



## 10 Do's and Don'ts For Good Cyber Hygiene

There are a lot of easy ways to improve cyber hygiene within your organization. Many of them involve simply being mindful of how you use your work device on a daily basis.

Here are 10 practices to start with that can have an immediate impact on the security of your organization:

### Do's

### Don'ts

- 

Use the **Provided VPN** (Virtual Private Network) and systems for remote working
- 

**Check** with IT if you need to travel with your work laptop
- 

**Lock** or **Log Off** from your devices when they are not in use
- 

Be **Aware** who can see sensitive information
- 

Connect your **Work Devices** to **Trusted** home networks
- 


**Report** suspected incidents, breaches or disclosures to your IT or IS Manager
- 


**Contact** your security team before sharing sensitive data
- 


Follow your organization's **Cybersecurity** policies and procedures
- 


Only use **Company Approved Software** on company machines
- 


Keep your **Passwords Long** and **Unique** to each system


- 


Use **Work Devices** for personal purposes
- 


Use **Personal Devices** for work purposes
- 


Leave **Confidential Information** unattended
- 


Use **Public WiFi** on your work devices
- 

Use **Unauthorised Devices** to connect to Jumio networks
- 

Use **Personal Cloud Storage** (DropBox, BOX, OneDrive or iCloud)
- 

Share **Cardholder Data** in any form (excluding valid exceptions which have been reported to infosec).
- 

Change or **Jailbreak** work machines
- 

Download **Unapproved Software** to your work devices
- 

Share or **Reuse** your **Passwords**

For more advice or information, feel free to contact us for a friendly chat.