulnerabilities from USB connected devices.

Karsten Nohl and Jakob Lell said that a USB stick that has been formatted and is completely empty can still contain malware that can infect computers. This flaw can be hidden in any USB-connected device."

http://www.computerweekly.com/news/2240226605/USB-connected-devices-present-cyber-vulnerabilities
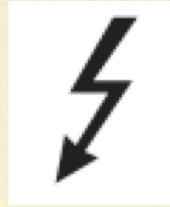
Active hardware vulnerabilities

○ USB Ports (Oct 2014) **UNFIXABLE**

"It's been just two months since researcher Karsten Nohl demonstrated an attack he called BadUSB to a standing-room-only crowd at the Black Hat security conference in Las Vegas, showing that it's possible to corrupt any USB device with insidious, undetectable malware."

"Like Nohl, Caudill and Wilson reverse engineered the firmware of USB microcontrollers sold by the Taiwanese firm Phison, one of the world's top USB makers. Then they reprogrammed that firmware to perform disturbing attacks: In one case, they showed that the infected USB can impersonate a keyboard to type any keystrokes the attacker chooses on the victim's machine. Because it affects the firmware of the USB's microcontroller, that attack program would be stored in the rewritable code that controls the USB's basic functions, not in its flash memory—even deleting the entire contents of its storage wouldn't catch the malware. Other firmware tricks demonstrated by Caudill and Wilson would hide files in that invisible portion of the code, or silently disable a USB's security feature that password-protects a certain portion of its memory."

http://www.wired.com/2014/10/code-published-for-unfixable-usb-attack/

Active hardware vulnerabilities

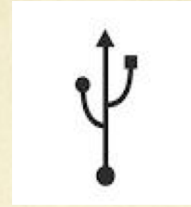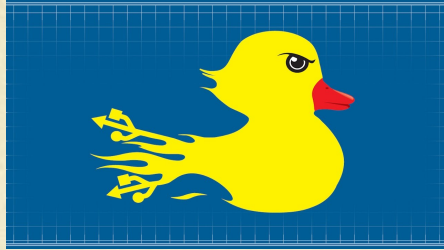- Use only your own Thunderbolt adapters.

- Do not lend your Thunderbolt adapters to anyone.

- Do not plug anyone else's Thunderbolt adapters into your Mac.

Active hardware vulnerabilities

- Only use USB devices you have purchased.

- Do not plug in USB devices from anyone else.

- Do not plug any USB device you find "lying around" into your computer.

- Do not loan your USB devices to anyone.

Additional good practices

○ Work in accounts that do not have administrator level privileges.

○ Do not leave your computer unattended, especially when traveling. Remember the hacker mantra: "physical access is full access".

○ Turn on your Firewall. Both Windows and Mac OS X have built in firewalls that can provide basic protection on hostile networks.

Sensitive Data

○ Massachusetts state law requires MIT safeguard all sensitive data. (Names, social security numbers, addresses, date of birth, credit card info, etc)

○ If you use a laptop to access or store sensitive data, the laptop needs to be encrypted.

○ We securely erase all machines that are given to us for disposal once the area is done using it.

○ Not sure if you have sensitive data on your computer? Identity Finder is available from the IS&T website.
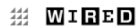
Data Breaches

- In the first 254 days of 2015 (January 1- September 11th) there were 112 reported data breaches

- Hacking attacks, malicious software attack, credit card skimming, physical theft of records, stolen laptops with confidential data

- Harvard University, University of Virginia, Penn State, United Airlines, Ashley Madison, ICANN.org, State of Minnesota, Heritage Foundation, CVS Pharmacy (Imperial Beach CA), UC Irvine Medical Center, UCLA Health System, Summit Financial Group, U.S. State Department, Bonita (CA) Unified School District, The Trump Hotel Collection, Mandarin Oriental Hotel (NYC), Mule Creek State Prison, Web.com, Orange County Employees Association, South Dakota Veteran Affairs Hospital, etc.

- http://www.privacyrights.org/data-breach/new

SECURITY | **LEER EN ESPAÑOL**

Exactis said to have exposed 340 million records, more than Equifax breach

We hadn't heard of the firm either, but it had data on hundreds of millions of Americans and businesses and leaked it, according to Wired.

BY ABRAR AL-HEETI | JUNE 28, 2018 10:14 AM PDT

LILY HAY NEWMAN   SECURITY   12.07.18 09:00 AM

THE WIRED GUIDE TO DATA BREACHES

ANOTHER WEEK, ANOTHER massive new corporate security breach that exposes your personal data. Names, email addresses, passwords, Social Security numbers, dates of birth, credit card numbers, banking data, passport numbers, phone numbers, home addresses, driver's license numbers, medical records—they all get swept up by shadowy, amorphous hackers for fraud, identity theft, and worse. Sometimes the affected company will send you an email suggesting that you change a password or credit card number, but for the most part, these incidents are invisible —until they aren't.

Think of data breaches as coming in two flavors: breaches of institutions that people choose to entrust with their data— like retailers and banks—and breaches of entities that acquired user data secondarily—like credit bureaus and marketing firms. Unfortunately, you can't keep your information perfectly safe: It is often impossible to avoid sharing data, especially with organizations like governments and health insurers. Furthermore, in cases

A new data breach may have exposed personal information of almost every American adult

Published: June 28, 2018 8:19 a.m. ET

f 🐦 in 📷 ✉ 💬 77   Aa 🖨

Exactis data leak reportedly contained detailed information on 230 million consumers

Knowledge

- Knowledge is power.

- The more you learn from searching the web for answers, research, or talking to us, the better you will be able to discern what is legit and what isn't. This will empower you to better protect yourself against bad people and criminals.

- Don't be afraid to ask questions. Always ask questions.

- There are no dumb questions.

Protect your stuff

- Your data is the most important thing on your computer.

- Have backups.

- All Mac users should be using **Time Machine**.

- PC Users should be using **Windows Backup**.

- Both of these programs are DISASTER RECOVERY solutions and require an external HD to work.

Recommended external HDs

- Western Digital "My Book" drives, 2-4TB, large form factor, desktop HD

- Western Digital "Passport" drives, 2-4TB, small form factor, portable HD

- Avoid certain Seagate HDs due to low reliability issues https://www.backblaze.com/blog/best-hard-drive/

BACKBLAZE

Your Data is Life

- **Crash Plan** is IS&T's free cloud data backup solution. This solution is great for secondary off site backup for your data.

- **Crash Plan** is NOT a suitable primary disaster recovery solution. No application or system files are backed up. Files take as long to bring back from the cloud as they take to save up TO the cloud. For users with 50-100 GB of data or more this could take days to a week.

- Use local backups like Time Machine (Mac) or Windows Backup (PC) for fastest primary data disaster recovery.

- Remember, ONLY YOU can prevent data loss.