A presentation by Albert Wang
Systems Administrator Lead
SHASS Dean's Office
11/17/2014

Safe Computing @MIT

What everyone needs to know

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
- Exchange users get Spam Quarantine: https://mailsec-cc.mit.edu/brightmail/
- Authenticate with your MIT Kerberos username and password.

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 on CNET.com for download or on 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.

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, AVG for PC) (ClamXAV, Avast! for Mac)
- Update it. Use it once in a while.
- Everyone should be using Sophos on their work machines at MIT. 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.

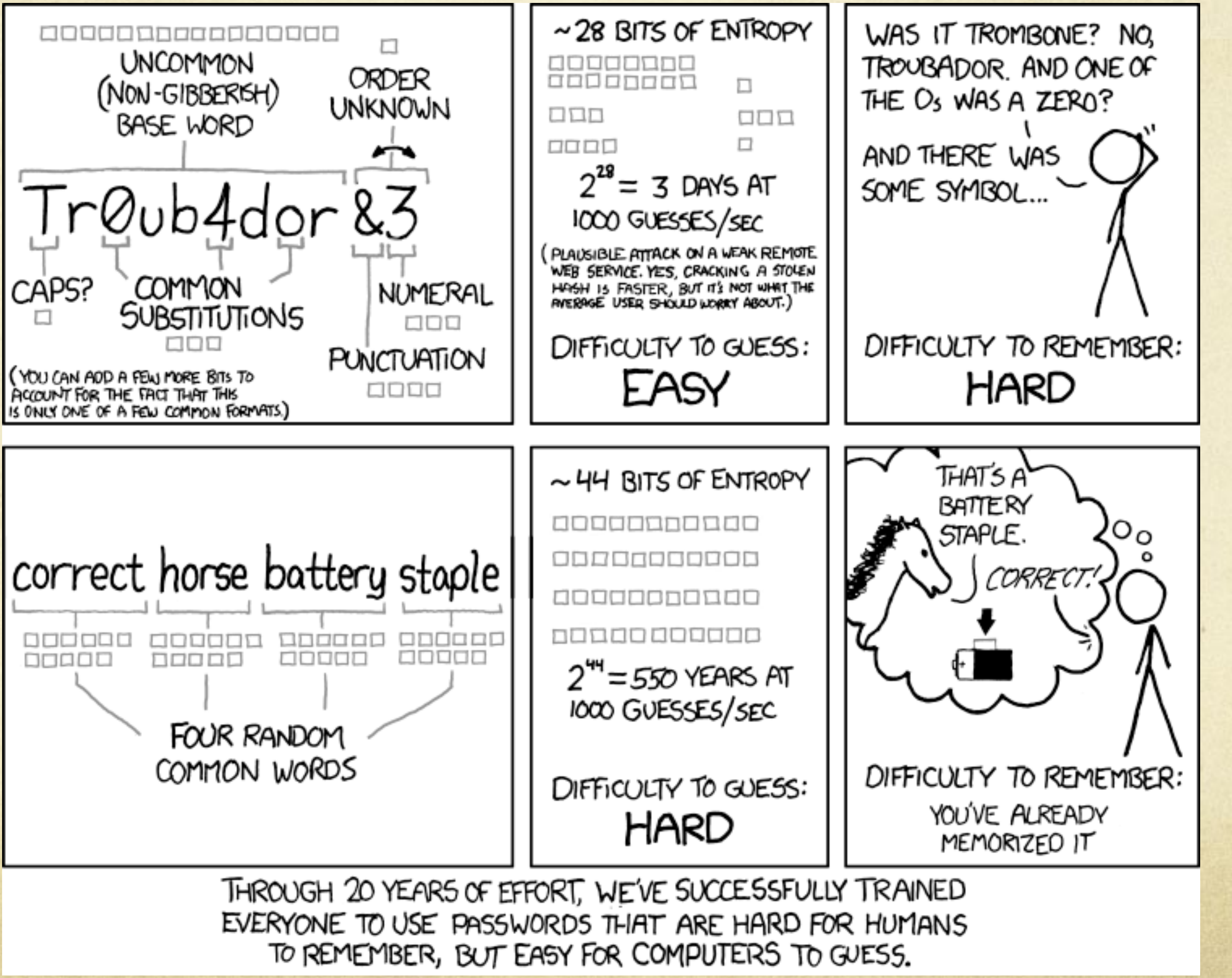
- 1 **123456** (*Up 1*), 2 **password** (*Down 1*), 3 **12345678** (*Unchanged*), 4 **qwerty** (*Up 1*), 5 **abc123** (*Down 1*), 6 **123456789** (*New*), 7 **111111** (*Up 2*), 8 **1234567** (*Up 5*), 9 **iloveyou** (*Up 2*), 10 **adobe123** (*New*), 11 **123123** (*Up 5*), 12 **admin** (*New*), 13 **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*)

splashdata

What is a good password?

