

Safe Computing: Lower Exposure and Risk

Presented by: Emyll Almonte
IT Systems Administrator

Disclaimer

Any instruction / proof-of-concept shown on this presentation has been done on systems owned by me, is for educational purposes only, and most of the information disclosed is readily available on the internet. I am not responsible for what you do with the information, even though as cybersecurity professionals, you need to understand the different forms of attack in order to come up with a protection plan.

What is “Safe Computing” ?

- In simple terms: Safe Computing combines the use of cybersecurity best practices, physical precautions with your equipment, and common sense.
- One of many online definitions: Safe Computing involves using available tools to aid the protection of computer systems from theft, infiltration, exfiltration, damage to the hardware, software, electronic data, as well as from the disruption or misdirection of the services they provide.
- Computers are up against hardware malfunctions, viruses, malware, adware, phishing, hijacking, spyware, identity theft, ransomware, and so on..

Exposure and Risks?

- Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. Protecting the system from exposure doesn't necessarily protect the user (email phishing, online scams, etc).
- These cyber/digital attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.
- As IT Professionals, we must focus on figuring out ways to lower the risk of our systems and their users from such attacks because there is no tool or software that can protect with 100% guarantee.

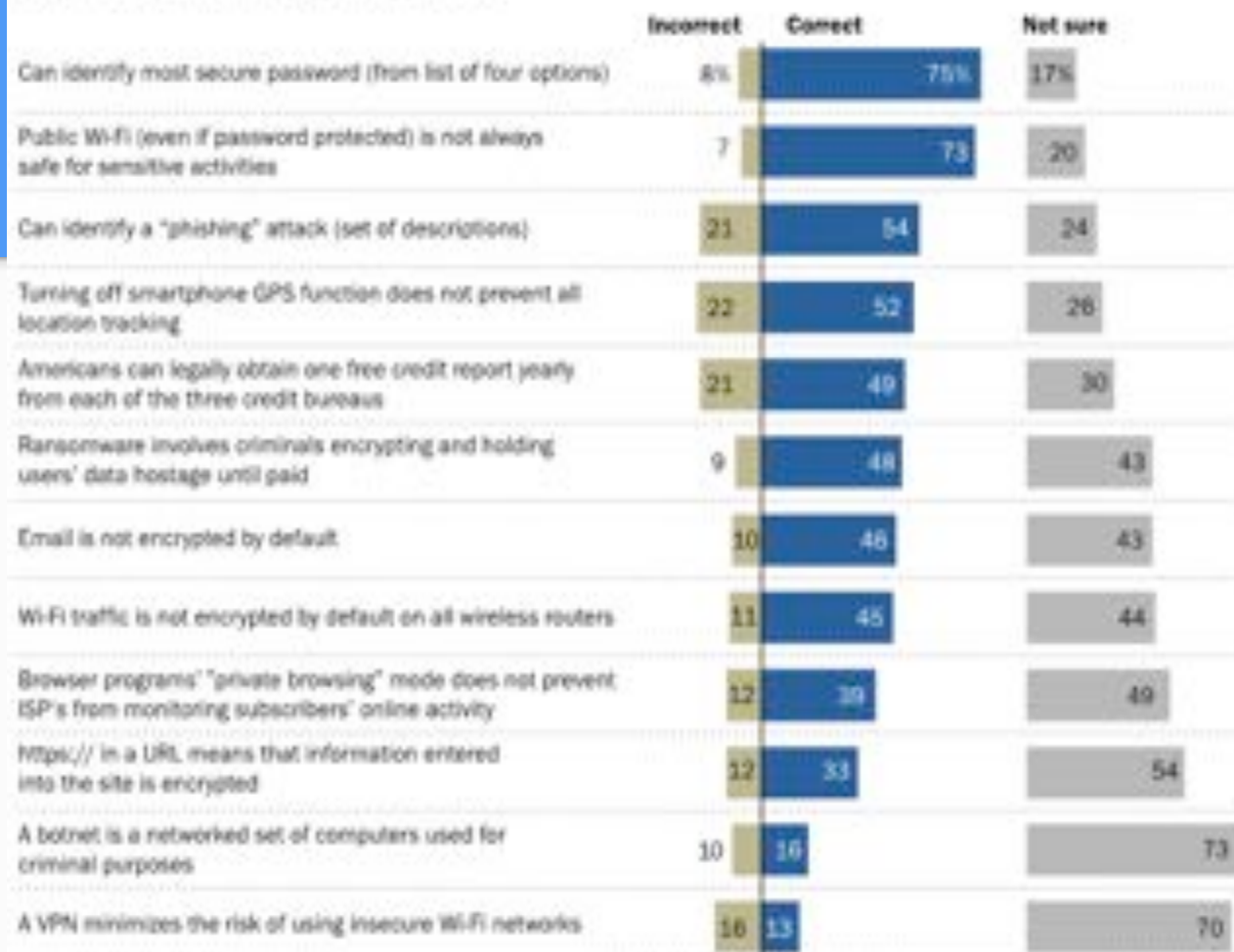
“ Click here to
protect your
account! ”

The average computer user
has very basic general
knowledge and
understanding of
cybersecurity and how
networks function overall..

It's up to us to protect them
as much as possible..

