A presentation by Albert Wang
Systems Administrator Lead
SHASS Dean's Office
05/02/2025

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 email or call you 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)

Common Examples of Phishing

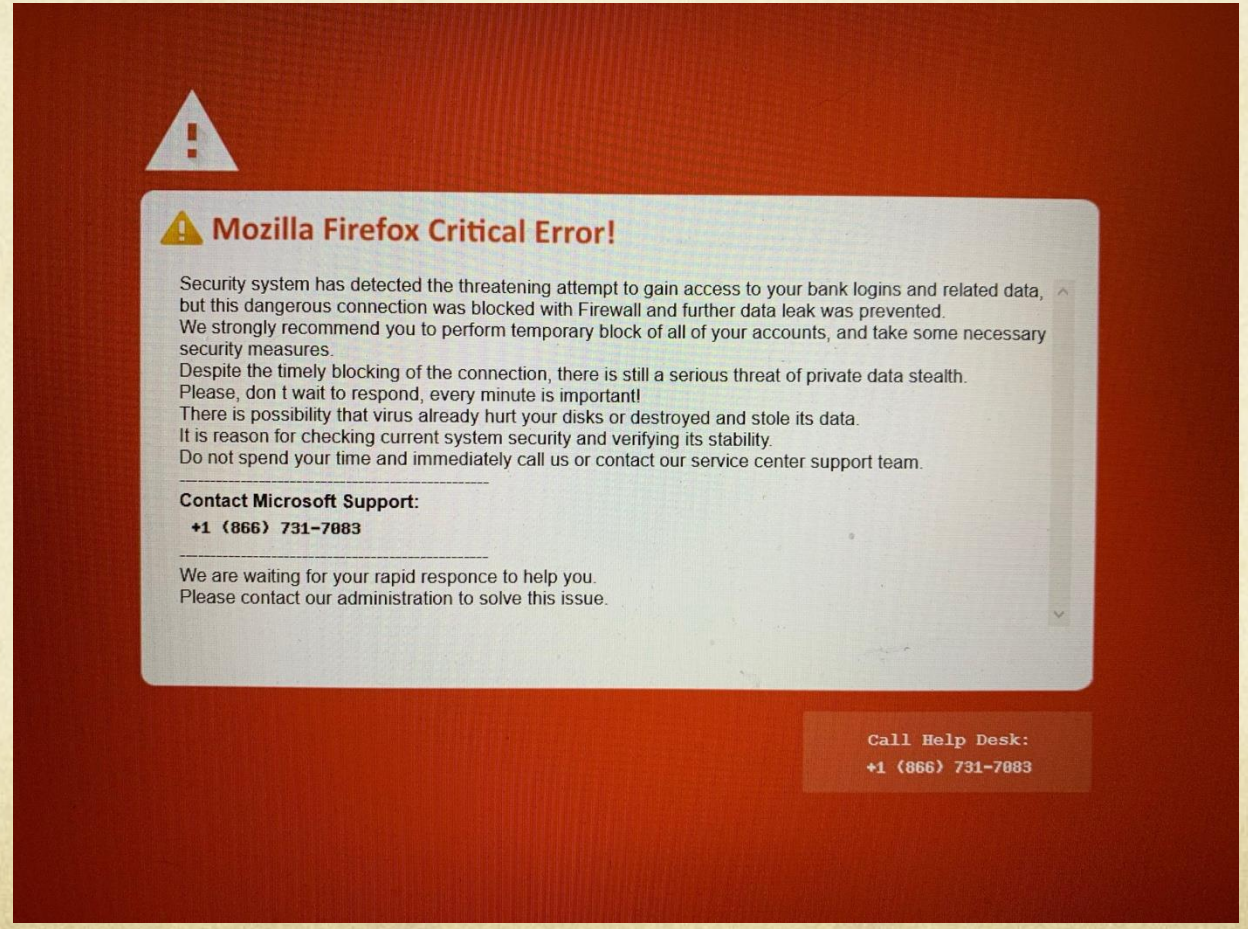
- IT "upgrade" notices that require you to click on a link or download an application.
- Bank alert notices that require users to type in their bank/credit card account numbers, usernames and passwords.
- Emergency distress notices from people you may know claiming they're trapped overseas and need you to send money, gift cards, etc.
- IRS or FBI or law enforcement notices claiming you owe money and you must pay up or be arrested.

Common Examples of Phishing

- Exortion/Sextortion attacks where a bad actor claims they've hacked you and give an example of an old password (usually an old one from a previous/old data breach) and threatens to release compromising photos or data about you unless you pay a ransom.
- Fake Product Order, Postal Service, or Delivery Service notices saying a package/product could not be delivered and they want you to open an attachment or click on a link with the invoice/information that's actually malware and/or spyware.

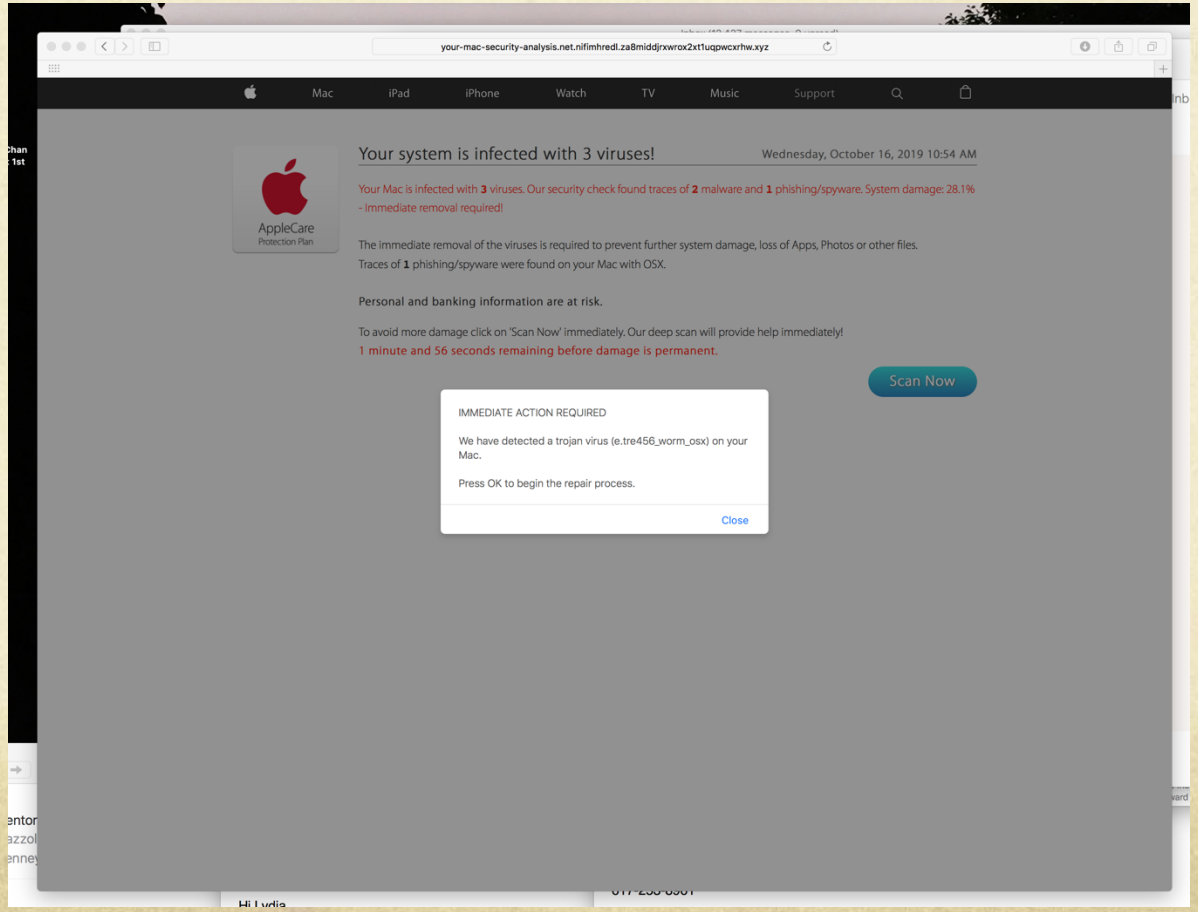
Common Examples of Phishing

- "You've been hacked!" web browser popups.



