

VCU School of Medicine
Information Security
Best Practices

Dan Han
School of Medicine

Why Security?

- Impact of Security Incidents
 - Loss of critical data
 - Loss of credibility among students and peers
 - Loss of research funds
 - Investigations
 - Lawsuits
 - Regular audits
- Examples: UCLA & CardSystems security incident

Why Security?

- Things that are valuable and important to you, which the thieves may see an incentive to obtain them
- Not much different than our home or automobile security

Why security?

What will happen when you leave your car, house or other valuables unlocked in a bad neighborhood?



You are going to get robbed!

This concept is the same as...

Passwords & Passphrases

Where

Internet = Bad Neighborhood

Your data = your valuables

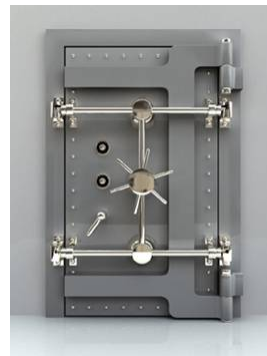
Your passwords and passphrases = your locks



So which lock would you prefer?

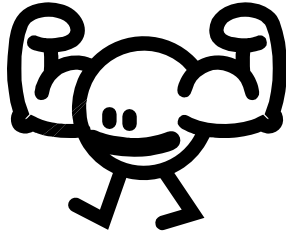


Simple and weak
password



Strong password or
passphrase

So...



Strong



Pass



Word

Point 1 – Strong Passwords

- **Point 1: Always protect your systems and data with a strong passwords or passphrases!**
 - Combination of letters and numbers or unique characters. (e.g. “H4x0r55T”, “W0lver1n3S”)
 - Use of passphrases (e.g. “34t my 5h0rts!”, “1 L0ve p1zzA”)
 - Never leave your password laying around.
 - Use multiple layers of passwords (like multiple locks)
 - Logon
 - ScreenSaver
 - BIOS



However...

When you are in a really bad neighborhood...

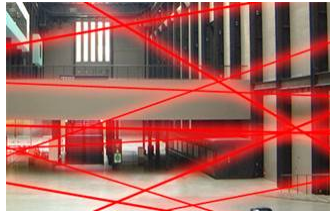
- Locks just aren't enough to protect you...



This is where alarm and theft deterrent systems come in...

Anti-virus, Firewall and Anti-Malware software = Alarms and Theft Deterrent systems

But...



These system must be kept up-to-date in order to be effective...

Point 2 – Antivirus

- **Point 2 – Always keep VCU approved and up-to-date antivirus (For PC and Mac)**
 - Sophos
 - Get it at <http://www.ts.vcu.edu/security/virus.html>
 - Also available for your home machine if you are a VCU employee.
 - **Do not** install two Anti-virus systems



Point 3 – Firewall and Anti-Malware

- **Point 3 – Always keep up-to-date anti-spyware software and firewall on your computer**
 - Only use reputable firewall and anti-spyware software
 - Stateful Inspection Firewall (Windows Firewall)
 - Spybot S & D or Ad-Aware (get it at download.com)



And since we are talking about up-to-date...

Software



Outdated software is like a broken window.



Updates are like a Window repairman, who will patch your broken window for you.

Point 4 - Update

- **It is also imperative to keep your Operating System (Windows, Mac OS etc.) and software (Office, Firefox, iTunes etc.) up-to-date**
 - Most operating systems and some software packages come with automatic updates.
 - Make sure the automatic updates are turned on.
 - Periodically check within other software packages for updates.



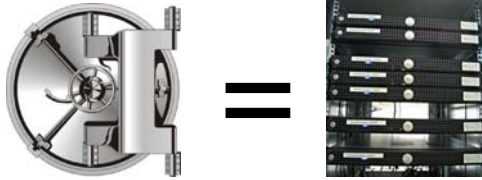
What if...

- The things you possess is so valuable, that you cannot afford to lose it?
 - Option 1: Build your own vault, hire armed guards, establish a 24 hour patrol etc.
 - Option 2: Deposit the valuables in a bank or any centrally managed secure facility



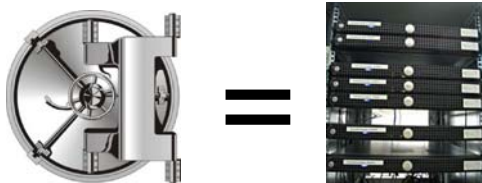
The concept of a vault or a bank...

