SECURITY

Training

DES LATHAM

OUTLINE

1. Digital
2. Personal

DIGITAL

1. Protecting Files
2. Protecting People
3. Methods

Manage The Risk Plan

PROTECTING FILES

1. Two-Factor Encryption
2. Email
3. PWD protect relevant Files
4. Hiding Files
5. Partition Drives
6. Non-connected Devices
7. External Drive Health Tips
8. Create False Trails

1. TWO FACTOR ENCRYPTION

Turn it on for all important Apps and Platforms

X
FB
Linkedin
Gmail/Youtube
Paypal
TikTok
Others?

WhatsApp....
Signal

2. EMAIL

75% of all cyberattacks start with Email

Phishing Attacks
Ransomware
Man in the Middle Attacks (Cloud)
Malware
Insider Threat
Social Engineering

EMAIL

Protecting yourself

a. Don't click on suspicious links in your email
b. Use Search Engine to check the sender
c. Tone and content
d. Follow pre-existing rules with senders

3. PASSWORDS

Use PWDs to protect files

Use a phrase

Make it oblique - but you need to remember:

IamaZuluWarrior

Add numbers and stuff

14m4ZuluW4rr10r&*(

PWD PROTECT FILES

Mac

Right Click

Get Info

Select “Locked”

To unlock repeat - but remember your computer PWD

PWD PROTECT FILES

PC

-Right-click the file or folder

-Select Properties

-Click Advanced

-Check Encrypt contents to secure data

-Click OK

-Click Apply

4. HIDING FILES

Check shared file later for specifics

Risk is you forget the pwd - and people can access by using commands “Show hidden Files”.

5. PARTITION DRIVE

https://www.easeus.com/partition-manager/epm-free.html

Slicing the Drive - allows you to create a little nook where you can hide files and add another layer of security

Cons: Professionals will notice

6. NON-CONNECTED DEVICES

Remove the Wifi and Internet chips (any reliable shop can do this)

Ensure clean data in. No-one can hack this computer from a remote point.

Useful to store data, spreadsheets.

Careful with the external drive...

7. EXTERNAL DRIVES

Factory reset/Format

Avoid sharing

Pass through an antivirus like Sophos

https://www.sophos.com/en-us

7. EXTERNAL DRIVES

Factory reset/Format

Avoid sharing

Pass through an antivirus like Sophos

https://www.sophos.com/en-us

8. CREATE FALSE TRAILS

Meetings
Schedules
Names and Places
Burner Devices

Questions

PERSONAL SECURITY

1. Situational Awareness
2. Schedules
3. Protecting Sources
4. Triggering Alarms
5. Hard Copies
6. Work with other Media

1. SITUATIONAL AWARENESS

1. Vary routines and dress code
2. Keep you head up get off your phone
3. Escape Routes and Emergency Procedure
4. Anticipate action

SITUATIONAL AWARENESS

5. Practice Reading people
6. Break the law of LEAST EFFORT
7. PATTERN DETECTION - Body language
8. Surprise is your friend
9. Memorise objects in the vicinity, car registrations/write them down

SITUATIONAL AWARENESS CTND

10. Entering/Exiting vehicles, business & homes
11. Use codes in your own handwriting – varied language
12. Backup – single trusted person – Need to know basis (normally the editor)

THANKYOU

Any Questions?