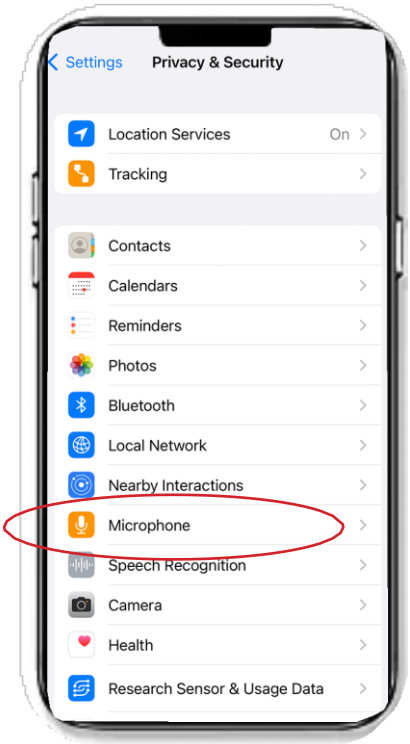
Toro's Guide to Good Cyber Hygiene

1.0 Executive Summary

- **Breached Accounts.** Check out if your email accounts or phone number have appeared in a data breach here.
- **Password Manager.** Apps such as 1Password, Dashline Premium (comes with a VPN), or Bitwarden are a must!
- **Passwords.** Long at strong (17 character+). Or use pass phrase like "h0w-now-Brown-C@w" perhaps use a memorable number: One-Hundred-And-Eighty-180. Or use three random phrase passwords because they are easier to remember and harder to guess, such as "RabbitSpainTrousers".
- **2FA.** Enable Two Factor Authentication (2FA) on your emails, iCloud and online accounts that store your cards (i.e. Amazon, eBay) or sensitive personal information (i.e. Facebook). Google how to turn on 2FA for each of your accounts. Toro recommends that you use an authenticator app such as Microsoft Authenticator, Authy or Google Authenticator over text or call
- **VPN.** You should use a Virtual Private Network (VPN) when connected to any Wi-Fi. It creates an encrypted tunnel from your computer through the internet and prevents your online traffic from being intercepted. NordVPN, ExpressVPN and Private Internet Access are popular. ProtonVPN is free. Consider using 4G for sensitive online activities such as banking.
- **Phishing, Vishing, Smishing.** Understand phishing. Understand Vishing by watching this and this. Understand Smishing
- **Phone Social Engineering.**
  - Were you expecting a call?
  - Are you certain you know the person who called you?
  - What information are they after? Avoid giving personal information.
  - Take their details, hang up, go online to get the real customer services number, wait 15 seconds from hanging up if you are using a landline, call the real customer services, and get put through to that department.
- **Anti-Virus.** Avast, Avira, Sophos Home, Malwarebyes and AVG are free.
- **Improve Office 365 Security.** Log into O365 account as an Admin>review your Secure Score >review improvement actions.
- **Improve Google Workspace Security.** Log into Google Workspace (previously called G-Suite) as an Admin>improve Security.
- **Back Up Laptop & Phone.** Regularly backup your devices to the cloud and to encrypted storage media.
- **Forwarding Rules.** Check whether someone has hacked and created forwarding email rules in Gmail, Outlook, and iCloud.
- **Web Browsers**
  - Consider Duck Duck Go, Chrome 'incognito' Brave or Safari In-Private browsing. Disable WebRTC in your browser
  - Enable Safari's Privacy and Security Settings. Settings>safari>block pop ups / disable auto fill / enable fraud warnings / clear history and website data. More advice is here.
  - Improve security and privacy settings for Google Chrome.
- **HTTPS.** Install a browser plug-in such as "HTTPS Everywhere" or "ForceTLS" to avoid accessing vulnerable HTTP websites
- **Ad Blocker.** Install an ad blocker extension from the App Store or for Chrome or Safari such as uBlock Origin.
- **Suspicious Websites.** Check suspicious website URLs by first pasting them into VirusTotal.