Many Americans are unsure on a range of cybersecurity topics

% of Internet users answering each question —




```
Oct 09 00:12:11 ip-172-31-16-216.us-east-2.compute.internal sshd[8395]: Invalid user Isabella02017 from 51.38.98.23 port 47594
Oct 09 00:14:00 ip-172-31-16-216.us-east-2.compute.internal sshd[8420]: Invalid user 123 from 159.65.30.66 port 59714
Oct 09 00:15:32 ip-172-31-16-216.us-east-2.compute.internal sshd[8444]: Invalid user 12345678xcvbnm from 45.77.137.186 port 47051
Oct 09 00:16:08 ip-172-31-16-216.us-east-2.compute.internal sshd[8446]: Invalid user Project from 51.38.98.23 port 58790
Oct 09 00:17:34 ip-172-31-16-216.us-east-2.compute.internal sshd[8456]: Invalid user P4ssw0rd_183 from 159.65.30.66 port 42360
Oct 09 00:19:19 ip-172-31-16-216.us-east-2.compute.internal sshd[8482]: Invalid user 12345678xcvbnm from 45.77.137.186 port 38187
Oct 09 00:21:09 ip-172-31-16-216.us-east-2.compute.internal sshd[12082]: Invalid user Psychel23 from 159.65.30.66 port 53242
Oct 09 00:23:05 ip-172-31-16-216.us-east-2.compute.internal sshd[12122]: Invalid user Algorithm2017 from 45.77.137.186 port 57551
Oct 09 00:24:14 ip-172-31-16-216.us-east-2.compute.internal sshd[12136]: Invalid user 123 from 14.63.167.192 port 42096
Oct 09 00:24:48 ip-172-31-16-216.us-east-2.compute.internal sshd[12138]: Invalid user centos2018 from 159.65.30.66 port 35886
Oct 09 00:25:44 ip-172-31-16-216.us-east-2.compute.internal sshd[12156]: Invalid user support from 202.88.241.107 port 47042
Oct 09 00:26:47 ip-172-31-16-216.us-east-2.compute.internal sshd[12166]: Invalid user 4rfr4TG86yhn from 45.77.137.186 port 48687
Oct 09 00:28:28 ip-172-31-16-216.us-east-2.compute.internal sshd[12206]: Invalid user centos2018 from 159.65.30.66 port 46764
Oct 09 00:28:45 ip-172-31-16-216.us-east-2.compute.internal sshd[12211]: Invalid user Password12 from 14.63.167.192 port 53026
Oct 09 00:30:30 ip-172-31-16-216.us-east-2.compute.internal sshd[12280]: Invalid user Sporting2017 from 45.77.137.186 port 39820
Oct 09 00:32:07 ip-172-31-16-216.us-east-2.compute.internal sshd[12303]: Invalid user 123Live from 159.65.30.66 port 57646
Oct 09 00:33:21 ip-172-31-16-216.us-east-2.compute.internal sshd[12651]: Invalid user Hotel02017 from 14.63.167.192 port 35612
Oct 09 00:34:04 ip-172-31-16-216.us-east-2.compute.internal sshd[12657]: Invalid user Sporting2017 from 45.77.137.186 port 59186
Oct 09 00:35:45 ip-172-31-16-216.us-east-2.compute.internal sshd[12684]: Invalid user Parolal238 from 159.65.30.66 port 40290
Oct 09 00:37:51 ip-172-31-16-216.us-east-2.compute.internal sshd[12704]: Invalid user p4ssw0rd082017 from 45.77.137.186 port 50322
Oct 09 00:37:57 ip-172-31-16-216.us-east-2.compute.internal sshd[12706]: Invalid user USA02018 from 14.63.167.192 port 46498
Oct 09 00:39:27 ip-172-31-16-216.us-east-2.compute.internal sshd[14714]: Invalid user Willkommen-123 from 159.65.30.66 port 51168
Oct 09 00:41:35 ip-172-31-16-216.us-east-2.compute.internal sshd[14824]: Invalid user Password2020 from 45.77.137.186 port 41455
Oct 09 00:42:26 ip-172-31-16-216.us-east-2.compute.internal sshd[14826]: Invalid user 123Dex from 14.63.167.192 port 57384
Oct 09 00:43:08 ip-172-31-16-216.us-east-2.compute.internal sshd[14833]: Invalid user Infinity123 from 159.65.30.66 port 33818
Oct 09 00:45:22 ip-172-31-16-216.us-east-2.compute.internal sshd[15027]: Invalid user P4ssw0rd08123 from 45.77.137.186 port 60833
Oct 09 00:46:53 ip-172-31-16-216.us-east-2.compute.internal sshd[15514]: Invalid user Toys123 from 159.65.30.66 port 44696
Oct 09 00:46:59 ip-172-31-16-216.us-east-2.compute.internal sshd[15521]: Invalid user Press02017 from 14.63.167.192 port 40048
Oct 09 00:49:06 ip-172-31-16-216.us-east-2.compute.internal sshd[17876]: Invalid user P4ssw0rd08123 from 45.77.137.186 port 51972
Oct 09 00:49:30 ip-172-31-16-216.us-east-2.compute.internal sshd[18116]: Invalid user 123 from 159.65.137.23 port 34348
Oct 09 00:50:44 ip-172-31-16-216.us-east-2.compute.internal sshd[18207]: Invalid user Null12017 from 159.65.30.66 port 55572
Oct 09 00:51:40 ip-172-31-16-216.us-east-2.compute.internal sshd[18211]: Invalid user lqw23er4 from 14.63.167.192 port 50822
Oct 09 00:53:04 ip-172-31-16-216.us-east-2.compute.internal sshd[18228]: Invalid user Nullen01233 from 45.77.137.186 port 43101
Oct 09 00:53:55 ip-172-31-16-216.us-east-2.compute.internal sshd[18233]: Invalid user Tel0123 from 159.65.137.23 port 56658
Oct 09 00:54:31 ip-172-31-16-216.us-east-2.compute.internal sshd[18239]: Invalid user Pass02017 from 159.65.30.66 port 38222
Oct 09 00:56:15 ip-172-31-16-216.us-east-2.compute.internal sshd[18254]: Invalid user lqw23er4 from 14.63.167.192 port 33572
Oct 09 00:57:02 ip-172-31-16-216.us-east-2.compute.internal sshd[18260]: Invalid user 123Chain from 45.77.137.186 port 34245
Oct 09 00:58:11 ip-172-31-16-216.us-east-2.compute.internal sshd[18269]: Invalid user West02017 from 159.65.137.23 port 49982
Oct 09 00:58:32 ip-172-31-16-216.us-east-2.compute.internal sshd[18274]: Invalid user LowLow123 from 159.65.30.66 port 49100
Oct 09 01:00:49 ip-172-31-16-216.us-east-2.compute.internal sshd[18286]: Invalid user Xew2lqar from 14.63.167.192 port 44452
Oct 09 01:00:59 ip-172-31-16-216.us-east-2.compute.internal sshd[18290]: Invalid user Admin020 from 45.77.137.186 port 53605
Oct 09 01:02:17 ip-172-31-16-216.us-east-2.compute.internal sshd[18313]: Invalid user Cannes_123 from 159.65.30.66 port 59982
Oct 09 01:02:28 ip-172-31-16-216.us-east-2.compute.internal sshd[18311]: Invalid user P855w0rd082015 from 159.65.137.23 port 43294
Oct 09 01:04:52 ip-172-31-16-216.us-east-2.compute.internal sshd[18342]: Invalid user Antoine-123 from 45.77.137.186 port 44736
Oct 09 01:05:23 ip-172-31-16-216.us-east-2.compute.internal sshd[18356]: Invalid user Psyche_123 from 14.63.167.192 port 55354
Oct 09 01:06:23 ip-172-31-16-216.us-east-2.compute.internal sshd[18363]: Invalid user 123Premium from 159.65.30.66 port 42628
Oct 09 01:06:50 ip-172-31-16-216.us-east-2.compute.internal sshd[18366]: Invalid user 123Winter from 159.65.137.23 port 36828
Oct 09 01:08:58 ip-172-31-16-216.us-east-2.compute.internal sshd[18372]: Invalid user 5tgb8NY*7ujm from 45.77.137.186 port 35881
Oct 09 01:09:58 ip-172-31-16-216.us-east-2.compute.internal sshd[18383]: Invalid user P855w0rd082020 from 14.63.167.192 port 38004
Oct 09 01:10:12 ip-172-31-16-216.us-east-2.compute.internal sshd[18387]: Invalid user P4SSW0RD082020 from 159.65.30.66 port 53504
Oct 09 01:11:14 ip-172-31-16-216.us-east-2.compute.internal sshd[18417]: Invalid user 123Lobater from 159.65.137.23 port 58764
[root@ip-172-31-16-216 conf]#
```

... Just minutes after turning on one of my Amazon EC2 instances.

