SAFE AND SECURE ONLINE

PRESENCE AND BROWSING

SEWANTE LEONARD

Today's focus is on a couple of key areas including safe online interactions and device safety.

- Many of us have probably experienced something negative in our time using the internet and
- the rest of us have certainly heard about some scary things in the news when it comes to the online world.
- This has led to the unfortunate expectations of the internet being a hard place to navigate with hidden dangers around every corner.

Awareness

- The goal of this presentation is not to scare you away from the internet,
- But to reflect on safe use of internet Unfortunately,
- There are a lot of bad people out there using the internet to prey on people.
- Like most things in life, the internet is going to be a lot less scary and dangerous with awareness and training.

About You

What Do you mostly use internet for...

Connect with other people?

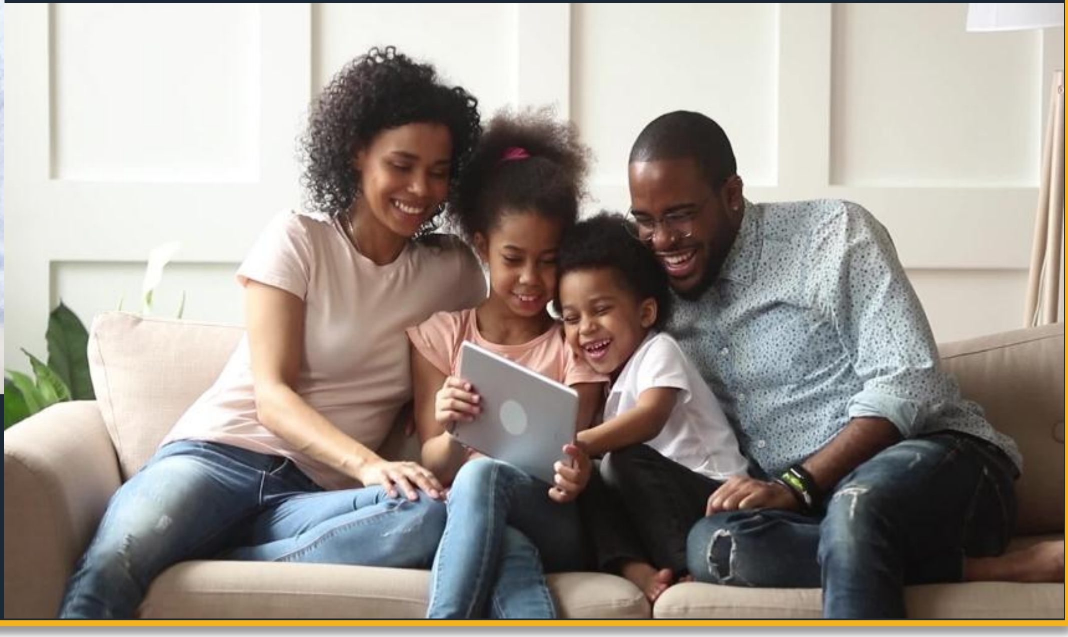
Research?

Bank and shop

What else do you do?

UNDERSTANDING THE CYBERWORLD

‘Digital Immigrants’ vs ‘Digital Natives’