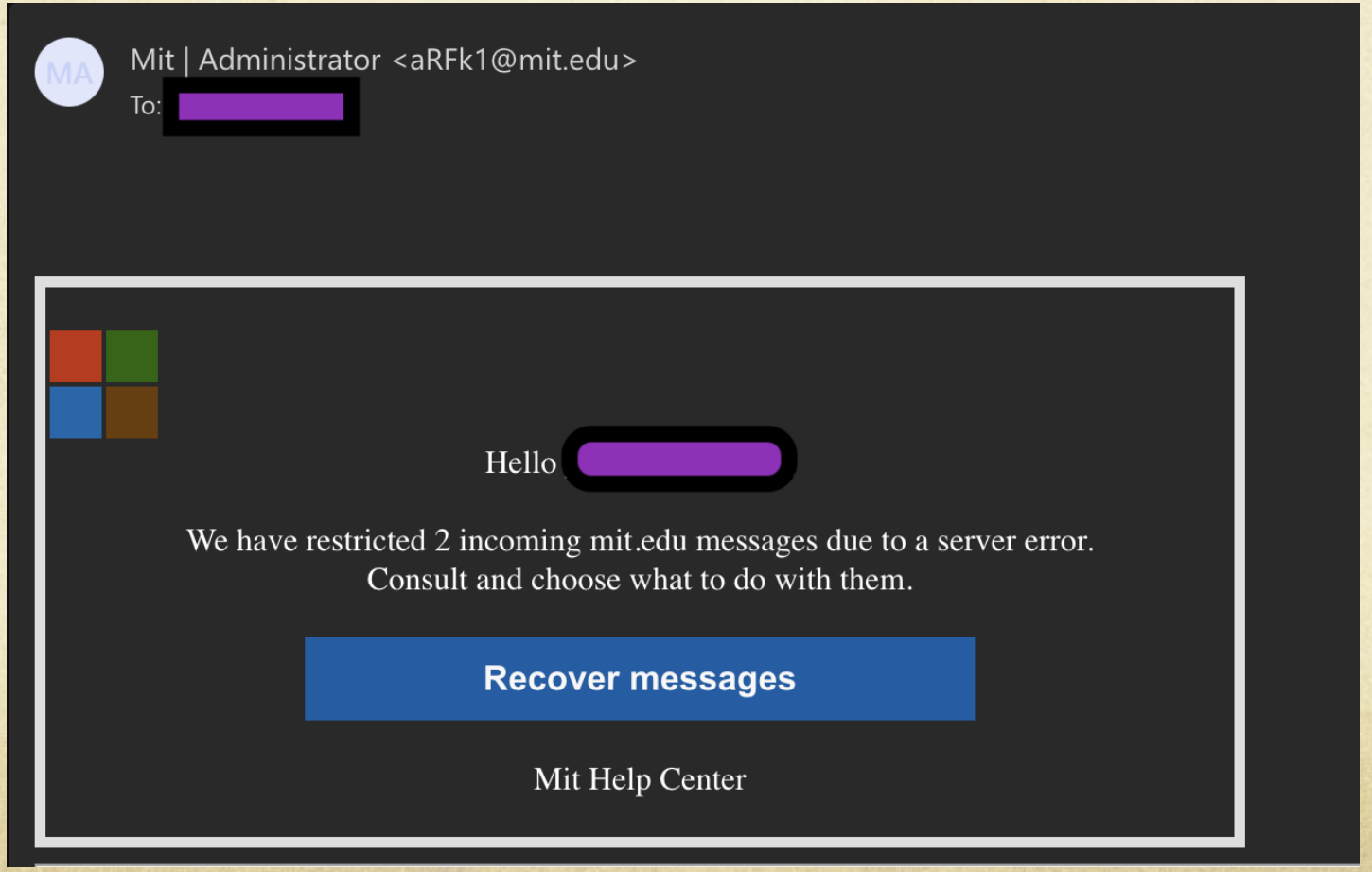
Common Examples of Phishing

- "You have been infected!" web browser popups.



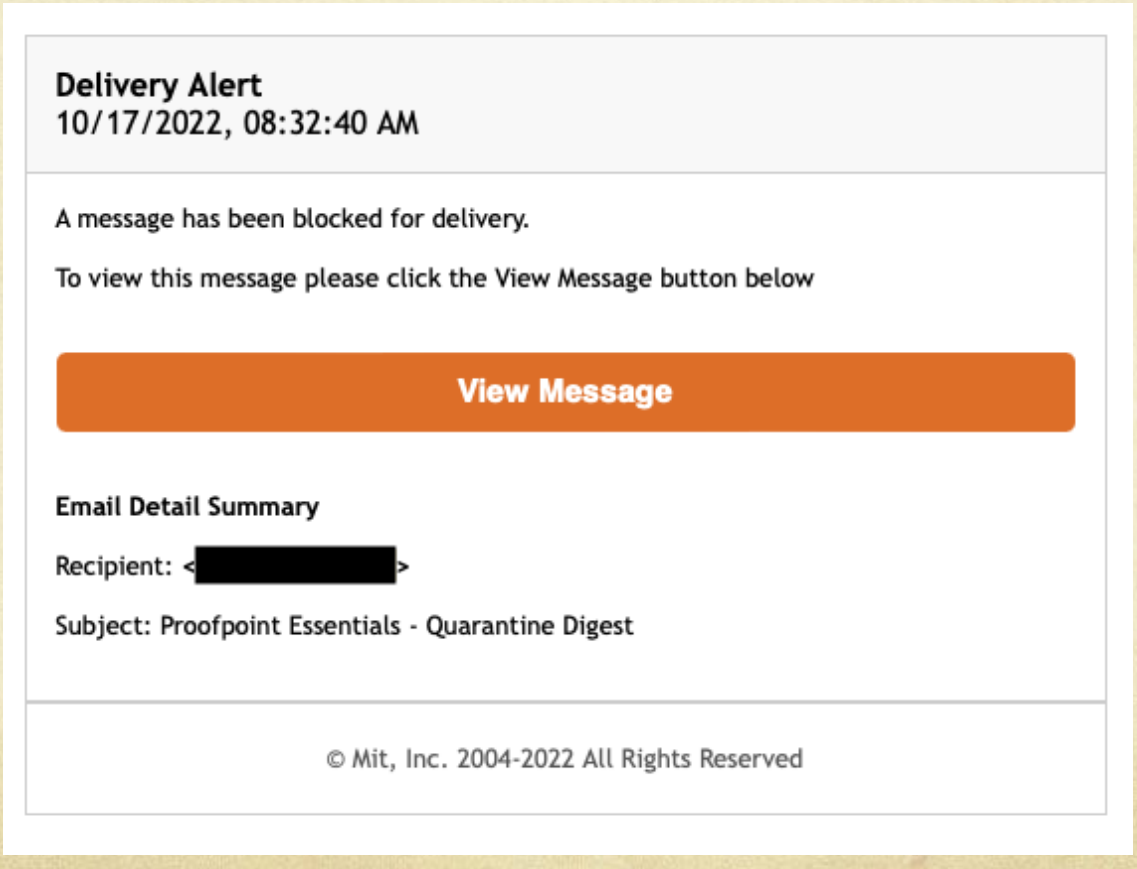
Common Examples of Phishing

- “Recover Messages” email phishing.



Common Examples of Phishing

- "Delivery Alert" email phishing.



Delivery Alert
10/17/2022, 08:32:40 AM

A message has been blocked for delivery.

To view this message please click the View Message button below

View Message

Email Detail Summary

Recipient: <[redacted]>

Subject: Proofpoint Essentials - Quarantine Digest

Common Examples of Phishing

- Impersonation email phishing.

