KEEP YOUR PESKY HANDS OFF MY MOBILE DATA!

TURNING IT ON

Set up a strong password for your device (think combination of capitals, numbers and special characters) and ensure it has an automatic wipe function to kick in as a result of password failure – **this is the first and simplest step to protect your sensitive company data**

CONTROL YOUR CONNECTIVITY

Turn off your Bluetooth and deactivate the automatic connection to Wi-Fi, this setting can automatically be connecting to any/every public network wherever you go - **avoid hooking up to any old network or you risk having to explain to your boss where you have been**

Where are you hooking up?

BE CAREFUL WHAT YOU DO IN PUBLIC

If you want to participate in open networking and hotspots, then ensure you stay safe – always check the network is the genuine version and secure - **NEVER access sensitive company information or online banking on a public network**

HACKERS LURK ON OPEN NETWORKS

YOU CAN TRUST ME!

YOU CAN'T TELL IF AN APP IS INFECTED JUST BY LOOKING

IM A BAD APP

Only download from trusted or approved sources - bad apps can carry malware, viruses, spyware and worms - **never allow apps to 'remember' your passwords**

pick me!

hellooo!

BEWARE: FREE APPS CAN CARRY INFECTION

KEEP IT HEALTHY

Only download company-approved operating system updates to keep your mobile device in full health and on top of the latest security threats – **your IT department is there to make sure all of your security holes are patched**

hey there...

IT ONLY TAKES A FEW SECONDS...

to have your mobile device stolen – **are you prepared to tell your boss you have just lost the latest sensitive company information?** (If you phone is stolen report it to the IT department immediately)

DO IT BY REMOTE CONTROL

If all else fails you can do-it-yourself – take back control by installing a remote-wipe app to ensure your sensitive work data doesn't fall into the wrong hands

I'm wiped out!

YOU ARE IN MY POWER AND WILL DO AS I SAY...

DON'T GET CAUGHT IN COMPROMISING SITUATIONS:

- DOWNLOADING APPS
- PUBLIC WI-FI/HOTSPOTS
- SOCIAL NETWORKS PHISHING
- EMAIL PHISHING
- SMS PHISHING

TAKE CARE:

- ONLINE BANKING
- OPEN NETWORKS

PROTECT:

- WORK AND PERSONAL DATA

JAILBREAK PHONES ARE MORE AT RISK

Jailbreaking is the process of removing the limitations on some mobile devices to allow the use of unauthorized software and apps **but at the same time this opens your device, and the data it contains, to the threat of hackers and infected apps**

i'm out of here

Symantec.