START WITH THE BASICS

Knowing basic terminology will help you navigate the internet safely

MALWARE

PHISHING

CLOUD

WIFI

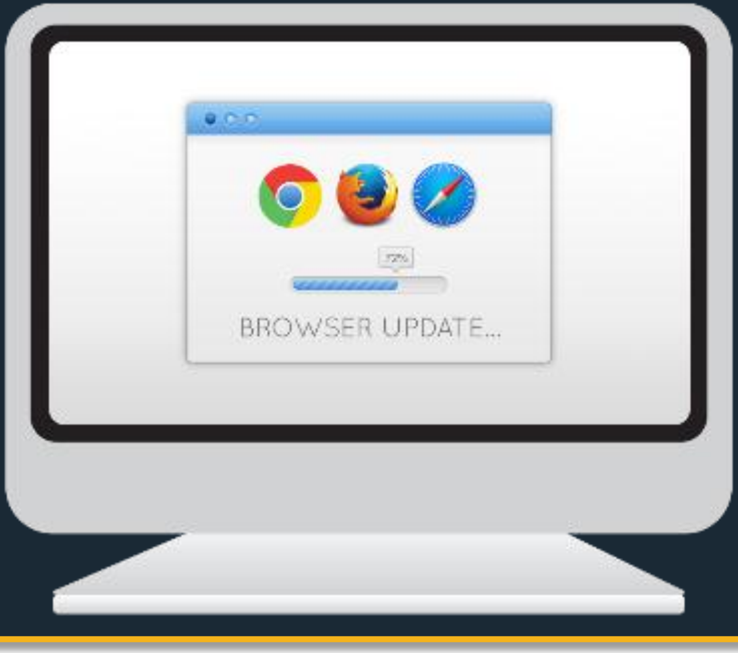
APP

MALWARE PROTECTION

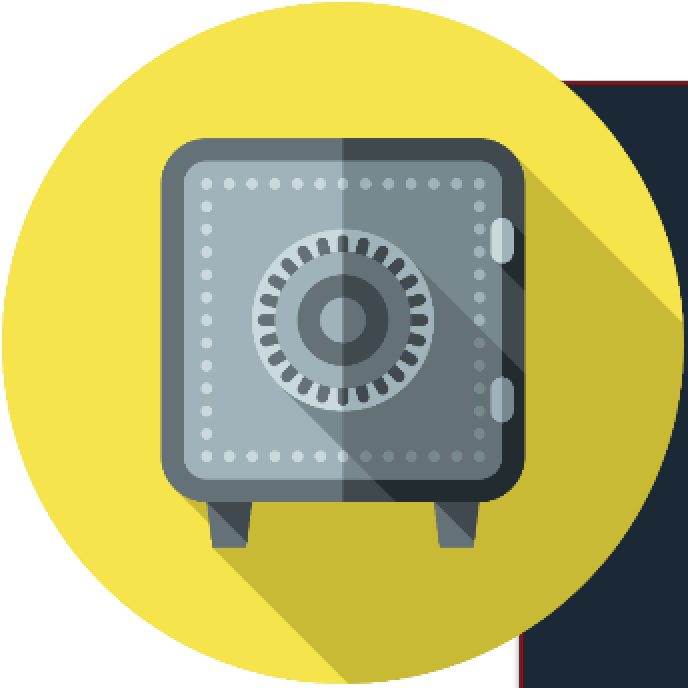
Use of anti-virus and keeping it updated

SECURITY UPDATES

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



SAFE PASSWORDS



Create Strong Passwords

Combine lower case, upper case, numbers, and special characters

Try a 'Passphrase'

Longer and stronger than a password

CREATING A PASSPHRASE

safe and secure

I am safe and secure online

IamSafeandSecureOnline

IamS@f3@nd$ecur3Online!

PASSWORDS EVERYWHERE.

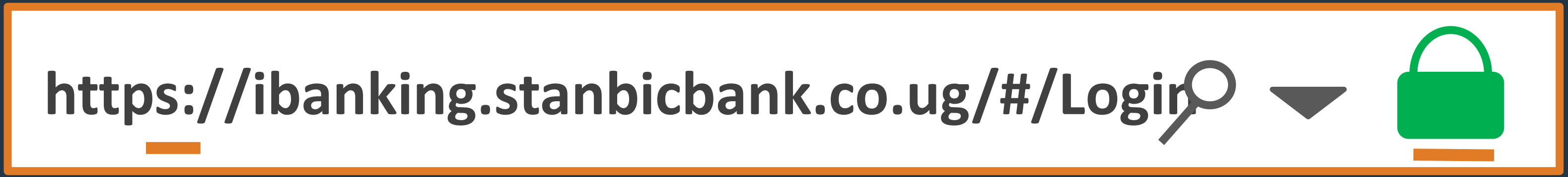
P@$$WORD T!P:

Use passwords or PINs on lock screens for all mobile devices and computers

Wi-Fi Hotspots

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

ONLINE SHOPPING AND BANKING



https://ibanking.stanbicbank.co.ug/#/Login

- Be sure you are on a genuine, secure site before entering personal information, including credit card numbers.
- Never bank or shop on Wi-Fi hotspots.
- Banks will not ask for your credit card or password information via email or phone call.
- 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

And more….