From: Agustín Rayo <deaninterim787@gmail.com>
Subject: Hello
Date: March 25, 2024 at 8:39:58 AM EDT
To: timthebeaver@mit.edu

Available cellphone number?

Bests Regards,

Agustín Rayo
Kenan Sahin Dean
Massachusetts Institute of Technology

Is it Phishing?

- If there is ever a question whether an email is real, you can Message->Forward as Attachment (in Apple Mail) the suspect email to shassithelp@mit.edu and ask us if the email is legit.

- If you know the message is definitely phishing, you should Message->Forward as Attachment (in Apple Mail) to phishing@mit.edu so that IS&T gets the data to block these types of attacks in future.

Fake Brower Popup Phishing

- These browser windows pop up and typically use scare tactics like “you are infected” messages. Do not do anything they ask you to.

  If you get one of these:

  1) Force quit the browser immediately.
  2) Shut down your computer.
  3) Wait about 30 seconds.
  4) Turn your computer back on.
  5) Relaunch the browser. It should be back to normal.

Growing Sophistication

- Bad actors are doing their research and customizing their attacks by using correct layout and image branding for the institutions/companies they're trying to impersonate.
- Some are doing research to target specific people within organizations. The bad guys gather information from public web data and then pretend to be a department head, manager, or the Dean of a school, sending phishing emails to their faculty and staff asking for things like Apple or Amazon Gift Cards.
- Don't fall for it!

Variants of these attacks

- Email contents are simple questions which may seem out of character.
- Sometimes you can move your mouse to the Email From Address and see that the email is not correct, which makes it a phishing attack.
- However, we have also seen emails that are coming from a real person at MIT, potentially from a user on campus whose machine has been compromised by a bad actor. But why would an IT notice be coming from a Biology professor? It wouldn't.

Growing Sophistication

- These attacks can come in either Email or Voicemail or a phone call. It is best not to answer any numbers you don't recognize.

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
- As of Thursday, March 21, 2019 Any email marked as spam will now be sent directly to the user's Junk folder.

How to create a black/white list

- IS&T maintains an instructional document here:

  How do I manage my "blocked senders" or "allowed senders" list with MIT spam filtering?

  https://kb.mit.edu/confluence/pages/viewpage.action?pageId=159398159

Attachments

- Attachments are files sent with an email.
- Never open attachments from people you don't know.
- Never open attachments from people you do know but weren't expecting an attachment from.
- Attachments (some examples: pdf, doc, jpg, exe, zip, gzip) are used as Trojan horses by bad people to deliver bad stuff payloads like viruses, malware, and root kits.
- If in doubt, ALWAYS email the sender to verify the attachment is legitimate.

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 free software.
- The bad guys know this.
- Hacked or fake 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.
- Unless you have vetted the source of the software by doing web searches to see if it's safe and not malware, never install it.

Safe ‘free’ software

- Legitimate shareware and freeware do exist, but Google (or Duck Duck Go) them if you’re not familiar to verify their authenticity. See what people are saying.
- 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. (eg. Malwarebytes, Spybot S&D)
- If in doubt, email shassithelp@mit.edu to ask. There are no dumb questions.

Online app stores

- Apple rigorously vets all of their apps. Sometimes overly so.
- Microsoft vets nothing. It's the Wild West in MS land. 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. Everyone at MIT should be using Sophos on their work machines.
- Great free options.
  - Spybot S&D, Super AntiSpyware, Malwarebytes for Windows
  - ClamXAV, Avast!, Malwarebytes for Mac
- Update it. Use it once in a while.

Anti-Bad Stuff software

- Crowdstrike Falcon

  Falcon is the CrowdStrike platform purpose-built to stop breaches via a unified set of cloud-delivered technologies that prevent all types of attacks — including malware and much more.

  Today's sophisticated attackers are going "beyond malware" to breach organizations, increasingly relying on exploits, zero days, and hard-to-detect methods such as credential theft and tools that are already part of the victim's environment or operating system, such as PowerShell.

Anti-Bad Stuff software

- Crowdstrike Falcon

  Q: Who should use Crowdstrike Falcon?

  A: Definitely anyone who works with sensitive or private data and/or anyone who must travel with their work laptop to countries where the cyber attack profile could be high. These countries and regions include but are no limited to China, North Korea, Russia, the Middle East or Eastern Europe.

Anti-Bad Stuff software

- Crowdstrike Falcon

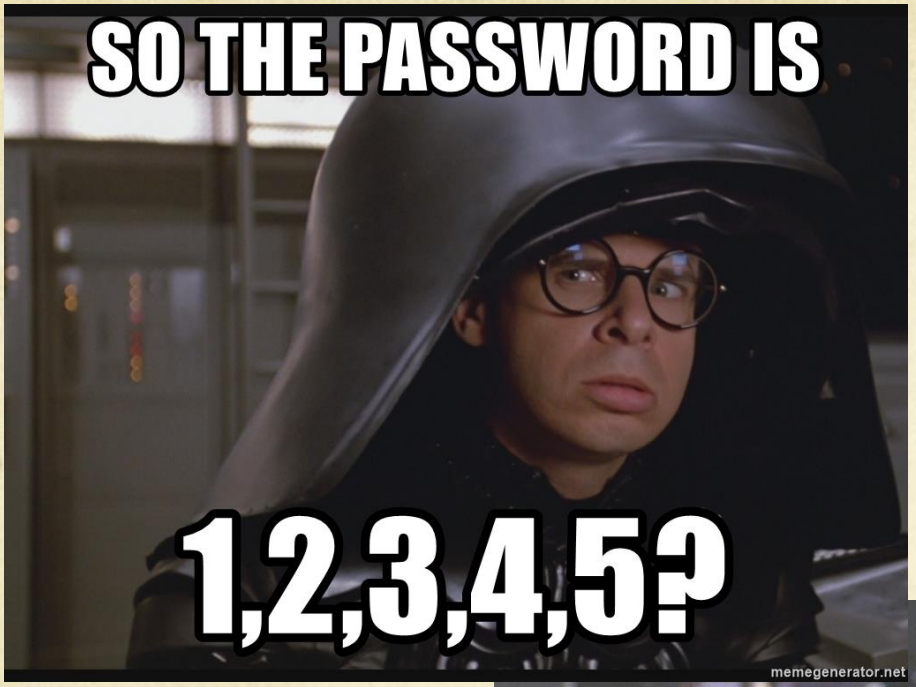
  If you **decide to install** Crowdstrike Falcon, be aware the software seizes control of your OS. Its control mechanism is itself virus-like and because of that it imposes strict rules on the machine:

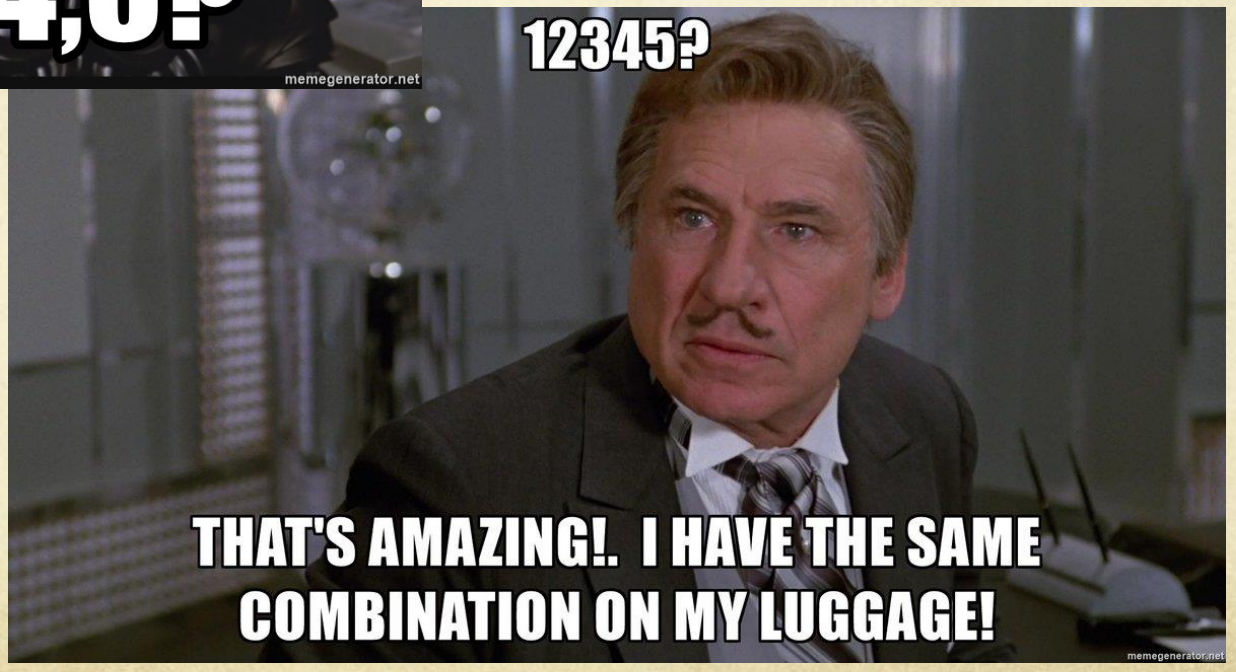
  1) You must stall the version for your **specific version of the operating system**. (eg. Mac OS 10.15, Mac OS 11, etc)