- Is the same as a network shared storage...
 - Centrally managed
 - Protected against attacks
 - Fault tolerant
 - Controlled access



Point 5 – Network Storage

- **Store all confidential and sensitive data on VCU or VCUHS centrally managed servers.**
 - Individually Identifiable Health Information (PHI)
 - Personal Identifiable Information
 - SSNs
 - Credit Card and VCUCard Numbers
 - Other important information such as documentations etc.



Since we are talking about network storage...



Fault tolerant - Backs up your data

So... How important are backups?

You don't need it until something happens

Hard drives are mechanical devices that can fail at any time and due to various causes...

Not backing up of your important data is like driving in a desert with no spare tire or water



O boy, I wish I had that spare tire...

Point 6 – Backup

- **Create multiple backups of your most important data**
 - Use Network storage (Always backed up), External hard drives and USB drives etc.
 - Sensitive and Personally identifiable information **should only be stored** on the server
 - Consider encrypting data backed up on external storage devices

Next...

We will talk about Trust...

- Scenario: An air conditioner repair man comes to your house in the bad neighborhood and said he is here to service your air conditioner, do you let him in your house?

Depends?

- Is my air conditioner broken?
- Did I schedule for him to come?
- Does he look like a repair man?
- Is he with who he says he is with?

Point 7 – Email Awareness

- **Do not trust emails and attachments sent by anyone**
 - Do you know the sender?
 - Are you expecting an email or attachment from this person?
 - Is the email asking for your personal information?
 - Does this sound too good to be true?
 - Is this email using correct grammar?

Conversely...

Point 8 – Website Awareness

- Avoid less reputable and suspicious websites
 - Did I get this link from a suspicious email?
 - Does this site sound legit? (ex. 227799.net or gigilm.com)
 - Is the spelling of the website address correct? (ex. Ghoogle.com, Yohoo.com etc.)
 - Does the website prompt you to install something?

Software Security

- The installation of many software packages are like adding glass windows and doors to your house.
 - Privacy issues
 - Entry points for bad guys
- Choosing software to install is just like choosing a Window or door for your house.
- When choosing a Window or a door, we must be sure it has:
 - Lock (proper safety mechanisms)
 - Build quality
 - Warranty or support



Point 9 – Other Infection Sources

- **Be aware of other means of infection:**
 - Instant Messaging
 - Skype and its cousins
 - GoToMyPC.com and its cousins
 - Chat rooms
 - Peer-to-Peer (P2P) networking
 - Facebook and Myspace
 - Poorly configured machines (Windows file and printer share etc.)

Finally...

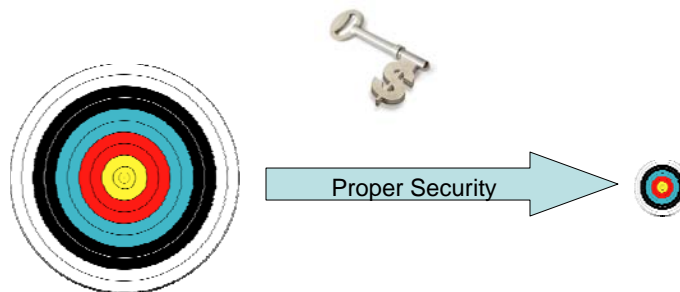
Point 10 - Physical Security

- **Be aware of the “social engineers” among us...**
 - What are Social Engineers?
 - Con artists and thieves
 - Gathers information through interactions with the victim.
 - Physical Security (Best practices):
 - Lock your computer when you step away from it.
 - Lock your office when you step out.
 - Shut off your computer every night unless told not to.
 - Be aware of strangers in your area.
 - Be aware of overly friendly strangers and do not offer sensitive information
 - Keep an eye out for anything abnormal

Phew... So are we safe now?

NOPE!

There are always going to be risks...



Goal: Minimize the attack target through the use of proper security

Contact Information:
Dan Han
s2dhan@vcu.edu

Questions?