- Eight characters or longer. The longer, the better.
- Mixed case (lower and upper case letters), with a number, and a symbol.
- Something you'll easily remember.
- Eg. M@rvinthem@rtian, D@ffyduck!, TrueBl00d, Gam3ofThron3s!, Cak3syearbirthd@y, Happydogsmilesatme2, Skippy_peanut_butter_smiles!
- If you have to write it down, it's not a good password.

What's easy to remember and hard to hack?


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^{28} = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^{44}=550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

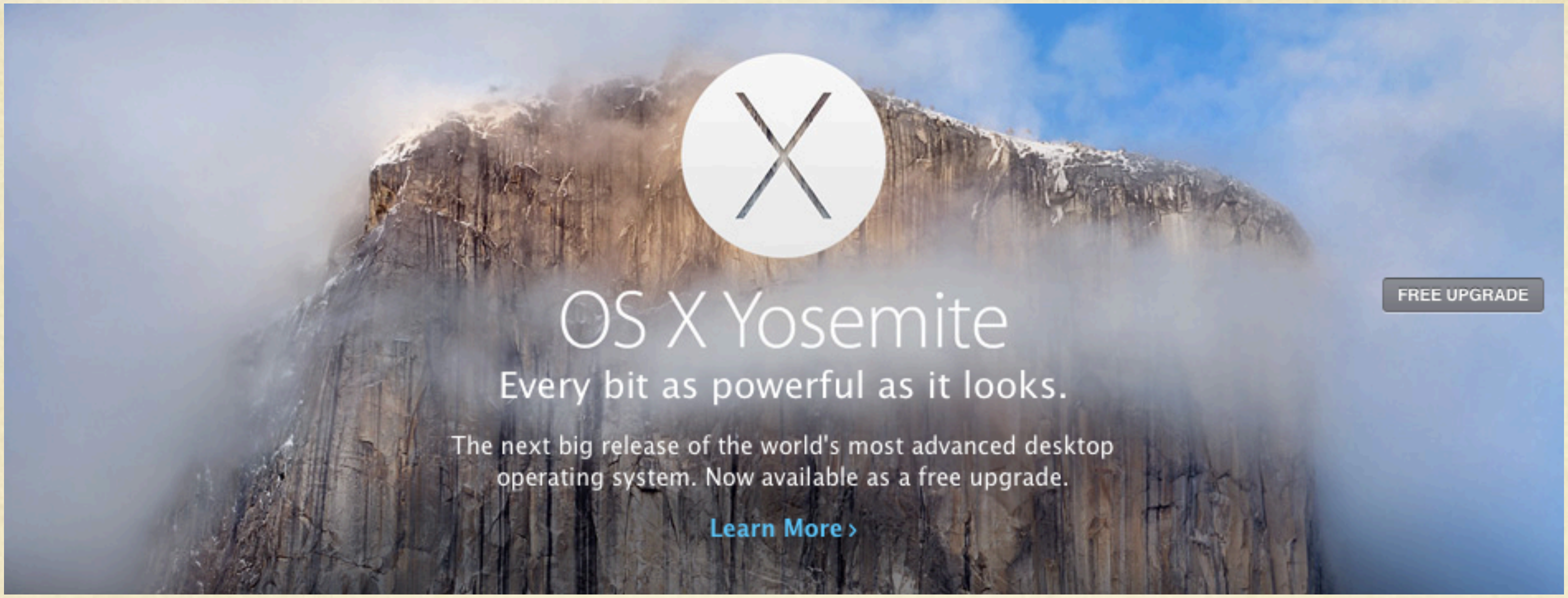
Storing passwords

- Never send or store passwords in email.
- Many of us can end up with as many as 10 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 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.