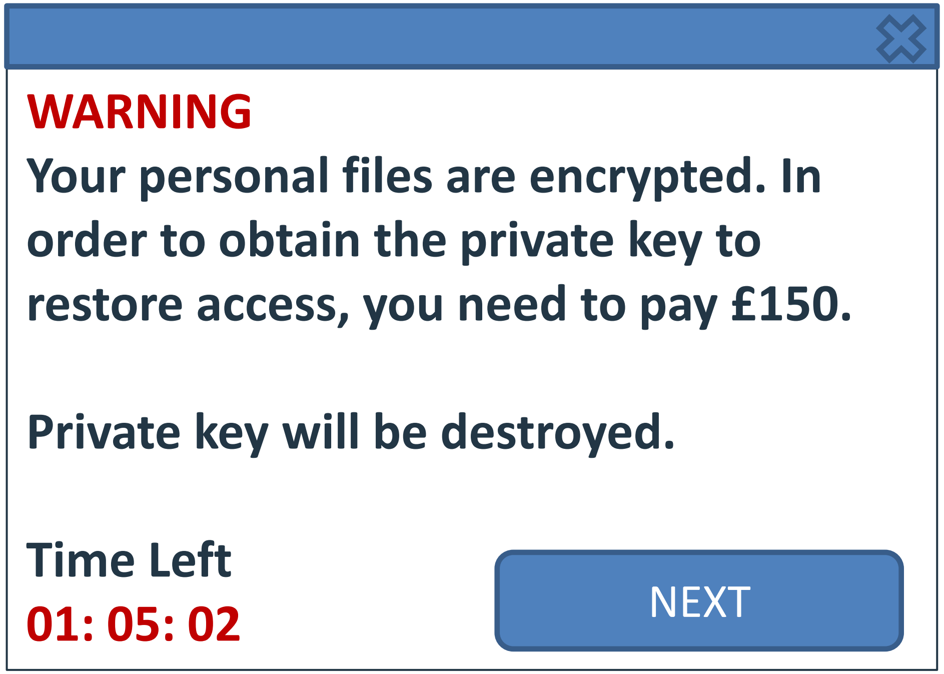
COMPUTER COLD CALLING SCAM

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 ransom 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 £150.

Private key will be destroyed.

Time Left

01: 05: 02

SCAM VICTIM ACTION PLAN

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 Action Fraud.