  2) Once installed you should **NEVER upGRADE** your operating system to the next/newest version.
  - For example, upgrading from Mac OS 13 Ventura to Mac OS 14 Sonoma.
  - Attempting to do so with Crowdstrike installed could damage you machine and cause it to be unusable.

Loaner laptops for travel

- If you don't need to travel with your work or personal laptop, IS&T provides loaner laptops for travel.
- Anyone traveling to or near countries where the cyber attack profile could be high (eg. China, North Korea, Russia, the Middle East or Eastern Europe) should consider borrowing a loaner laptop.
- Information here: https://ist.mit.edu/secure-devices-travel


SO THE PASSWORD IS
1,2,3,4,5?
memegenerator.net


12345?
THAT'S AMAZING!. I HAVE THE SAME COMBINATION ON MY LUGGAGE!
memegenerator.net

Passwords

- The most recent SplashData worst passwords lists can be found via Tech Cult at:

  https://techcult.com/most-common-passwords/

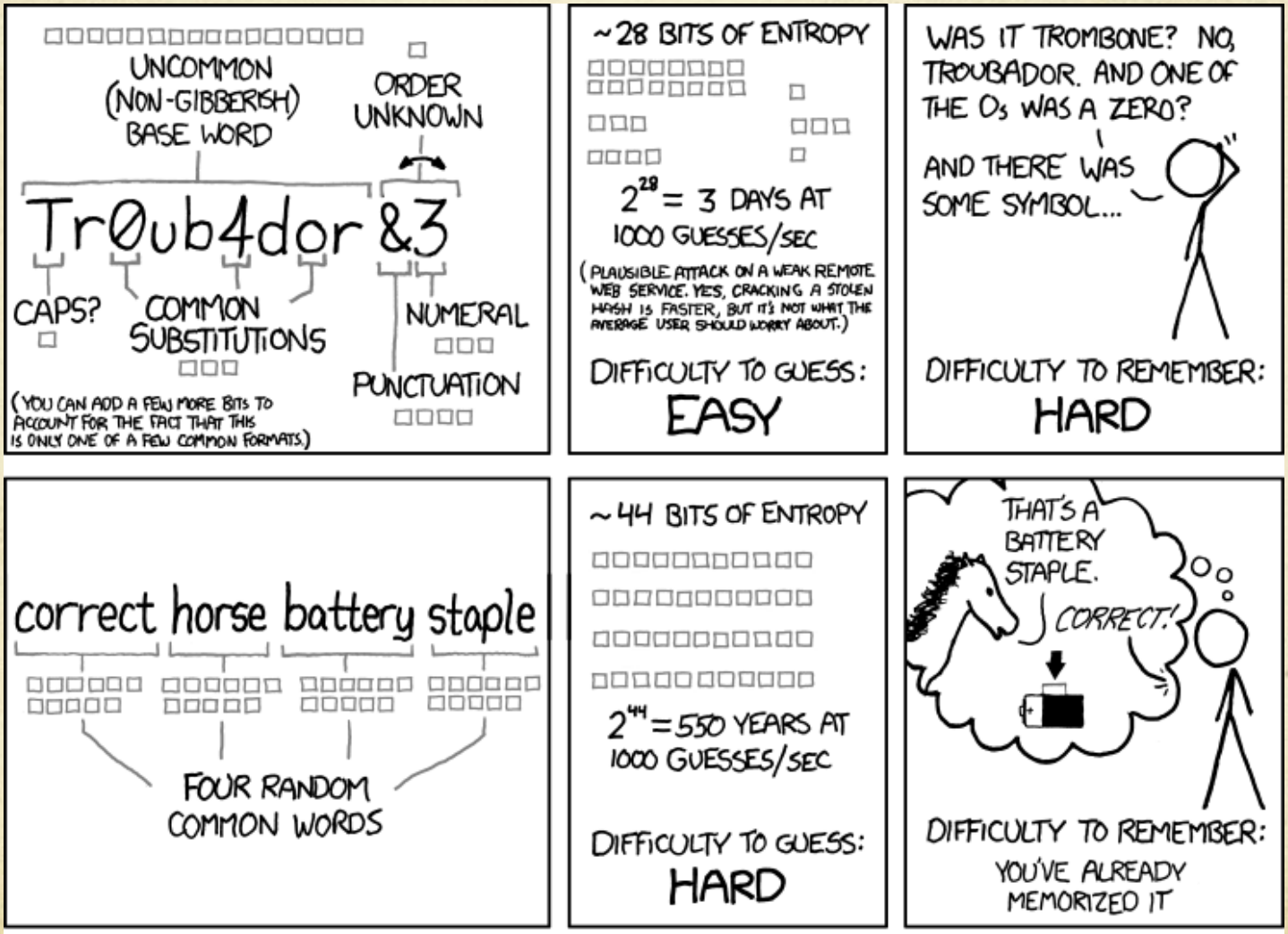
- 1,2,3,4,5 is #7 of the top 10.
- 1,2,3,4,5,6 is #1 of the top 10.

splashdata

What is a good password?

- Back ten years ago, eight characters or longer was pretty good. Today, 12 or longer is safe. 16 or longer is best.
- To maximize the amount of time cracking programs will take to crack the password, have at least 1 upper case letter, one number, and one symbol.
- ALWAYS choose something you'll easily remember.
- Eg. WinniethepoohandTigger2!
  Inanthroareyoumysteryorsciencefiction?
  Fortunethehappydogsmilesatme2day!
  Makeway4skippypeanutbutterducklingsinboston!
  Correcthorsebatterystaple
- If you have to write it down, it's not a good password.

What's easy to remember and hard to crack?