... Imagine an out of the box computer being used by the average user with default settings.

“Keep all software up-to-date, he said”

- Do not trust that your data or system is 100% safe just because you installed a firewall, antivirus or anti-malware software..

MD5: message digest

SHA: secure hashing algorithm

www.theverge.com > [ccleaner-hack-malware-security](#) ▼

Hackers hid malware in CCleaner software - The Verge

Sep 18, 2017 - Hackers have successfully breached CCleaner's security to inject malware into the app ... An unusual attack on software update mechanisms.

www.vice.com > [en_us](#) > [article](#) > [hackers-hijacked-asus-software-upd...](#) ▼

Hackers Hijacked ASUS Software Updates to Install ... - Vice

Mar 25, 2019 - Two different attacks discovered in 2017 also compromised trusted software updates. One involved the computer security cleanup tool known as CCleaner that was delivering malware to customers via a software update. More than 2 million customers received that malicious update before it was discovered.

File Edit View Search Terminal Help

```
eagr@eadebian:~$ cat file1
```

```
this is file 1
```

```
1234567890
```

```
eagr@eadebian:~$ cat file2
```

```
this is file 1
```

```
1234576890
```

```
eagr@eadebian:~$ cat file3
```

```
this is file 1
```

```
1234567890
```

```
eagr@eadebian:~$ md5sum file1 file2 file3
```

```
3663b8dbfb125398a3a279ee70c35e12 file1
```

```
c5e55be7448b57372c0b5581e99a83e5 file2
```

```
3663b8dbfb125398a3a279ee70c35e12 file3
```

```
eagr@eadebian:~$ shasum file1 file2 file3
```

```
e008800d102b65ffccdc3840a861e9bfbe2b84b file1
```

```
087d0d94fb7125e8eba46570a4a8a2d7626c8fb3 file2
```

```
e008800d102b65ffccdc3840a861e9bfbe2b84b file3
```


“Keep all software up-to-date, he said”

- Do not trust that your data or system is 100% safe just because you installed a firewall, antivirus or anti-malware software..

SHA256

Before writing an image to DVD or USB drive, it is highly recommended that you follow the instructions, please see [HowToSHA256SUM](#). Below is a list of SHA256 sums to

kubuntu-19.10-desktop-amd64.iso : e56388512a0610bd991192b197a1311496c

kubuntu-18.04.3-desktop-amd64.iso : 9c98cda0d3b95b4776a55c7908560917a

kubuntu-18.04.3-desktop-i386.iso : 0eeb5fc7b6492f5f114c3ae814ad5033c335f17

MD5SUM

You can also check the ISO using MD5SUM as well:

kubuntu-19.10-desktop-amd64.iso : 9854741e5f8ecc349fcd073ea13f2ea

kubuntu-18.04.3-desktop-amd64.iso : a8e0652262ab3588130c7588e680901e

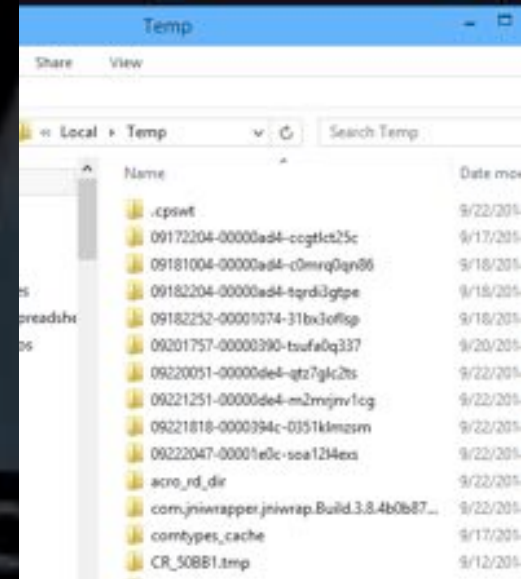
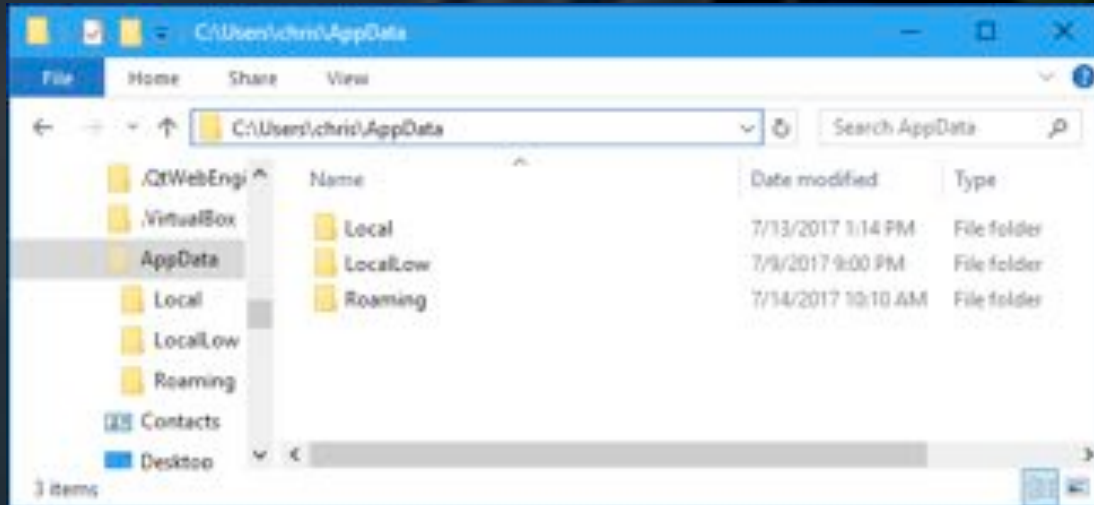
kubuntu-18.04.3-desktop-i386.iso : 327a061de91bb051e5e75d60cbd97909

```
Administrator: Command Prompt
C:\Users\Administrator\Downloads>certutil -hashfile kubuntu-18.04.3-desktop-amd64.iso md5
MD5 hash of kubuntu-18.04.3-desktop-amd64.iso:
a8e0652262ab3588130c7588e680901e
CertUtil: -hashfile command completed successfully.
```

...What is the difference between encryption, hashing, and checksum?