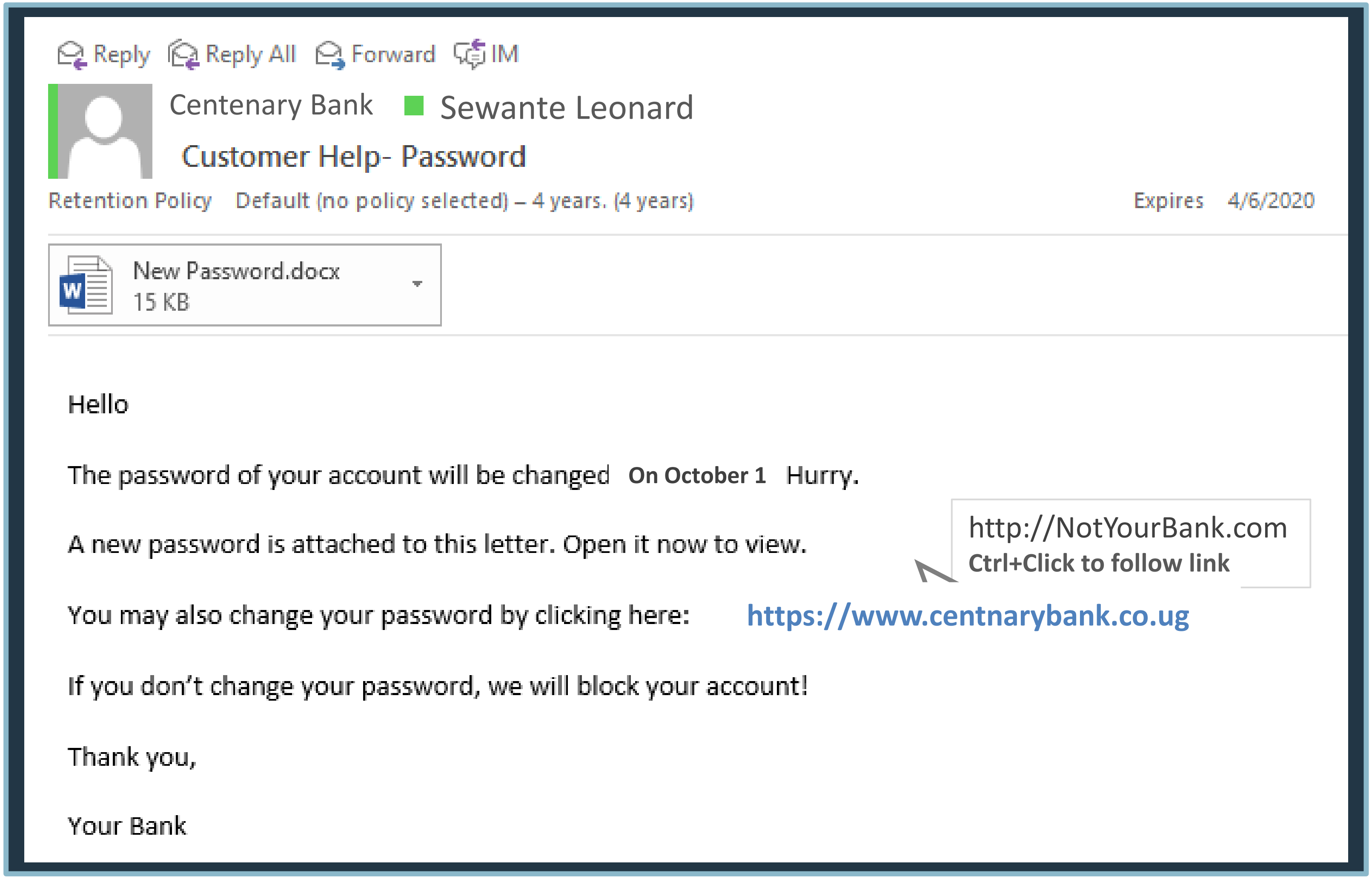
SAFE EMAIL HABITS

- Never follow links or instructions from unknown or untrusted sources
- Never send sensitive information through email
- 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 lure in victims.

PHISHING EXAMPLE



Centenary Bank 🟩 Sewante Leonard

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 October 1** Hurry.

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

You may also change your password by clicking here: **https://www.centnarybank.co.ug**

