

(ISC)<sup>2</sup>  
**Safe and Secure Online**<sup>®</sup>  
by the Center for Cyber Safety and Education

SENIORS  
EDITION



CENTER FOR  
**CYBER SAFETY  
AND EDUCATION**



This presentation has been created by the Center for Cyber Safety and Education with the help of the world's leading cybersecurity professionals: the certified global members of (ISC)<sup>2</sup>.

# Expectations



# Awareness

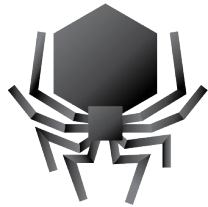
# About You

Do you mostly ...

- Connect with other people?
- Bank and shop?
- Watch movies and play games?
- What else do you do?

# UNDERSTANDING THE CYBERWORLD

Knowing basic terminology will help you navigate the internet safely



MALWARE



PHISHING



CLOUD



WIFI



APP

# MALWARE PROTECTION



Get anti-virus and keep it updated!

# SECURITY UPDATES

- Operating System
- Internet Browser
- Software
- Anti-virus



# SAFE PASSWORDS

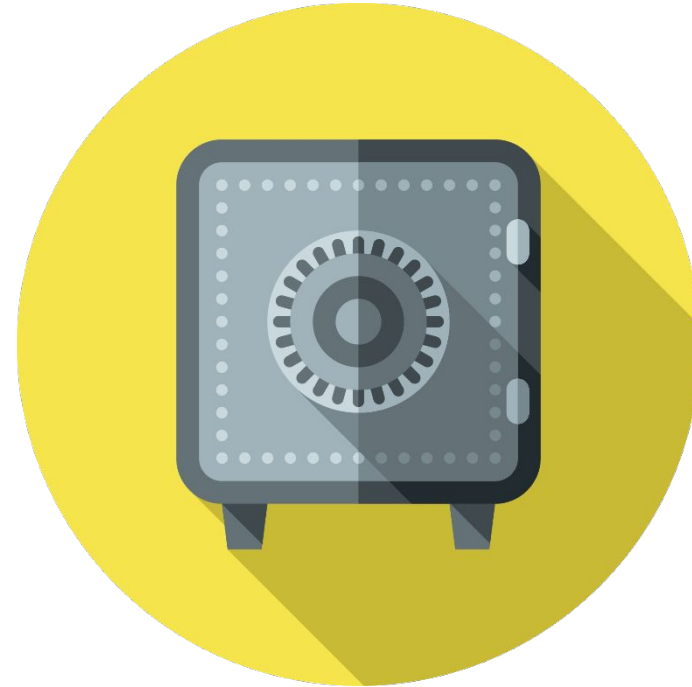


- Make it a phrase- the longer the better!
- 8 character minimum with no repetitive or sequential characters.
- No commonly used passwords and no context-specific words.
- Use 2-Factor whenever offered.
- Make sure passwords are used on all mobile devices and computers.



# PASSWORD VAULTS

- Store all passwords in a secure location
- Don't have to remember passwords



# OPEN WIFI



- Connect with caution
- Do not auto-connect
- Avoid banking
- Avoid checking e-mail
- Avoid making purchases

# ONLINE SHOPPING AND BANKING

<https://www.yourbank.com/>



- Be sure you are on a real, secure site before entering personal information, including credit card numbers.
- Never bank or shop on open Wi-Fi
- Banks will not ask for your credit card or password information via e-mail.
- Ensure you use strong, unique passwords for financial and shopping sites.

# SCAMS

- Fake Emergencies
- False Promises
- Fabricated Prizes
- Bogus Investments
- Deceptive Money Offers
- Phony Lotteries



# COMPUTER COLD CALLING SCAM

Someone calls and asks to take control of your device to help you.



- “Your computer has a virus. I’m calling to help. Please go to our website and download the tool so I can fix it for you.”

# RANSOMWARE SCAM

A scare tactic that takes control of your device or files; designed to scare you into sending money to get your access back.



## **WARNING**

**Your personal files are encrypted. In order to obtain the private key to restore access, you need to pay \$300.**

**Private Key will be destroyed.**

**Time Left**

**01: 05: 02**

**NEXT**

# ADVANCED FEE SCAM

Convinces you that in return for sending money in order to help someone, you will receive even more money eventually



**“I am a prince and my father left me \$40 million in his will, but I have to first bribe government officials to get it out.”**

# STRANDED TRAVELLER SCAM

Appears to be coming from a family member or a friend, but really is coming from a criminal trying to convince you to send money.