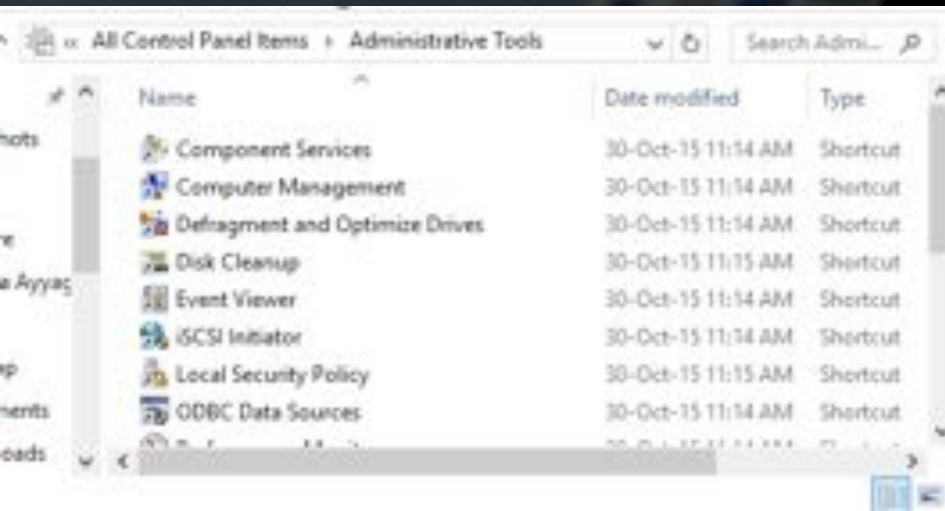
Safe Computing: the OS + Network + Apps

- Prepare the OS before letting anyone touch it, configure the system using best practices: (depends on the use case {government, banking, grandma})
 - Setup user access to lower attack surface (thus lowering risk)
 - Intrusion comparison {admin vs standard vs guest}
 - Appdata folder vs System folder {adware/malware}



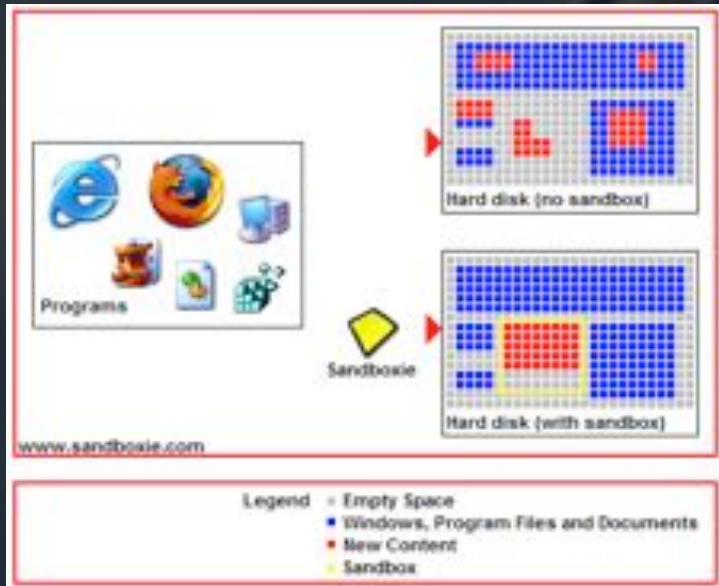
Safe Computing: the OS + Network + Apps

- Prepare the OS before letting anyone touch it, configure the system using best practices: (depends on the use case {government, banking, grandma})
 - Setup user access to lower attack surface (thus lowering risk)
 - Intrusion comparison {admin vs standard vs guest}
 - Appdata folder vs System folder {adware/malware}



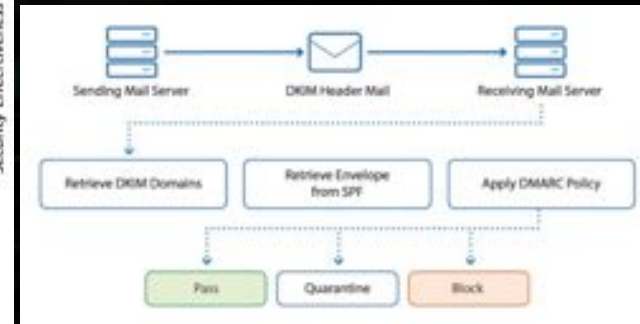
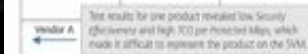
Safe Computing: the OS + Network + Apps

- Prepare the OS before letting anyone touch it, configure the system using best practices: (depends on the use case {government, banking, grandma})
 - Setup user access to lower attack surface (thus lowering risk)
 - Intrusion comparison {admin vs standard vs guest}
 - Appdata folder vs System folder {adware/malware}
 - Sandboxing (apps) or DeepFreeze (system)



HOME USER WINDOWS

- 100

www.garrett.org

Safe Computing: the OS + Network + Apps

- Prepare the OS before letting anyone touch it, configure the system using best practices: (depends on the use case {government, banking, grandma})
 - Install verified software (Firewall, AV, Antimalware, Anti-phishing, Encryption)
 - Compare products using NSS Labs and AV-Test results
 - Sender Policy Framework and DomainKeys Identified Mail
 - Bitdefender, Avast, Lulu, Snort, OpenDNS, Sandboxie, Firejail..