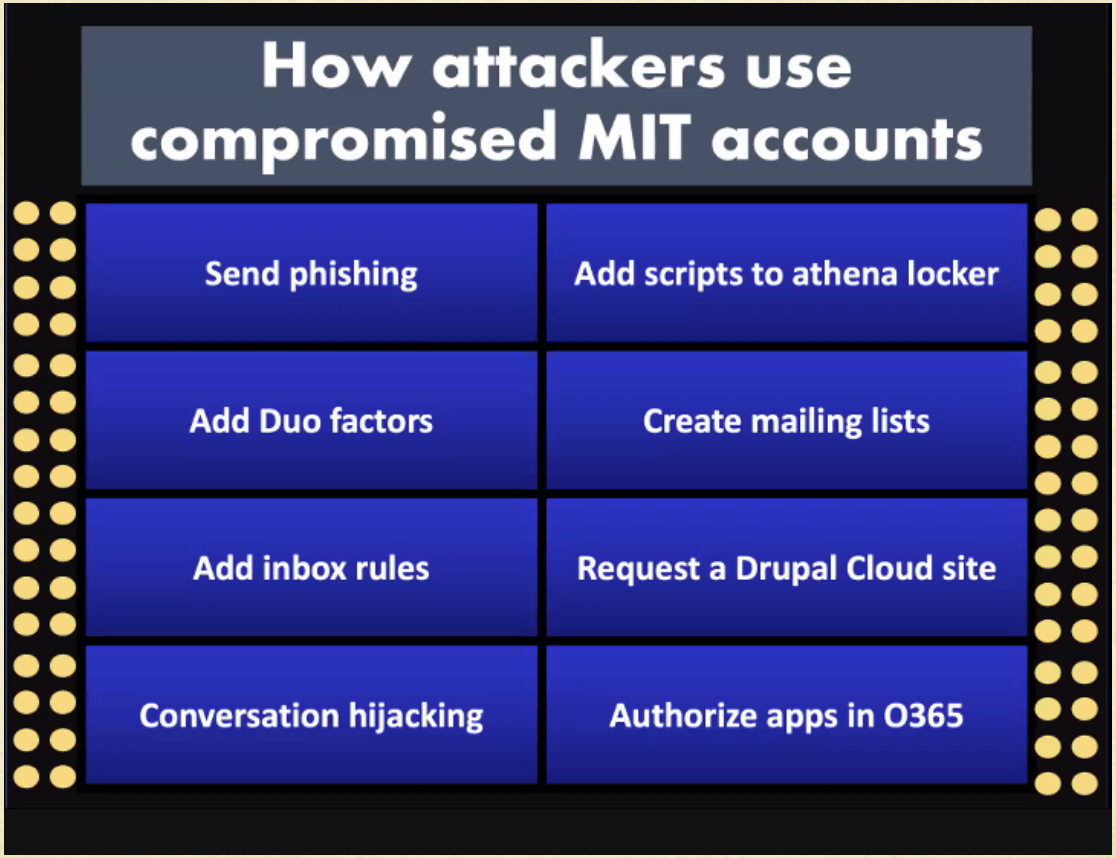
How secure is my password?

Security.org now maintains an app at https://www.security.org/how-secure-is-my-password/ to tell you how long it would take to crack your password. If in doubt, use this to see how good your password is.

Storing passwords

- Never send or store passwords in email.
- If you have a lot of passwords, you can store the passwords in an encrypted (password protected) MS Word file or use a management system like LastPass or Bitwarden.
- Don't keep passwords under your keyboard or written down on a piece of paper on your desk in your office.
- Don't keep using default passwords. They're not secure. Change it to anything else.

From the MIT Security Team

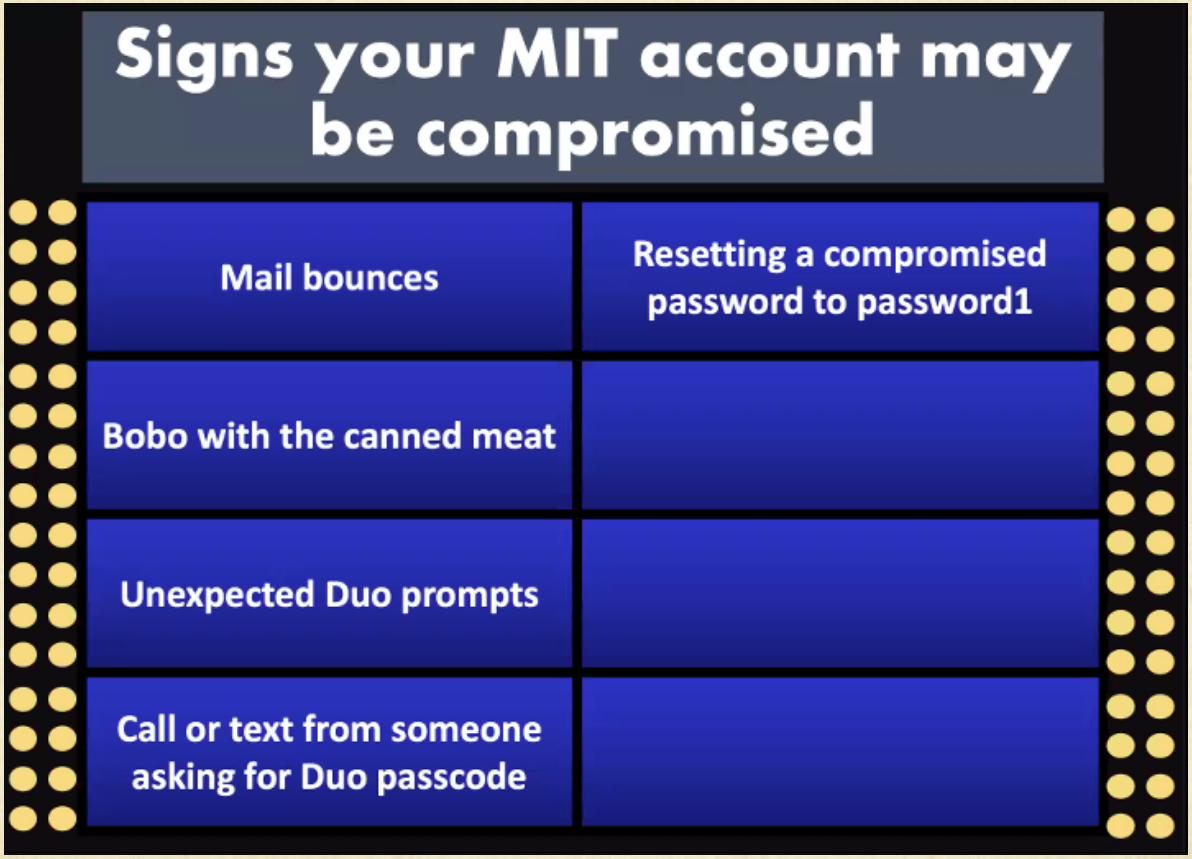


From the MIT Security Team

What should I do if my MIT Kerberos account is compromised?

- email security@mit.edu
- KB http://kb.mit.edu/confluence/x/MZIBCQ
- Change your password
- Check your Duo factors
- Check your mail forwarding settings
- Check for any new lists that may have been created
- Check mail forwarding settings and inbox rules
- Try to recover deleted items
- Check for applications using Microsoft 365 credentials