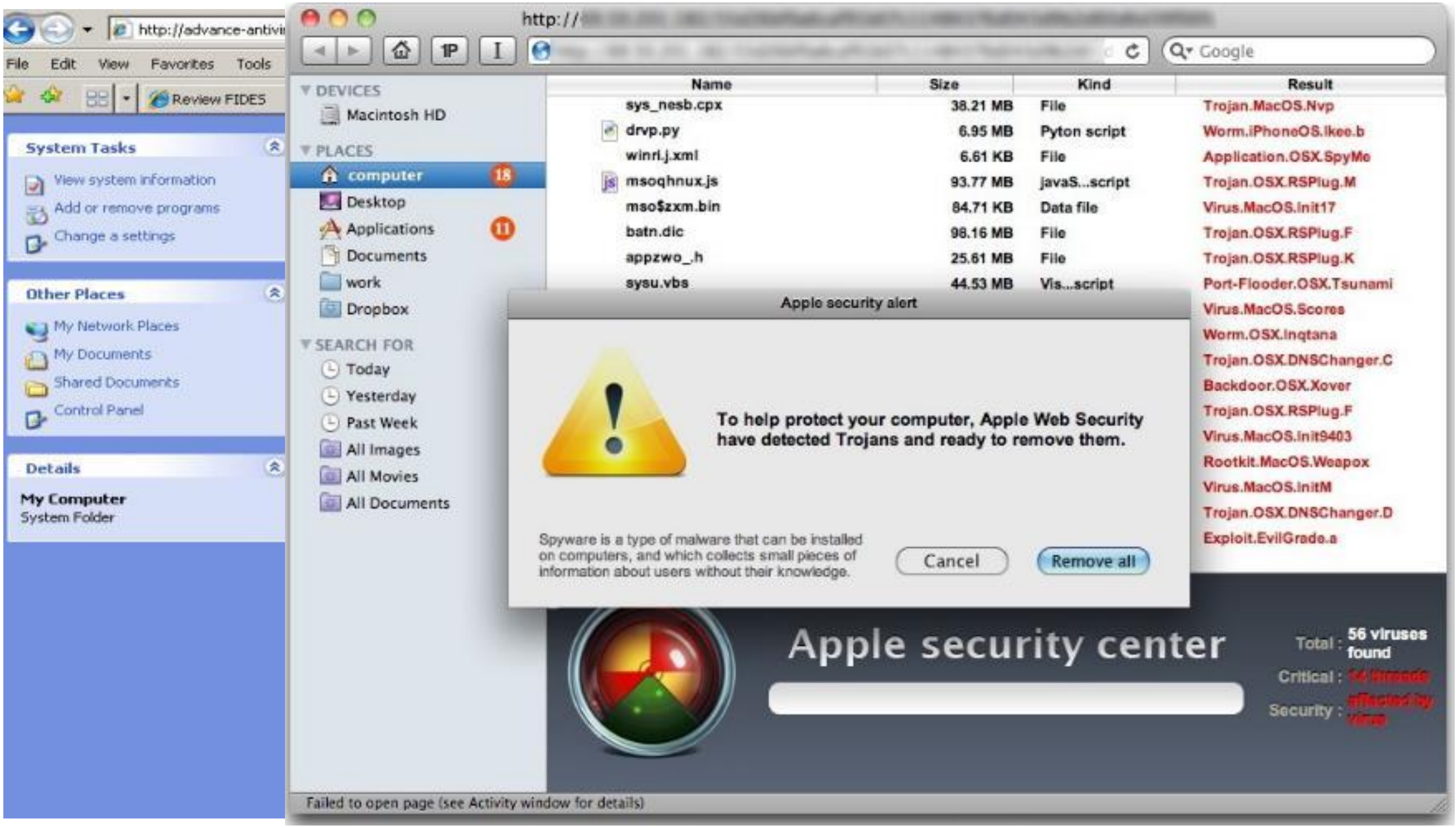
http://NotYourBank.com
Ctrl+Click to follow link

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

Thank you,

Your Bank

QUESTION WHAT YOU SEE



Name	Size	Kind	Result
sys_nesb.cpx	38.21 MB	File	Trojan.MacOS.Nvp
drvp.py	6.95 MB	Pyton script	Worm.iPhoneOS.Ikee.b
winrl.j.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.dic	96.16 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
			Virus.MacOS.Scores
			Worm.OSX.Inqtana
			Trojan.OSX.DNSChanger.C
			Backdoor.OSX.Xover
			Trojan.OSX.RSPlug.F
			Virus.MacOS.Init9403
			Rootkit.MacOS.Weapox
			Virus.MacOS.InitM
			Trojan.OSX.DNSChanger.D
			Exploit.EvilGrade.a