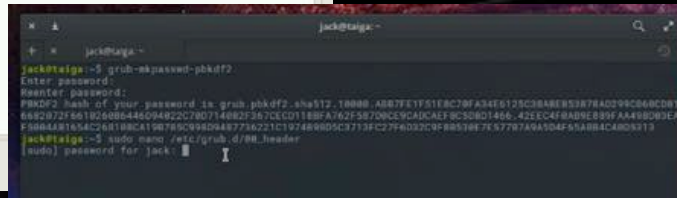
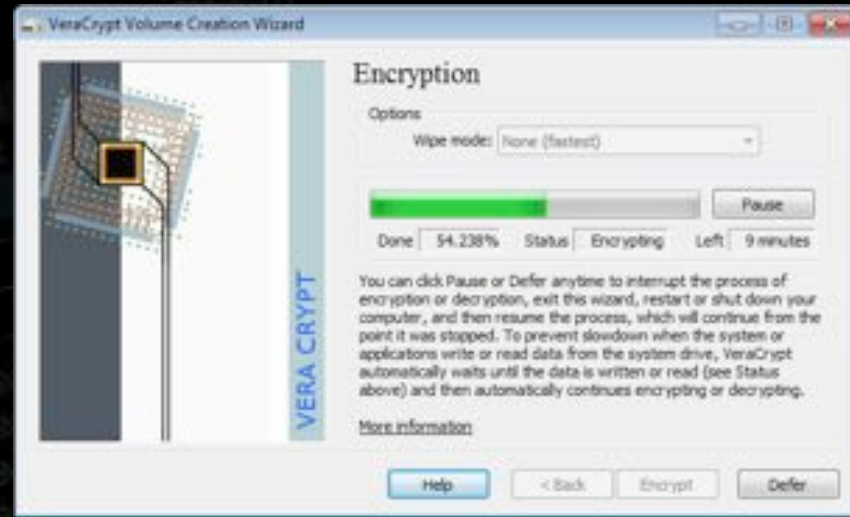
Safe Computing: the OS + Network + Apps

- Prepare the OS before letting anyone touch it, configure the system using best practices: (depends on the use case {government, banking, grandma})
 - Install security extensions/add-ons on browser if necessary.. Balance between usability and protection..
 - uBlock, NoScript, Privacy Badger, VirusTotal, HTTPS Everywhere..



Safe Computing: the OS + Network + Apps

- Prepare the OS before letting anyone touch it, configure the system using best practices: (depends on the use case {government, banking, grandma})
 - Install verified software (Firewall, AV, Antimalware, Anti-phishing, Encryption)
 - Compare products using NSS Labs and AV-Test results
 - Sender Policy Framework and DomainKeys Identified Mail
 - Bitdefender, Avast, Lulu, Snort, OpenDNS, Sandboxie, Firejail..
 - Entire Disk/Volume/System Encryption (VeraCrypt, LUKS, FileVault), TPM-chips..



Safe Computing: the OS (linux)

- If you don't password-protect the bootloader and volume with encryption...

```
kubuntu@kubuntu:~$ sudo su
root@kubuntu:/home/kubuntu# mkdir /mnt/recover
root@kubuntu:/home/kubuntu# mount /dev/
Display all 218 possibilities? (y or n)
root@kubuntu:/home/kubuntu# mount /dev/sda
sda sda1 sda2 sda5
root@kubuntu:/home/kubuntu# mount /dev/sda2 /mnt/recover/
mount: /mnt/recover: wrong fs type, bad option, bad superblock on /dev/sda2, missing codepage or helper program, or other error:
root@kubuntu:/home/kubuntu# mount /dev/sda1 /mnt/recover/
root@kubuntu:/home/kubuntu# ls -lah /mnt/recover/
total 188K
drwxr-xr-x 21 root root 4.0K Oct 18 2017 .
drwxr-xr-x  1 root root  60 Feb  2 01:08 ..
drwxr-xr-x  2 root root 4.0K Oct 18 2017 bin
drwxr-xr-x  3 root root 4.0K Oct 18 2017 boot
drwxr-xr-x  4 root root 4.0K Oct 18 2017 dev
drwxr-xr-x 126 root root 12K Feb  2 00:45 etc
drwxr-xr-x  3 root root 4.0K Oct 18 2017 home
lnsdrwxrwx  1 root root  31 Oct 18 2017 initrd.img -> boot/initrd.img-4.9.0-4-686-pae
lnsdrwxrwx  1 root root  31 Oct 18 2017 initrd.img.old -> boot/initrd.img-4.9.0-4-686-pae
drwxr-xr-x 16 root root 4.0K Oct 18 2017 lib
drwx----- 2 root root 16K Oct 18 2017 lost+found
drwxr-xr-x  3 root root 4.0K Oct 18 2017 media
drwxr-xr-x  2 root root 4.0K Oct 18 2017 mnt
drwxr-xr-x  3 root root 4.0K Oct 11 2017 opt
drwxr-xr-x  2 root root 4.0K Jul 13 2017 proc
drwx----- 16 root root 4.0K Oct 18 2017 root
drwxr-xr-x  2 root root 4.0K Oct 18 2017 run
drwxr-xr-x  2 root root 4.0K Oct 18 2017/sbin
drwxr-xr-x  2 root root 4.0K Oct 18 2017/srv
drwxr-xr-x  2 root root 4.0K Jul 13 2017/sys
drwxrwxrwt  8 root root 4.0K Feb  2 01:02 tmp
drwxr-xr-x 10 root root 4.0K Oct 18 2017/usr
drwxr-xr-x 11 root root 4.0K Oct 18 2017/var
lnsdrwxrwx  5 root root  30 Oct 18 2017 vmlinuz -> boot/vmlinuz-4.9.0-4-686-pae
```

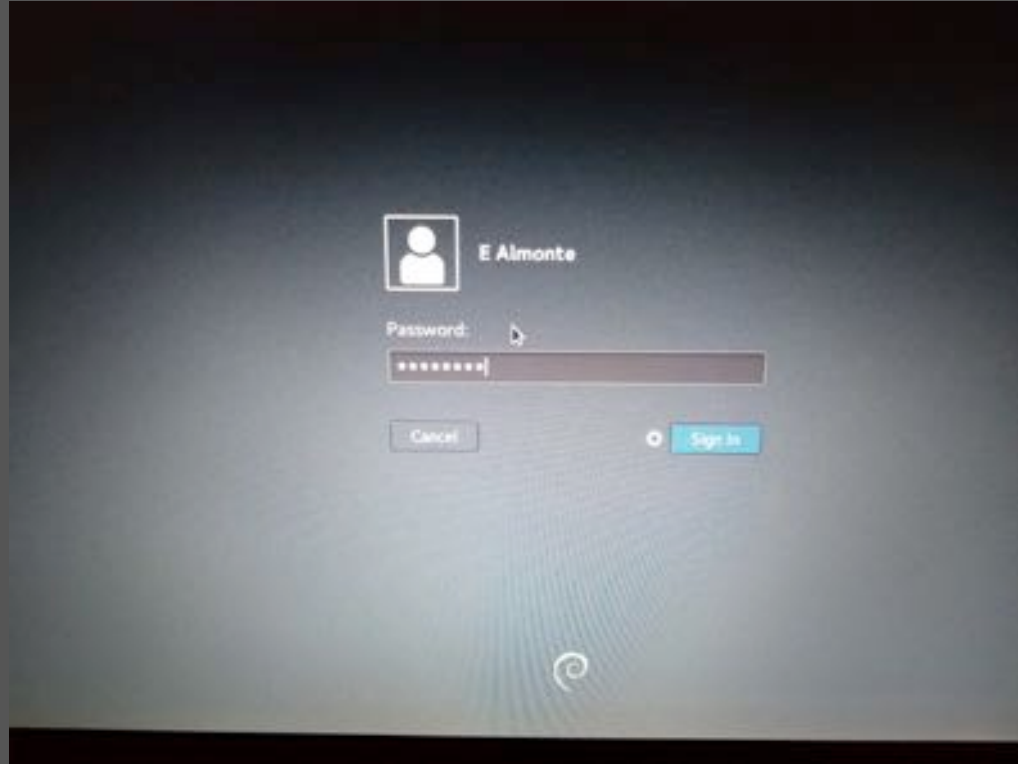
Safe Computing: the OS (linux)