From the MIT Security Team

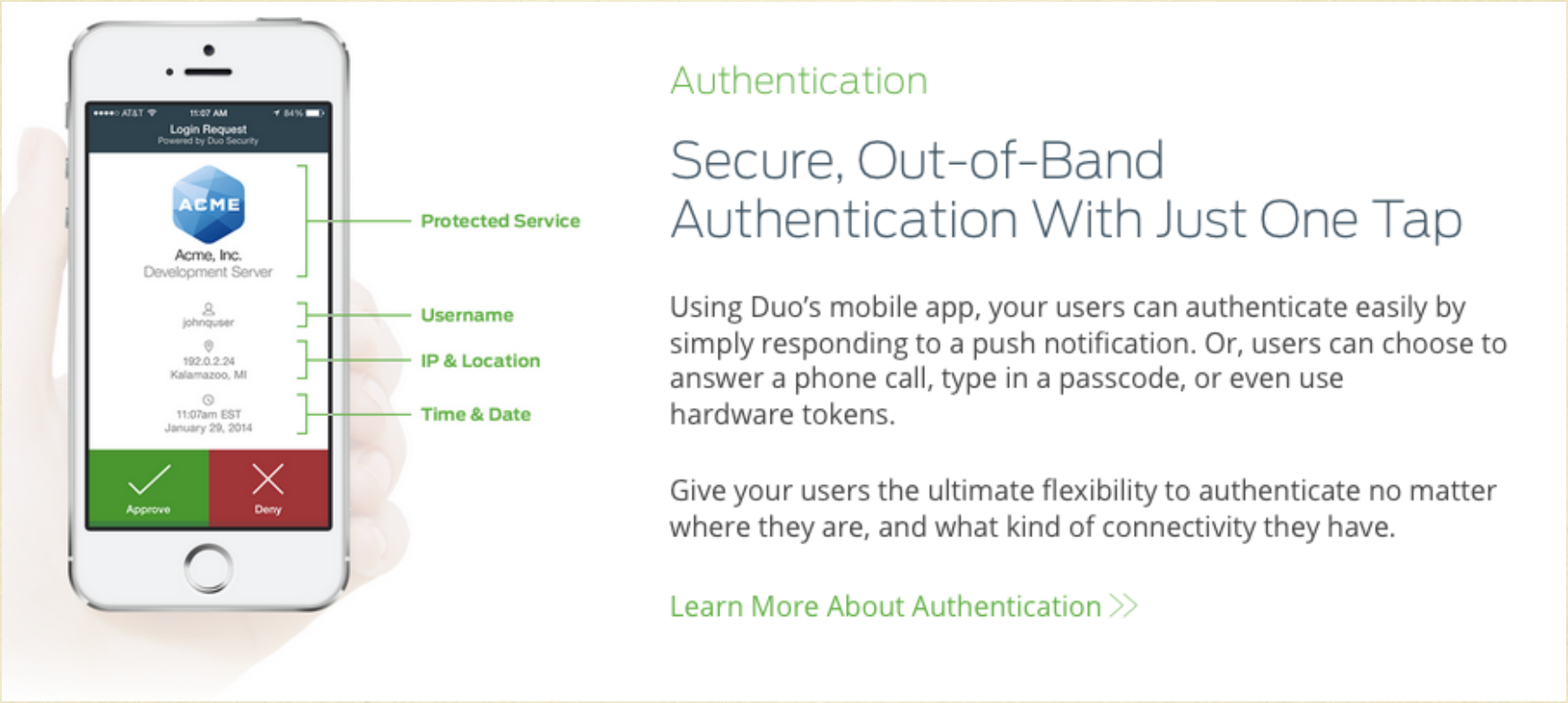


What is Bobo with the canned meat:
https://kb.mit.edu/confluence/pages/viewpage.action?pageId=151093401

What is Bobo with the canned meat?

- Unable to send email through outgoing.mit.edu
- Trying to send authenticated email through outgoing.mit.edu generates the error "554 5.7.1 Bobo with your canned meat?"
- Note: also check the list of mail errors here: Email bounce error messages
- The mail is rejected by outgoing.mit.edu
- https://kb.mit.edu/confluence/pages/viewpage.action?pageId=151093401

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 secondary 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 or cellphone 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 IS&T 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 are less convenient to use with iMacs unless you have a USB extension cable so the USB ports on the back are front accessible.

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 which DUO authentication device you want, you must register it at http://duo.mit.edu
- IS&T recommends that all users register **TWO devices** to be safe. 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.

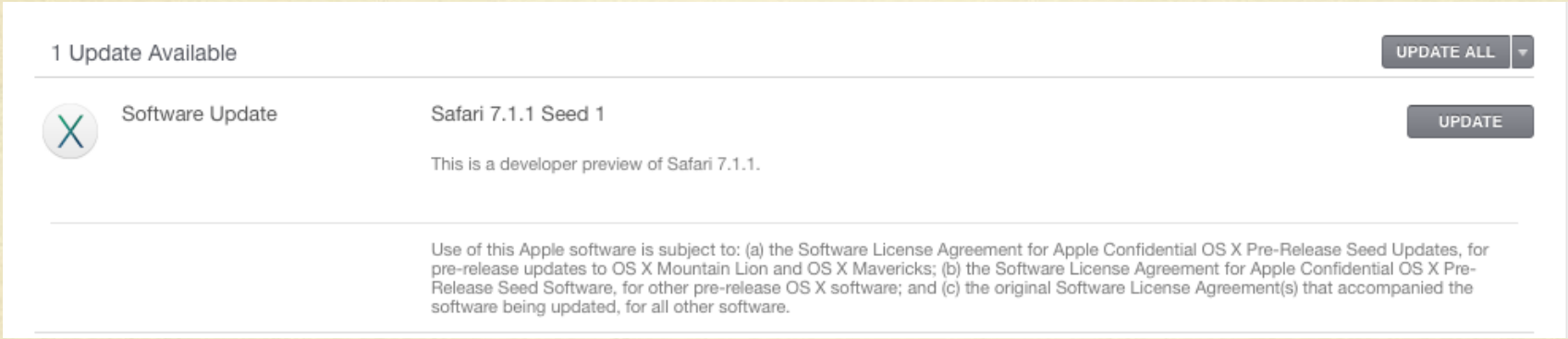
Software UpDATES

- UpDATES are improvements to the current version of a piece of software.
- 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.)
- Microsoft Office Updates are generally always safe to do. It's ok to do those when they come out.

Don’t do the free upGRADE

- Your machine runs best on the OS version it originally came with.
- There are always bugs (some severe) with every new version of the Mac and Windows OS.
- Once an upGRADE is done it CANNOT be undone.
- If you have Crowdstrike Falcon installed NEVER DO any of these upGRADES.

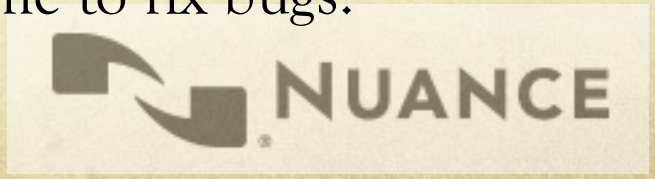
System UpDATES are OK



- Your normal system upDATES that appear underneath the upgrade banner either in the white boxes or text link saying “other updates are available”.

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 and/or WiFi performance.
- Slow or buggy web performance. Often the browser companies need to update their software to make it work correctly.
- Nuance products (Dragon) are usually incompatible with new OS versions. They need time to fix bugs.