1.0 Executive Summary cont.

- **Electoral Register.** Opt out of the open electoral register here and remove your home address from 192.com here.
- **Social Media Privacy:**
  - **Instagram.** Privacy settings for Instagram.
  - **Facebook.** Privacy settings for Facebook
  - **Snapchat.** Privacy settings for Snapchat, more advice here about two-factor authentication and QuickAdd. Disable Snapchat syncing your phone contacts, Profile>Settings>Contacts>Disable Share Contacts with Snapchat.
  - **Discord.** Privacy settings for Discord.
  - **Recruiters.** Don't friend strangers and don't reveal sensitive info to recruiters.
  - **LinkedIn.** Don't allow LinkedIn connections to see your mobile number or email address. Prevent "People also Viewed". Conduct a 'friend cull' of 1st connections you don't know. Other privacy settings are here.
  - **Twitter.** Settings here. Turn off GPS for Twitter on your phone or every tweet will be stamped with your location.
  - **TikTok.** Privacy settings for TikTok. Here is what you can do if your account has been hacked here.
  - **Surveys.** Beware of online surveys - you might continue to get sent them with increasingly sensitive questions.
  - **Children.** Other advice for parents.
- **WhatsApp.** Settings>account>Two-Step Verification>turn on. Settings>account>privacy>decide whether you are happy with strangers seeing when you were last online, 'About' information, or seeing your profile picture. In Privacy, check whether live location is shared. Settings>WhatsApp Web/Desktop and see if your account is being accessed from a computer.
- **Slack.** Ensure that your company or business uses two-factor authentication and admin controls to review and accept invitations, so only the right people have access to information. More advice about privacy settings for Slack.
- **Home Wi-Fi Router.** Update Wi-FI router firmware. Reset default administrator and Wi-Fi passwords via Router admin console.
- **UK Credit Rating.** Register with a credit rating alert service. This will provide warning if an attacker has stolen your identity and loans applied for. Credit Karma is free. Consider signing up for CIFAS' Protective Registration service.
- **Scan your Domain.** There are several free tools where you can scan your domain / website for vulnerabilities. These are MX Toolbox, Wormly and Securi.
- **Privacy Settings.** Turn off apps that don't need access to your microphone, location, camera, contacts etc. Disable any unwanted voice activated apps such as Cortana (Windows) or Siri (Mac / iPhone).
- **Memorable Info.** Make sure attackers can't glean memorable information (e.g. pet's names, mother's maiden name, birthday, school etc.) from your social media posts. Ensure that geotags are turned off for posts on social media sites such as Instagram and Facebook because geotags can be included automatically.
- **Webcam.** Cover with a sticker when webcam is not being used.



1.0 Executive Summary cont.

- **Privacy Screen.** Use a detachable Privacy Screen to prevent strangers from 'shoulder surfing'.
- **USB Sticks.** Don't plug unknown USB devices into your computer. Always virus scan USB sticks before running them on your computer. Encrypt USB sticks before storing data on them.
- **Screen Lock.** Set the computer screen to lock after a few minutes.
- **Bluetooth & Wi-Fi.** Turn off your Bluetooth and Wi-Fi when it is not being used. It will save your battery and protect privacy.
- **Email Aliases.** Sign up to online services using email alias. Use + create an Gmail alias. Add email address to Outlook account.

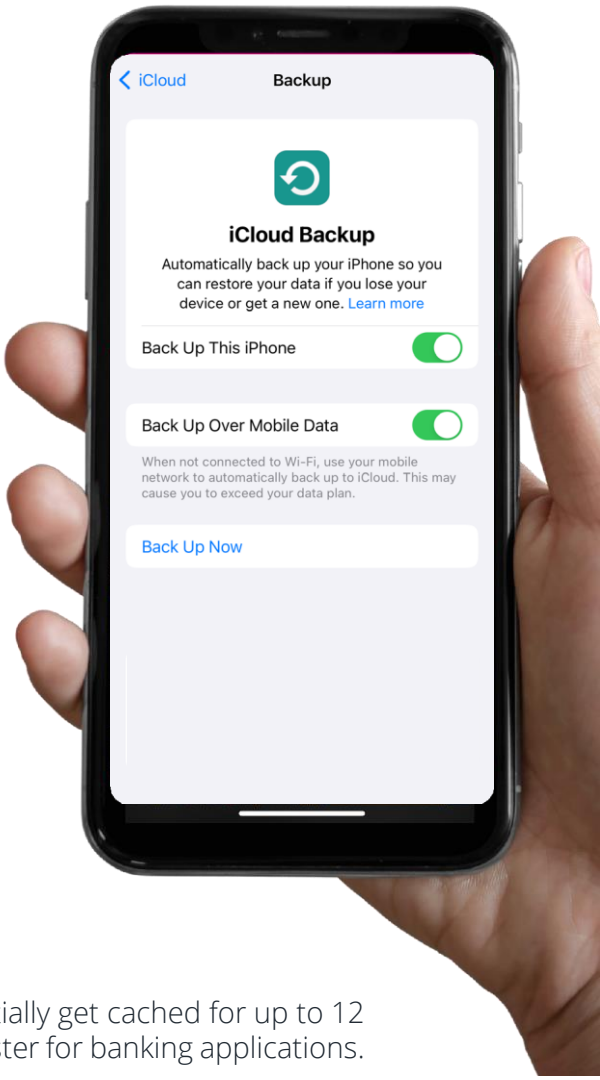
- **Browser Data Leakage.** Check what data your browser and VPN is leaking by using a testing service.
- **DNS.** Consider using a different DNS provider such as CloudFlare or Quad9. CloudFlare also offer an application to secure your DNS requests via profiles (iOS, Android)
- **Public Wi-Fi and Hotspots.** Utilise tethering and VPN's when using public Wi-Fi to ensure that your movements cannot be tracked, and your personal information cannot be intercepted. Always use secure hotspots with a password. More information about tethering can be found here
- **Secure Messaging / Calling Apps.**