- If you don't password-protect the bootloader and volume with encryption...

```
drwxr-xr-x  2 root root 4.0K Oct 10 2017 sys
drwxr-xr-x  2 root root 4.0K Jul 13 2017 sys
drwxrwxrwt  8 root root 4.0K Feb  2 01:02 tmp
drwxr-xr-x 10 root root 4.0K Oct 10 2017 usr
drwxr-xr-x 11 root root 4.0K Oct 10 2017 var
lnwxwxrwx  1 root root  28 Oct 10 2017 vmlinuz -> boot/vmlinuz-4.9.0-4-686-pae
lnwxwxrwx  1 root root  28 Oct 10 2017 vmlinuz.old -> boot/vmlinuz-4.9.0-4-686-pae
root@kubuntu:/home/kubuntu# chroot /mnt/recover/
root@kubuntu:/# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@kubuntu:/# ls /home/
ealmonite
root@kubuntu:/# passwd ealmonite
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@kubuntu:/# exit
exit
root@kubuntu:/home/kubuntu# um
umask          umask_pp          umount          umount.udisks2
root@kubuntu:/home/kubuntu# umount /mnt/recover
root@kubuntu:/home/kubuntu#
```

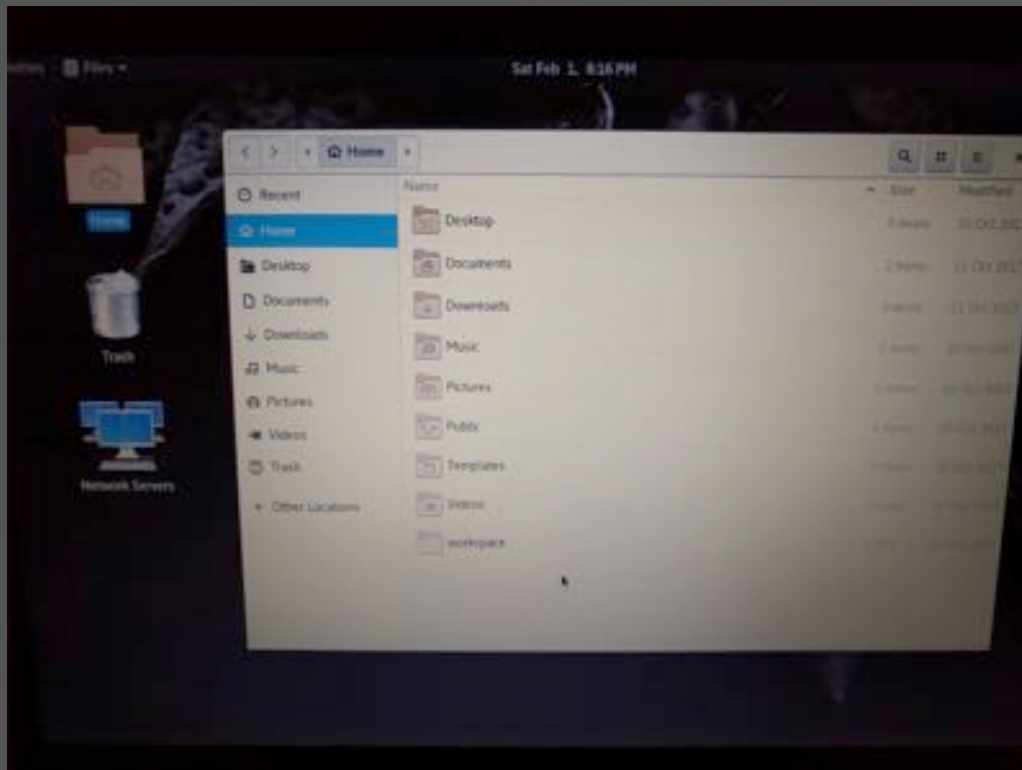
Safe Computing: the OS (linux)

- If you don't password-protect the bootloader and volume with encryption...



Safe Computing: the OS (linux)

- If you don't password-protect the bootloader and volume with encryption...



Safe Computing: the OS (windows)

- If you don't password-protect the bootloader and volume with encryption...

```
kubuntu@kubuntu:~$ sudo su
root@kubuntu:/home/kubuntu# mkdir /mnt/recover1
root@kubuntu:/home/kubuntu# mount /dev/
Display all 224 possibilities? (y or n)
root@kubuntu:/home/kubuntu# mount /dev/sda
sda sda1 sda2 sda3 sda4
root@kubuntu:/home/kubuntu# mount /dev/sda1 /mnt/recover1/
root@kubuntu:/home/kubuntu# ls /mnt/recover1/
Recovery/                               System Volume Information/
root@kubuntu:/home/kubuntu# mount /dev/sda2 /mnt/recover2/
mount: /mnt/recover2/: mount point does not exist.
root@kubuntu:/home/kubuntu# mkdir /mnt/recover2
root@kubuntu:/home/kubuntu# mkdir /mnt/recover3
root@kubuntu:/home/kubuntu# mkdir /mnt/recover4
root@kubuntu:/home/kubuntu# mount /dev/sda2 /mnt/recover2/
root@kubuntu:/home/kubuntu# mount /dev/sda3 /mnt/recover3/
mount: /mnt/recover3: wrong fs type, bad option, bad superblock on /dev/sda3, missing codepage or helper program, or other error.
root@kubuntu:/home/kubuntu# mount /dev/sda4 /mnt/recover4/
root@kubuntu:/home/kubuntu# ls /mnt/recover4/
Desktop Authority/  Intel/  PerfLogs/  Program Files (x86)/  swapfile.sys  Windows/
Documents and Settings/  MSOCache/  ProgramData/  Recovery/  System Volume Information/  windows10Upgrade/
hiberfil.sys  pagefile.sys  Program Files/  $Recycle.Bin/  Users/
root@kubuntu:/home/kubuntu# cd /mnt/recover4/Windows/System32/con
conctrl140.dll  configmanager2.dll  connect.dll  console.dll  control.exe  convertvhd.exe
config/  cschost.exe  consent.exe  container.dll  convert.exe
root@kubuntu:/home/kubuntu# cd /mnt/recover4/Windows/System32/config
root@kubuntu:/mnt/recover4/Windows/System32/config#
```