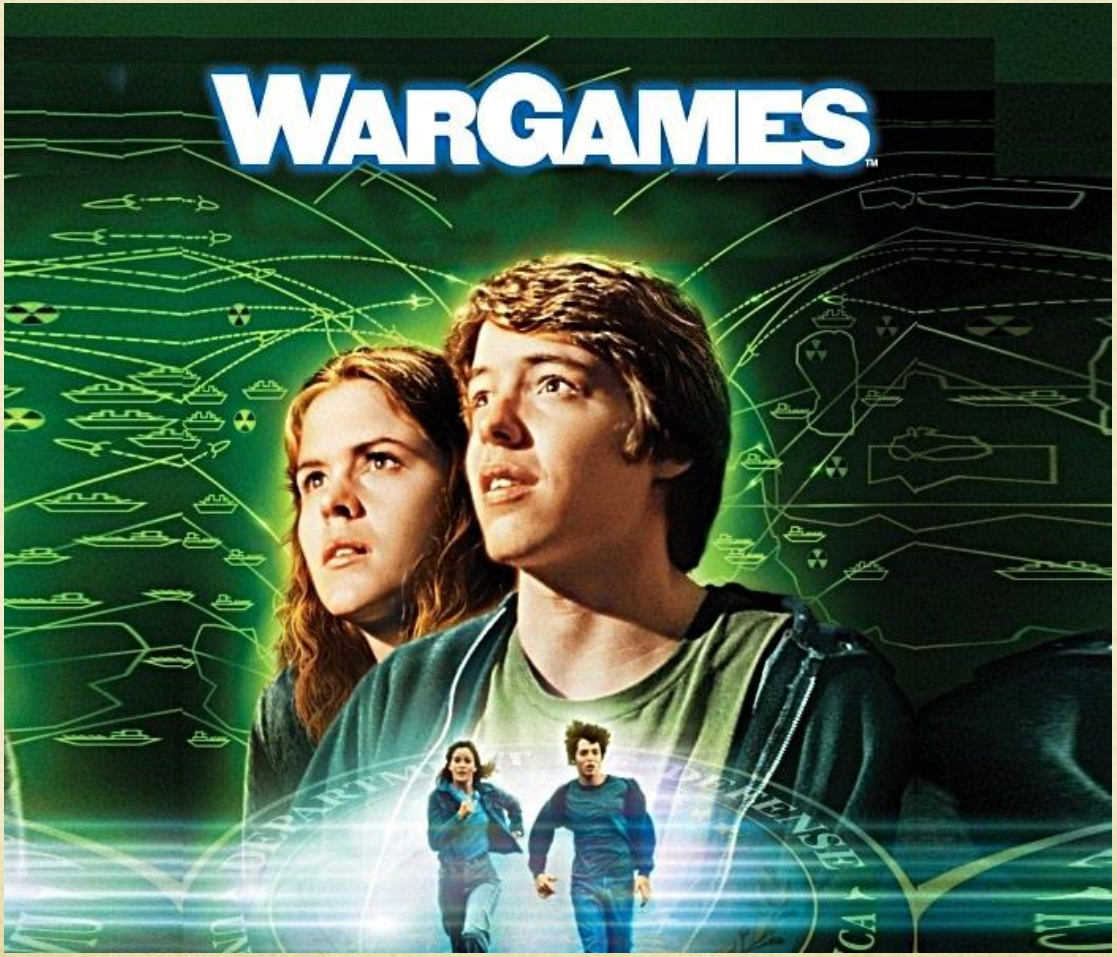


New Hardware can have bugs

(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.

Hackers and Security Research



Hackers and Security Research

- Hackers are also computer users and 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."

PC

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 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

PC Find products, advice, tech news

PCMag editors select and review products independently. If you buy through affiliate links, we may earn commissions, which help support our testing. Learn more.

Home > News > Security

PSA: If You Get a 'Best Buy Gift Card' on a USB Drive in the Mail, Don't Plug It Into Your PC

Trustwave has uncovered an incident where a hacker mailed a malicious USB stick to a victim on the pretense the thumb drive was part of a Best Buy gift card offer. In reality, the thumb drive was full of malware.

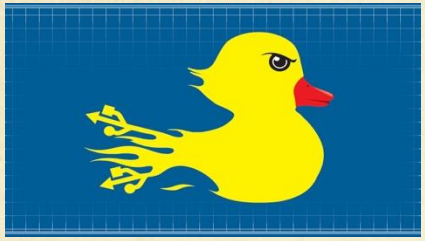
By Michael Kan March 26, 2020

https://www.pcmag.com/news/psa-if-you-get-a-best-buy-gift-card-on-a-usb-drive-in-the-mail-dont-plug

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.

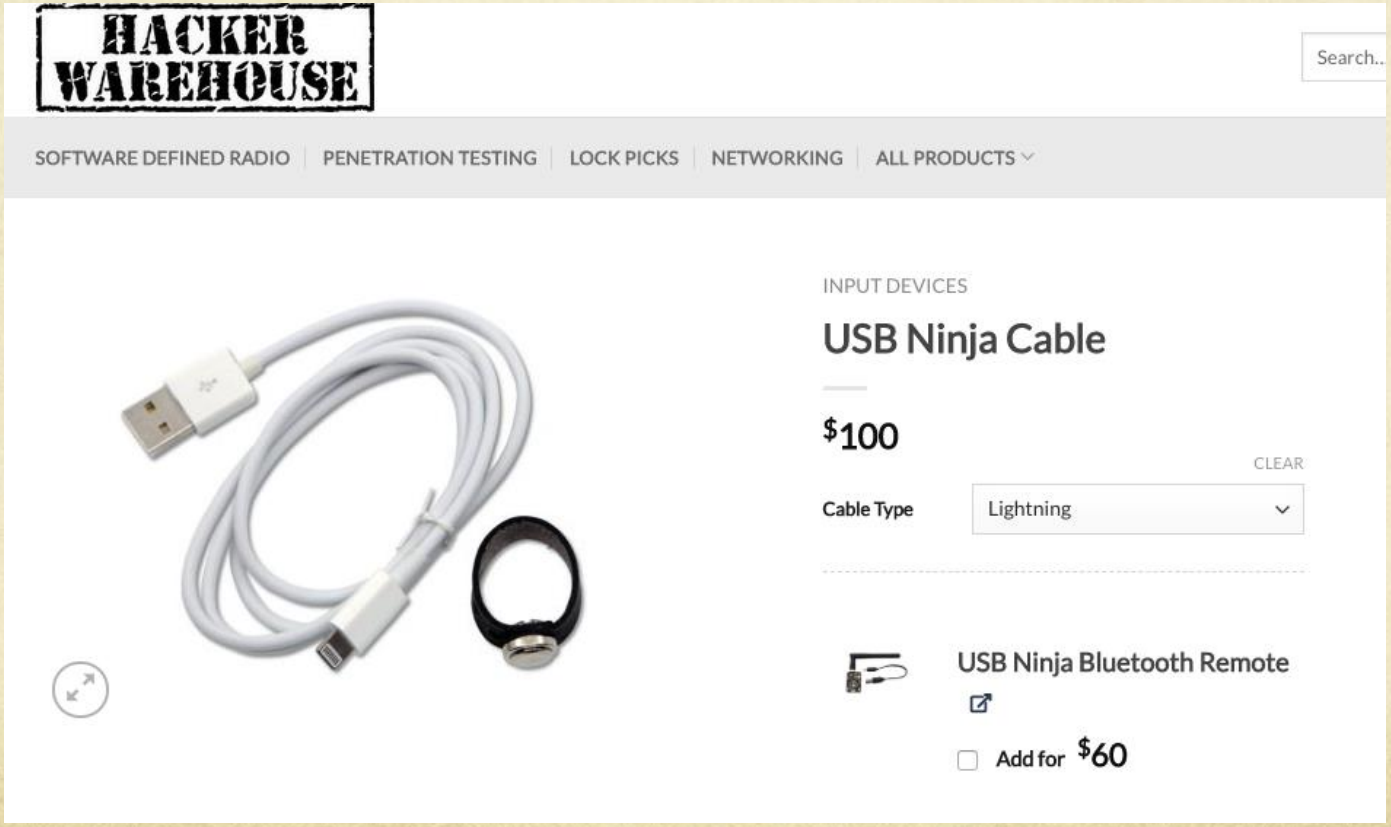
Active hardware vulnerabilities



- Only use USB devices you have purchased.
- Do not plug in USB devices from anyone else.
- NEVER plug any USB device you find “lying around” into your computer.
- Do not loan your USB devices to anyone.

Active hardware vulnerabilities

Sometimes things are not what they seem.



Active hardware vulnerabilities

There is an entire market of fake cables and USB devices that are hacker tools that can inject programming scripts and executables onto computers they are plugged into.