Apple security alert

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

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 threats

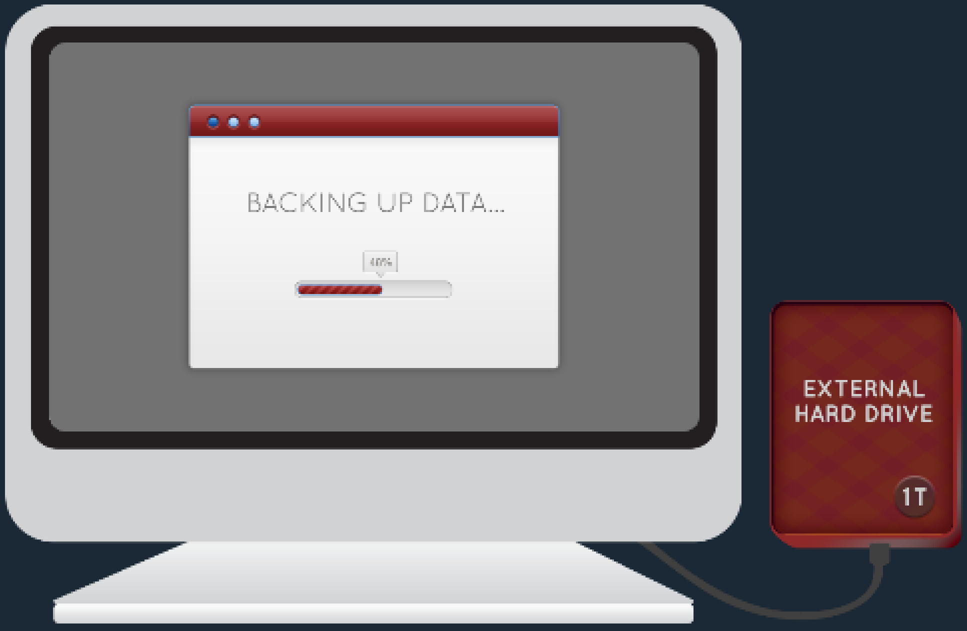
Security : affected by virus

Failed to open page (see Activity window for details)

BACK UP YOUR DATA!

This is extremely important—but easy to do.

- Use an external portable storage device or cloud services
- Back up your data daily, weekly or in real time



DOWNLOADS AND STREAMING

Use Reputable Sites Only!

- Download Documents
- Download apps
- Download music
- Watch films
- Stream TV

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
- Do not click on random links in posts or tweets
- **What goes on the internet, stays on the internet**

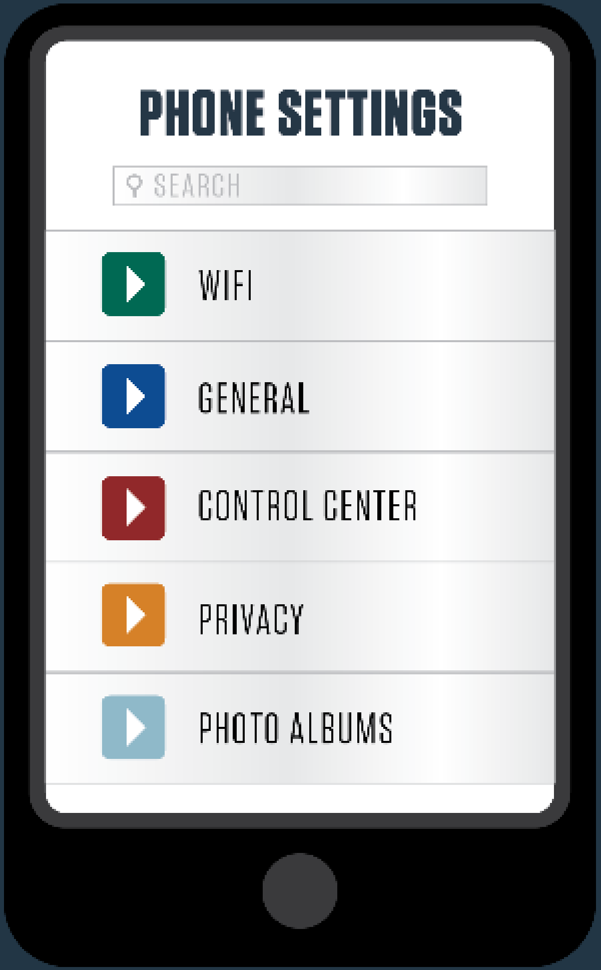
PICTURES

- Stop and think before posting pictures - Does this reveal your or others' personal information?
- Do not post pictures while still on holiday
- 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



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 docs, pics and other important files
5. Create strong, unique passwords for every site.
6. Be careful on public Wi-Fi connections.
7. Question what you see in emails and pop-ups.
8. Download and stream only from proper sites.
9. Do not post sensitive information on social media sites.
10. Be mindful of email, phone call, text and social media fraud attempts.

QUESTIONS?

Comments