Safe Computing: the OS (windows)

- If you don't password-protect the bootloader and volume with encryption...

```
kubu
File Edit View Bookmarks Settings Help
mount: /mnt/recover3: wrong fs type, bad option, bad superblock on /dev/sda3, missing code
root@kubuntu:/home/kubuntu# mount /dev/sda4 /mnt/recover4/
root@kubuntu:/home/kubuntu# ls /mnt/recover4/
Desktop Authority/ Intel/ PerfLogs/ Program Files/
Documents and Settings/ MSOCache/ ProgramData/ Recovery/
hiberfil.sys pagefile.sys Program Files/ $Recycle
root@kubuntu:/home/kubuntu# cd /mnt/recover4/Windows/System32/con
conctrl140.dll configmanager2.dll connect.dll console.dll control.es
config/ conhost.exe consent.exe container.dll convert.e
root@kubuntu:/home/kubuntu# cd /mnt/recover4/Windows/System32/config
root@kubuntu:/mnt/recover4/Windows/System32/config# /usr/sbin/chntpw -t SAM
chntpw version 1.99 148201, (C) Peter N Hogen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001820 ^ Subkey indexing type is: 606c <h>
File size 65536 [10000] bytes, containing 10 pages (= 1 headerpage)
Used for data: 299/29416 blocks/bytes, unused: 13/23512 blocks/bytes.

===== chntpw Main Interactive Menu =====
Loaded hives: <SAM>

1 - Edit user data and passwords
2 - List groups
- - -
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] -> 1

===== chntpw Edit User Info & Passwords =====
RID  Username  Admin?  Lock?
01f4 Administrator ADMIN
01f7 DefaultAccount dis/lock
01f5 Guest dis/lock
01f8 WDAGUtilityAccount dis/lock

Please enter user number (RID) or 0 to exit: [1f4] 01f4
```

Safe Computing: the OS (windows)

- If you don't password-protect the bootloader and volume with encryption...

```
Please enter user number (RID) or 0 to exit: [1f4] 01f4
***** USER EDIT *****

RID      : 0500 [01f4]
Username: Administrator
fullname:
comment  : Built-in account for administering the computer/domain
homedir  :

00000220 = Administrators (which has 2 members)

Account bits: 0x0210 =
[ ] Disabled           | [ ] Homedir req.      | [ ] Psswd not req. |
[ ] Temp. duplicate    | [X] Normal account   | [ ] RMS account   |
[ ] Domain trust ac   | [ ] Wks trust act.   | [ ] Srv trust act  |
[X] Pwd don't expir   | [ ] Auto lockout     | [ ] (unknown 0x08) |
[ ] (unknown 0x10)    | [ ] (unknown 0x20)   | [ ] (unknown 0x40) |

Failed login count: 0, while max tries is: 0
Total login count: 109

- - - - User Edit Menu:
1 - Clear (blank) user password
2 - Unlock and enable user account) [seems unlocked already]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > █
```


Safe Computing: the OS (windows)

- If you don't password-protect the bootloader and volume with encryption...

```
Failed login count: 0, while max tries is: 0
Total login count: 100

- - - User Edit Menu:
1 - Clear (blank) user password
(2 - Unlock and enable user account) [seems unlocked already]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!
***** USER EDIT *****

RID      : 0x00 [01f4]
Username: Administrator
fullname:
comment  : Built-in account for administering the computer/domain
homedir  :

00000220 = Administrators (which has 2 members)

Account bits: 0x0210 =
[ ] Disabled           [ ] Homedir req.      [ ] Psswd not req.
[ ] Temp. duplicate    [X] Normal account   [ ] NIS account
[ ] Domain trust ac    [ ] Wks trust act.    [ ] Srv trust act
[X] Pwd don't expire   [ ] Auto lockout    [ ] (unknown 0x00)
[ ] (unknown 0x10)    [ ] (unknown 0x20)    [ ] (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 100
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Try login with no password!

- - - User Edit Menu:
1 - Clear (blank) user password
(2 - Unlock and enable user account) [seems unlocked already]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > █
```

Safe Computing: the OS (windows)

- If you don't password-protect the bootloader and volume with encryption...

```
00000220 = Administrators (which has 2 members)

Account bits: 0x0210 =
[ ] Disabled           | [ ] Homedir req.      | [ ] Passwd not req. |
[ ] Temp. duplicate    | [X] Normal account    | [ ] MMS account     |
[ ] Domain trust ac    | [ ] Wks trust act.    | [ ] Srv trust act   |
[X] Pwd don't expir    | [ ] Auto logout      | [ ] (unknown 0x00)  |
[ ] (unknown 0x10)     | [ ] (unknown 0x20)   | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total login count: 100
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Try login with no password!

- - - User Edit Menu:
1 - Clear (blank) user password
(2) - Unlock and enable user account [seems unlocked already]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > q

<-----> cheipw Main Interactive Menu <----->

Loaded hives: <SAM>

1 - Edit user data and passwords
2 - List groups
- - -
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] -> q

Hives that have changed:
# Name
0 <SAM>
Write hive files? (y/n) [n] : █
```

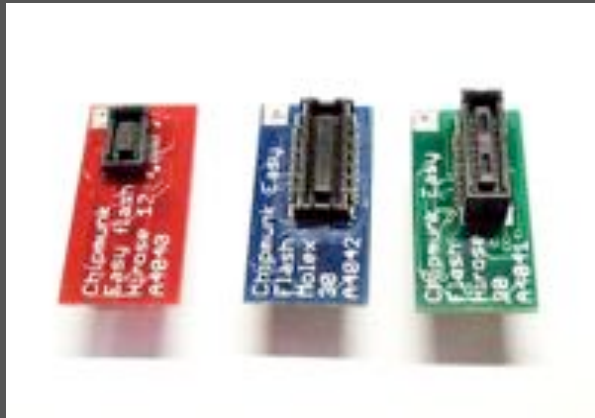
> Exit & reboot, account password cleared.