**“Please help me! My wallet and has been stolen and if I don’t pay the hotel right now, they will arrest me!”**





# SCAM VICTIM PLAN OF ACTION

1. Collect your thoughts and remain calm.
2. Change your passwords.
3. Make a list of all information that was stolen.
4. Track all communications.
5. Obtain a copy of your credit report and review it.
6. Notify credit card companies and financial institutions.
7. Contact your local law enforcement.

# SAFE EMAIL HABITS



- Never follow links or instructions from unknown or untrusted sources
- Never send sensitive information through e-mail
- Log out when you are finished


# PHISHING

A malicious attempt to acquire sensitive information by pretending to be a trustworthy source and using fake bait to catch victims.




# PHISHING EXAMPLE

Reply Reply All Forward IM

 Best Bank ■ customer5319  
Customer Help- Password

Retention Policy Default (no policy selected) – 4 years. (4 years) Expires 4/6/2020

 New Password.docx  
15 KB

Hello

The password of your account will be changed on February 1. Hurry.

A new password is attached to this letter. Open it now to view.

You may also change your password by clicking here: [www.YourBank.com](http://www.YourBank.com).

If you don't change your password, we will block your account!

Thank you,

Your Bank

<http://NotYourBank.com>  
Ctrl+Click to follow link

# QUESTION WHAT YOU SEE

The screenshot displays a Mac OS X desktop environment. On the left, a sidebar shows system tasks and navigation options. The main window is a web browser displaying a table of detected threats. An 'Apple security alert' dialog box is overlaid on the browser, warning of detected Trojans. Below the alert, the 'Apple security center' interface shows a total of 56 viruses found, with 14 critical threads affected.

Name	Size	Kind	Result
sys_nesb.cpx	38.21 MB	File	Trojan.MacOS.Nvp
drvp.py	6.95 MB	Python script	Worm.iPhoneOS.Ikee.b
winri.xml	6.61 KB	File	Application.OSX.SpyMe
msoqhnux.js	93.77 MB	javaS...script	Trojan.OSX.RSPlug.M
mso\$zxm.bin	84.71 KB	Data file	Virus.MacOS.Init17
batn.dlc	98.16 MB	File	Trojan.OSX.RSPlug.F
appzwo_h	25.61 MB	File	Trojan.OSX.RSPlug.K
sysu.vbs	44.53 MB	Vis...script	Port-Flooder.OSX.Tsunami

**Apple security alert**

To help protect your computer, Apple Web Security have detected Trojans and ready to remove them.

Cancel Remove all

Spyware is a type of malware that can be installed on computers, and which collects small pieces of information about users without their knowledge.