DESCRIPTION

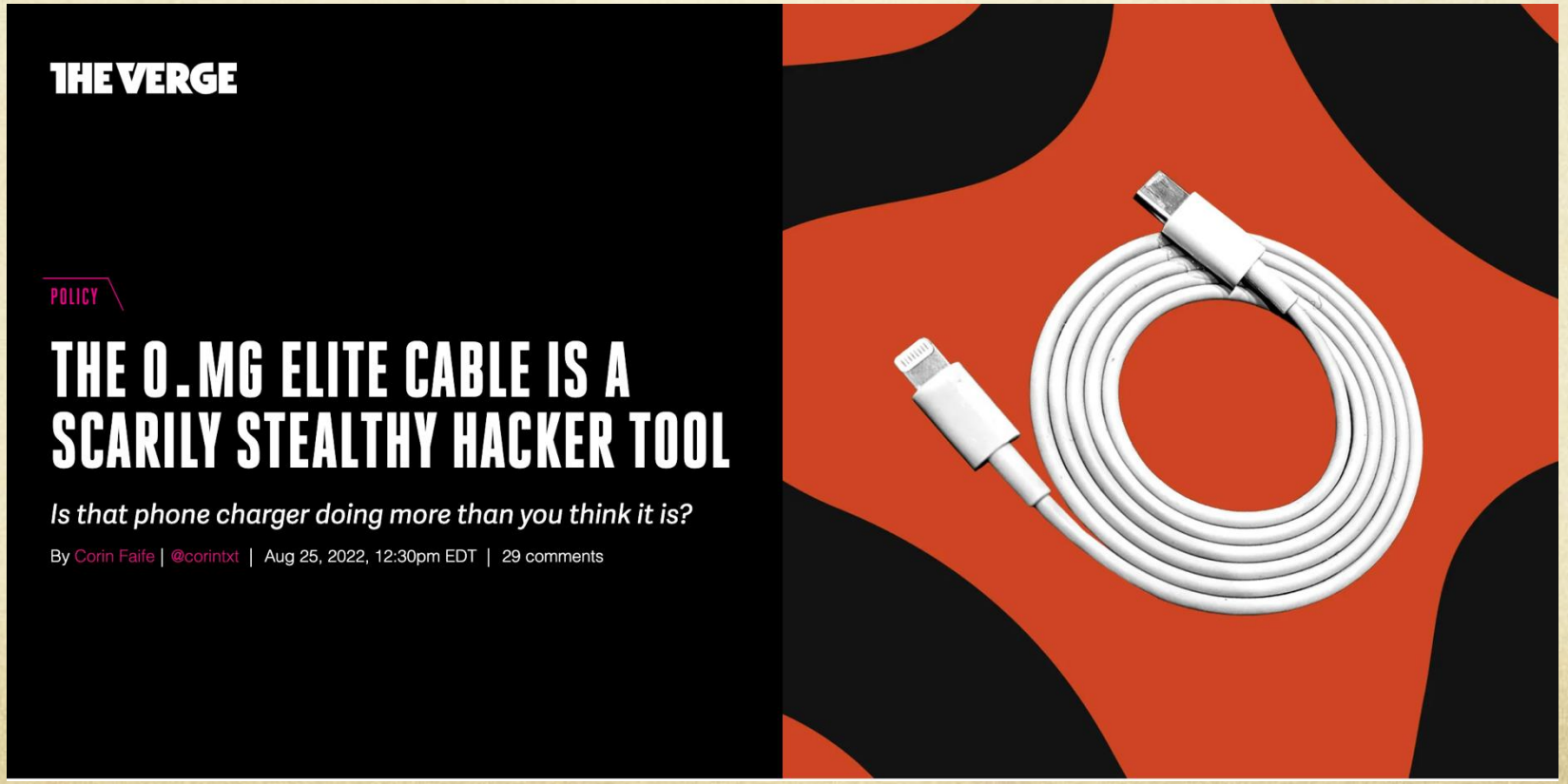
USB Ninja is an information security and penetration testing tool that looks and functions just like a regular USB cable (both power and data) until a wireless remote control triggers it to deliver your choice of attack payload to the host machine. In essence, USB Ninja is the next step in the evolution of BadUSB, embedding the attack in the USB cable itself.

Emulating keyboard and mouse actions, payloads can be completely customized and can be highly targeted. Undetectable by firewalls, AV software (**depending on payload of course**) or visual inspection, the USB Ninja is an ideal tool for penetration testers, police and government.

Includes: 1 cable type of choice and 1 trigger/programming ring.

Active hardware vulnerabilities

This one is disguised as a USB-C Lightning Cable for an iOS device.



Additional best 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 (public) networks.

Additional best practices

- Use VPN (Virtual Private Network) to encrypt your data across a public network like the public WiFi at airports, hotels, and restaurants.
- Some MIT campus resources like data servers, administrative systems, and printers are only accessible on campus via MITnet on campus or over MIT's GlobalProtect VPN. https://ist.mit.edu/prisma/client
- Third Party VPNs like Private Internet Access (PIA), Nord VPN, and ProtonVPN are often also used by clients to watch shows on streaming services not normally available in their country.

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**. On Macs this means turn on File Vault.
- We securely erase all machines that are given to us for disposal once the DLC is done using it.
- Not sure if you have sensitive data on your computer? Spirion is available from the IS&T website. https://ist.mit.edu/spirion/all

Data Breaches

- There are now too many data breaches to count and the magnitude of some of these breaches have been colossal in scale.
- In 2024 alone over a billion records of sensitive data were exposed/stolen including the social security numbers of everyone in the United States.

https://techcrunch.com/2024/10/14/2024-in-data-breaches-1-billion-stolen-records-and-rising/

Data Breaches

- Data Breaches are now so ubiquitious that Wikipedia maintains a running updated list of the largest data breaches.

  https://en.wikipedia.org/wiki/List_of_data_breaches

- The State of California maintains one of the most comprehensive list of data breaches of anywhere.

  https://oag.ca.gov/privacy/databreach/list

Data Breaches

- Users should lock their credit down from the 3 big credit agencies to protect themselves from fraud should bad actors attempt to use their stolen credit information.
- Recommended client remediation to counteract the damage done was posted to the news article on the shassit website about the massive social security data breach.

  https://shassit.mit.edu/news/massive-social-security-data-breach/

Current state of the Internet

- The current state of the Internet is a free-for-all cybersecurity hellscape.
- With the recent dissolution of federal cybersecurity agency watchdog teams and investigative personnel, both state actors and criminals are now running rampant across the Internet and attacking sites and digitally controlled infrastructure in the U.S.
- It is now up to each of us to remain vigilant and exercise caution on the Internet. Recognize the potentially fraudulent, emotionally-charged communications designed to fool us and stop them from stealing our private information and data.

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.

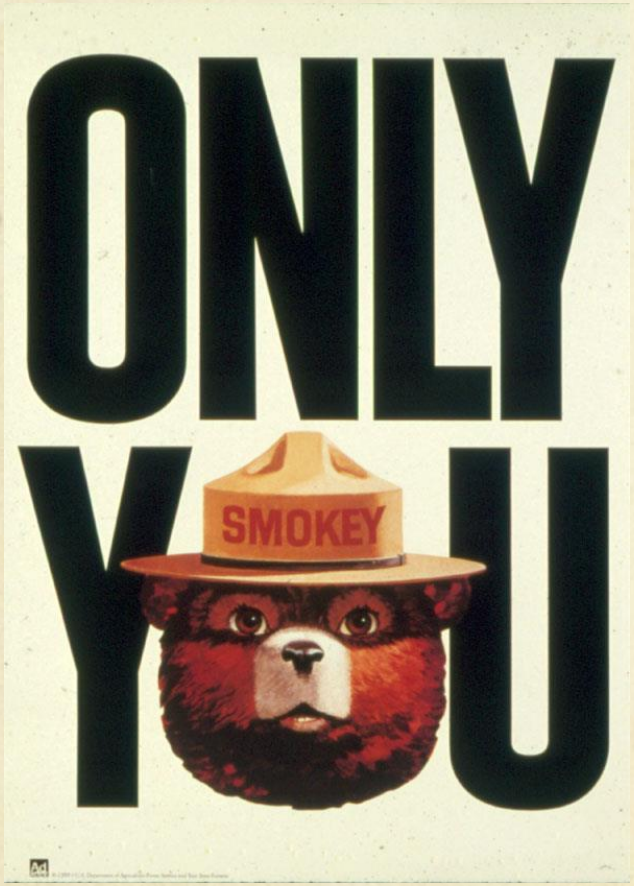
Protect your stuff

- Your data is the most important thing on your computer.
- Have backups. More than one.
- 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.
- Use Cloudbased Storage like DropBox and/or Cloudbased Backup like Code42 Crashplan from IS&T!

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
- https://www.tomshardware.com/reviews/best-external-hard-drive-ssd,5987.html

Your Data is Life



- **Code 42 Crash Plan** is IS&T's free cloud data backup solution. This solution is great for secondary cloud backup for your data.
- **Crash Plan** does not backup everything. 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.
- ALSO use local backups like Time Machine (Mac) or Windows Backup (PC) for fastest primary data disaster recovery.
- Use Cloud-based file sharing like Dropbox.
- Remember, ONLY YOU can prevent data loss.