Safe Computing: the OS (mac)

- If you do password-protect the bootloader but not the volume with encryption...
Can you still haz protekshun?



CMizapper



Safe Computing: the OS (mac)

- If you do password-protect the bootloader but not the volume with encryption...
Can you still haz protekshun?



A4068 Keyboard for use with Medusa

The Medusa allows you to read the serial number from one Mac and write it to another Mac. When you replace the motherboard in a customer's Mac it is nice if the Mac keeps its original serial number.

In case you can not read the original serial number from the old motherboard you can use this keyboard to edit the serial number to the one on the case of the Mac.

This keyboard allows you to edit the serial number stored in the Medusa so that you can write the modified number back to the Mac. Enter letters by holding the corresponding button down for a longer time.



```
eagr@eadebian:~$ nslookup www.icloud.com
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
www.icloud.com canonical name = www-cdn.icloud.com.akadns.net.
www-cdn.icloud.com.akadns.net canonical name = www.icloud.com.edgekey.net.
www.icloud.com.edgekey.net canonical name = e4478.a.akamaiedge.net.
Name:   e4478.a.akamaiedge.net
Address: 23.54.185.223

eagr@eadebian:~$ nslookup www.apple.com
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
www.apple.com canonical name = www.apple.com.edgekey.net.
www.apple.com.edgekey.net canonical name = www.apple.com.edgekey.net.globalredir.akadns.net.
www.apple.com.edgekey.net.globalredir.akadns.net canonical name = e6858.dsce9.akamaiedge.net.
Name:   e6858.dsce9.akamaiedge.net
Address: 184.25.177.104
Name:   e6858.dsce9.akamaiedge.net
Address: 2600:1408:20:193::laca
Name:   e6858.dsce9.akamaiedge.net
Address: 2600:1408:20:194::laca
Name:   e6858.dsce9.akamaiedge.net
Address: 2600:1408:20:183::laca

eagr@eadebian:~$ nslookup apple.com
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
Name:   apple.com
Address: 17.178.96.59
Name:   apple.com
Address: 17.142.160.59
Name:   apple.com
Address: 17.172.224.47
```

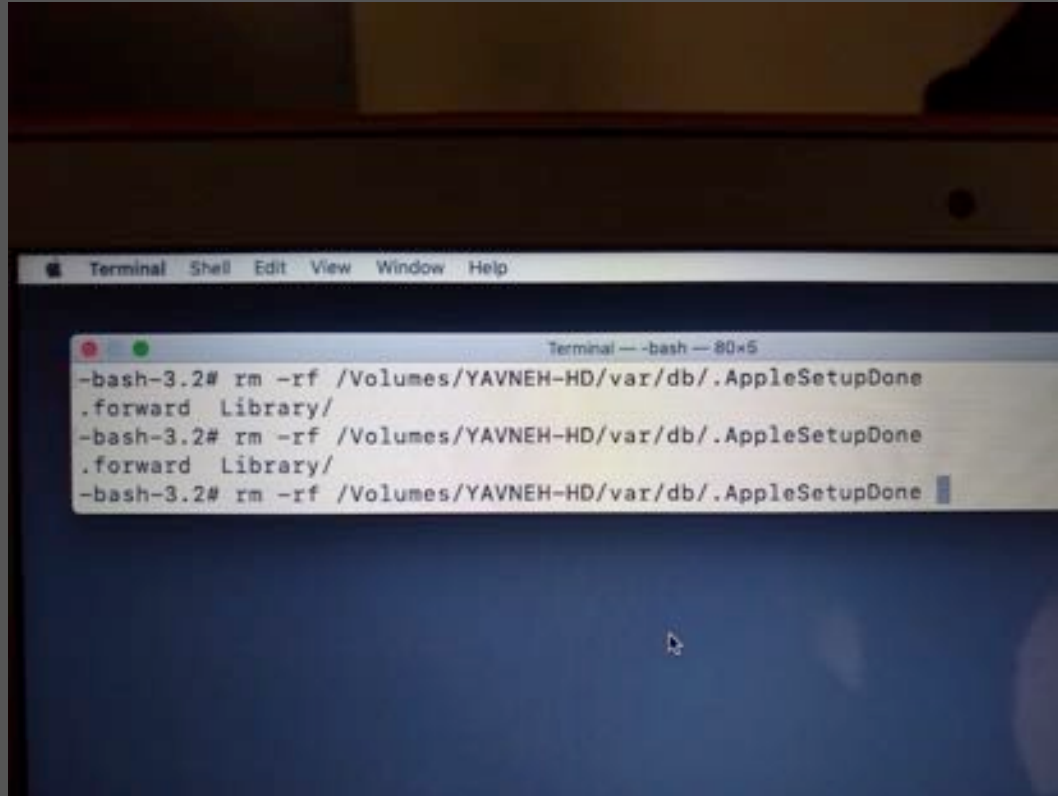

Safe Computing: the OS (mac)

- If you don't password-protect the bootloader and the volume with encryption...



Safe Computing: the OS (mac)

- If you don't password-protect the bootloader and the volume with encryption...



Safe Computing: the OS (mac)

- If you don't password-protect the bootloader and the volume with encryption...



Safe Computing: the OS (mac)

- If you don't password-protect the bootloader and the volume with encryption...



Create a Computer Account

Fill out the following information to create your computer account.

Full name:

Account name:

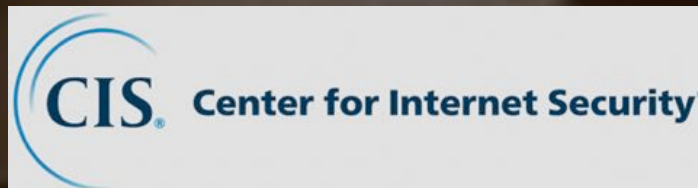
This will be the name of your home folder.

Password:

Hint:

Safe Computing: the OS + Network + Apps

- Prepare the OS before letting anyone touch it, configure the system using best practices: (depends on the use case {government, banking, grandma})
 - Read Technical Implementation guides from NIST, CIS, etc
 - STIG (Security Technical Implementation Guides) Viewer
 - CIS (Center for Internet Security) Benchmarks



Safe Computing: the OS + Network + Apps

- Demo { shodan & montclair “authorization required” website }



Safe Computing: the OS + Network + Apps

```
if [ -f ~/docs.google.com/eapresentation == done ]  
then  
  echo "The End"  
  break  
else  
  continue  
fi
```

Q & A time..