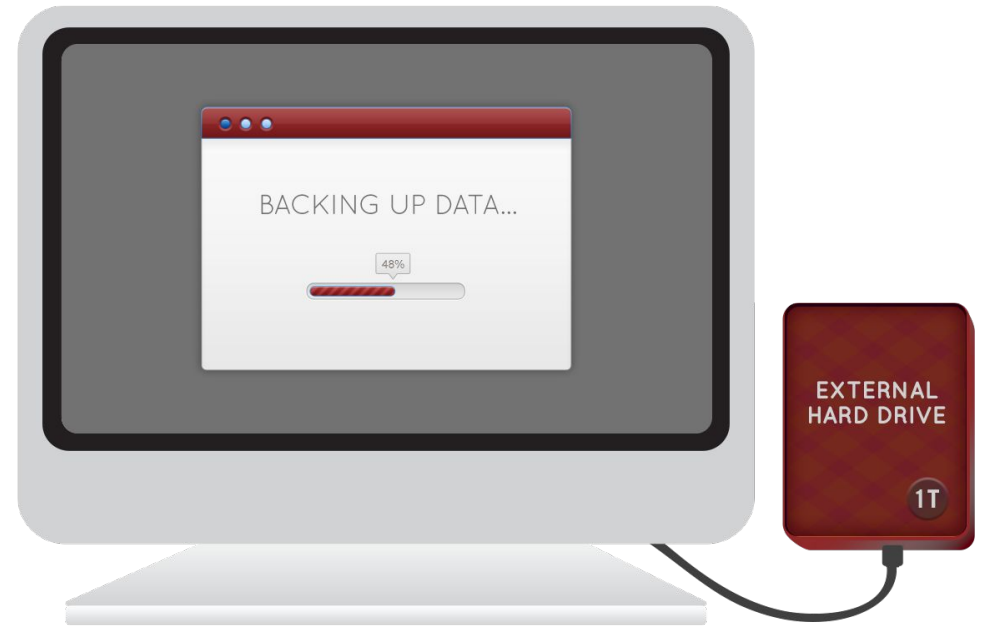
**Apple security center**

Total: 56 viruses found  
Critical: 14 threads affected by virus  
Security: affected by virus

# BACK UP YOUR DATA

This is extremely important—but, easy to do.

- Use an external portable storage device or cloud services
- Backup your data daily or weekly



# DOWNLOADS AND STREAMING

Use reputable sites only:

- Download music
- Watch movies
- Download apps
- Stream television
- Play games



# SOCIAL MEDIA



- Get permission before posting pictures of others
- Do not put sensitive information on social media
- Do not post that you are going out of town
- **What goes on the internet, stays on the internet**



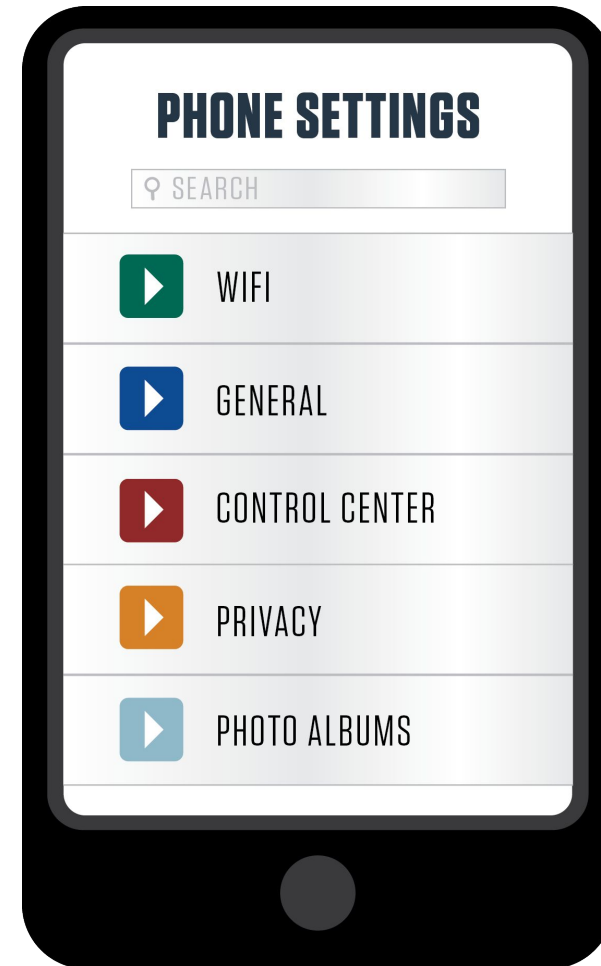
# PICTURES

- Stop and Think before posting pictures - Does this reveal personal information?
- Do not post pictures while still on vacation
- Look in the background of photos too
- Deactivate geotagging from your photos



# DEACTIVATE GEOTAGGING

- Only deactivate geolocation from pictures
- Leave other geolocation apps and services in place
- Check with your cellphone provider for instructions on how you can change the setting on your specific device



# RECAP: TOP TIPS

1. Think before you click.
2. Get anti-virus protection and keep it updated.
3. Keep your computer software and device apps updated.
4. Back-up your pictures and documents.
5. Create strong, unique passwords for every site.
6. Be careful on public Wi-Fi connections.
7. Question what you see in e-mails and pop-ups.
8. Download and stream from proper sites only.
9. Do not post sensitive information on social media sites.
10. Be mindful of e-mail and phone call fraud attempts.

# www.IAmCyberSafe.org



@IAmCyberSafe



@IAmCyberSafe



@Center for Cyber Safety and Education



@ISC2Cares

© 2018 Center for Cyber Safety and Education, a 501(c)(3) segregated fund of (ISC)<sup>2</sup>, Inc. Permission granted to reproduce for personal and educational use only. Commercial copying, hiring, lending is prohibited.