	SKYPE	TELEGRAM	IMESSAGE	ELEMENT	VIBR	MESSENGER	WHATSAPP	MESSAGES	WICKR	THREEMA	WIRE	SIGNAL	SESSION	SIMPLEX
JURISDICTION	USA	USA	USA	UK	USA	USA	USA	USA	USA	SWITZ	USA/SWITZ	USA	AUSTR	UK
MANUALLY VERIFY CONTACTS' FINGERPRINTS														
ENFORCES PERFECT FORWARD SECRECY														
COMPANY PROVIDES TRANSPARENCY REPORT														
COMPANY CAN READ MESAGES														
ENCRYPTED BY DEFAULT														
SURVEILLANCE BUILT INTO APP														
DISAPPEARING MESSAGES														
PROVIDED DATA TO INTELLIGENCE AGENCIES?														
PERSONAL INFORMATION HASHED														
DATA ENCRYPTED ON DEVICE														
AUDIT AND SECURITY ANALYSIS CONDUCTED														
BACKED UP MESSAGES ARE ENCRYPTED / NOT BACKED UP														
SECURES MESSAGE ATTACHMENTS?														
APP AND SERVER OPEN SOURCE?														
ENCRYPTS METADATA														
HARVESTS DATA														
DATA SENT TO PARENT COMPANY / THIRD PARTIES														
ANONYMOUS SIGN-UP														
COMPANY LOGS TIMESTAMPS / IP ADDRESSES														

- **Voicemail Pin.** Call your phone voicemail and set a pin.
- **Sim Pin.** Settings>Mobile Data>SIM PIN>turn on>set a 4-digit PIN you can remember.
- **Register your Devices.** Register your devices on immobilise.com and MissingX. Police use the database to reunite lost and stolen items with their owners.
- IMEI Code. Write down your International Mobile Equipment Identity code and store it somewhere safe so that you can provide it to your insurance company if the phone is stolen or lost: Dial *#06# to get the code.