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



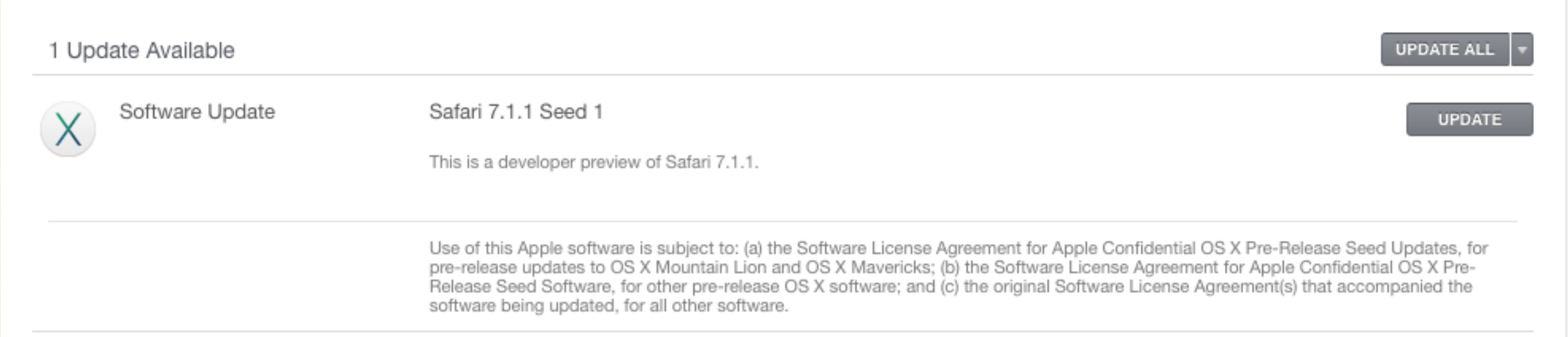
OS X Yosemite

Every bit as powerful as it looks.

The next big release of the world's most advanced desktop operating system. Now available as a free upgrade.

- 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



1 Update Available

Software Update

Safari 7.1.1 Seed 1

This is a developer preview of Safari 7.1.1.

Use of this Apple software is subject to: (a) the Software License Agreement for Apple Confidential OS X Pre-Release Seed Updates, for pre-release updates to OS X Mountain Lion and OS X Mavericks; (b) the Software License Agreement for Apple Confidential OS X Pre-Release Seed Software, for other pre-release OS X software; and (c) the original Software License Agreement(s) that accompanied the software being updated, for all other software.

- 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) usually inherently incompatible with new OS versions. They need time to work out the 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.

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)."

Active hardware vulnerabilities

- Thunderbolt adapters (all) through the Option ROMs

Connect directly to a display with a Thunderbolt or Mini DisplayPort cable or via an adapter

Exploit code can be passed through the Option ROM of any TB Adapter to a Mac which can then pass the infection 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)

"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 with 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.

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.

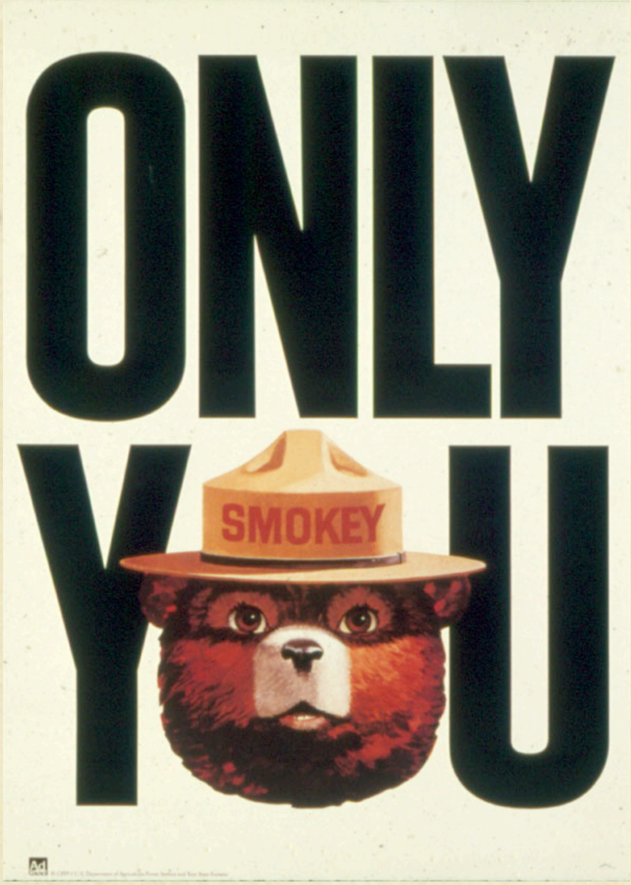
Knowledge

- Knowledge is power.
- The more you learn from talking to us, searching the web for answers, and personal investigations, the better you will be able to discern what is legit and what isn't and 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.

Your Data is Life



- Crash Plan is IS&T's free cloud data backup solution. This solution is a secondary off site backup for your data.
- Crash Plan is NOT a disaster recover solution, it is off site data backup. No application or system files are backed up. Files take as long to bring back from the cloud as they take to save TO the cloud. For users with 50-100 GB of data or more this could take days to a week.
- Remember, ONLY YOU can prevent data loss.