2.0 Device Specific Advice

2.1 iPhone



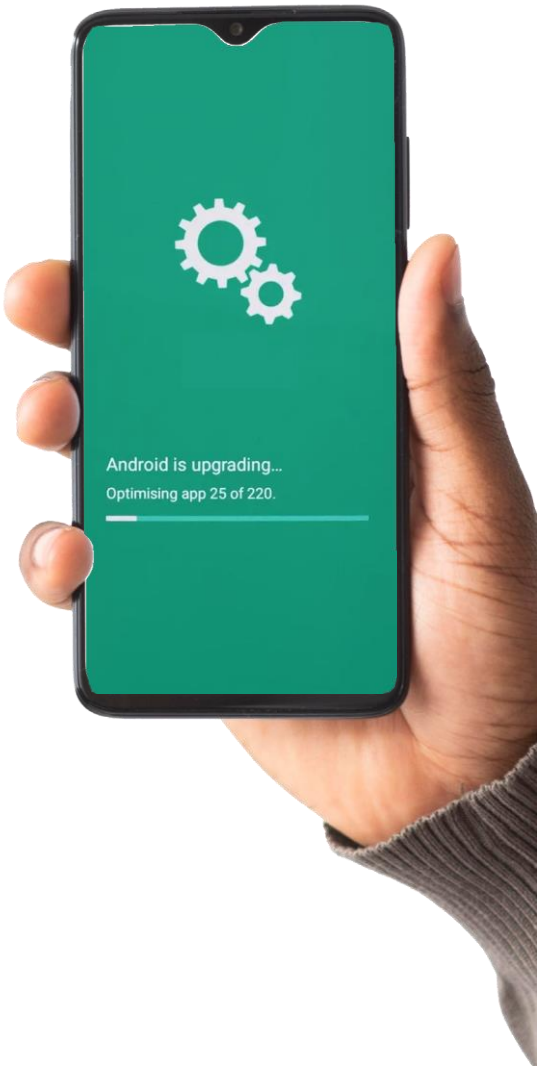
- **iVerify.** Download iVerify from the App Store. It detects if your iPhone has been Jailbroken (hacked). It offers top tips on better protecting your iPhone or iPad. It (version 20.0 onwards) also detects indications of the NSO Group's Pegasus software.
- **Auto Updates.** Ensure the latest iOS is installed as newer iOS updates will patch any vulnerabilities. Go to Settings>General>Software Updates>ensure Automatic updates are On.
- **Pin Code.** Use a minimum of 6 digits for your pin code. Fingerprint or face ID makes using the device easier and can be used to control access to specific apps such as Outlook and banking.
- **iCloud 2FA**. Settings>click name at top>Password &Security>Two-Factor Authentication>Turn on.
- **Backup.** Backup your iPhone to the iCloud or a computer. Here is how. If you use iTunes for backups on your laptop, then click the box to encrypt all backups.
- **Apps.** Use official app stores when buying or downloading apps. Also pay attention to reviews.
- **Updates.** Keep apps and the operating system regularly updated as these may contain security improvements. Turn on auto update: settings>click name at top>iTunes & app stores>set 'apps; and 'app updates' to automatic downloads.
- **Find My iPhone.** Turn this on as it helps you locate, lock, or erase your phone/iPad or Laptop if you lose it.
- **Locked Phone.** Turn off features that can be accessed when your iPhone is locked: settings>touch ID and passcode>voice dial / today / notifications view / reply with message / wallet / Siri.
- **Reset Keyboard.** All keystrokes entered on an iPhone could potentially get cached for up to 12 months, including account numbers entered on your iPhone to register for banking applications. Settings>general>reset>reset keyboard dictionary.
- **Privacy Settings.** Settings>privacy>location services>
  - >share my location - set to off
  - Go through each app and determine whether you need GPS on 'while using' or 'never'. Make sure nothing is on 'always'
  - Make sure 'never' is selected for: camera (or all your pictures are stamped with where they were taken); all social media apps (i.e. twitter, Facebook, Instagram)
  - >system services - all on except 'Wi-Fi Calling'
  - >frequent locations - 'clear history' and turn to 'off'. Product improvement - all off.
- **Significant Locations.** Stop your movements being tracked and recorded.
- **Notifications.** Settings>Notifications>check each app to ensure notifications can't be accessed in locked screen.
- **Beaconing.** Turn off the Wi-Fi. Turn off Bluetooth when not in use.
- **Private Address.** Settings>Wi-Fi>click the information associated with the Wi-Fi network and turn on Private Address.
- **Siri.** If you don't use it then turn off: settings>Siri & Search>turn all off.
- **Advertising & Diagnostic Data.** Settings>privacy>
  - >Tracking>Allow Apps to Request to Track> Turn to off
  - >Apple Advertising>Personalised Ads turn off
  - >App Privacy Report>Turn on and check
  - >Analytics & Improvements > turn Share Analytics to off
- Stolen Device Protection. Activate this feature to prevent attempts from unknown locations to change your account details: Face ID & Passcode>Stolen Device Protection.

2.0 Device Specific Advice

- Secure your Sensitive Apps. Hold down your finger on the app and select “Require FaceID” and, for extra security, hide the app so it is only available by swiping to the last home screen.
- “Stolen” Focus. Set up a “Stolen” focus mode that you can activate from another iOS device in the event your device is stolen, before you reset it via iCloud. Set the phone to lock the screen, take 3 photos with the front camera, 3 with the back camera, set the brightness to 0, and turn on low battery mode.

2.0 Device Specific Advice cont.

2.2 Android



- **Update.** Settings>Software Update>Auto Download over Wi-Fi.
- **Backup.** Backup your Android. Here is how.
- **Encrypt SD Card.** Settings>Biometrics and Security>encrypt or decrypt SD Card.
- **Strong Data Protection.** Settings>Biometrics and Security>Other Security Settings>Strong Protection,
- **Opt out of Ads.** Settings>privacy>ads.
- **Apps.** Use official app stores when buying or downloading apps. Also pay attention to reviews.
- **Camera and Microphone.** Pay attention to which apps use the camera and/or microphone. You can use the Quick Settings Menu to disable the camera and microphone.
- **Message Encryption.** Confirm that your dark-blue RCS messages have end-to-end encryption enabled. Messages>Settings>Chat Features
- **Disable Sensitive Notification from appearing on the lock-screen.** Settings>Privacy>Notifications on the lock screen>Show sensitive content only when unlocked.
- **Location Tracking.** Settings>Location>App permissions.
- **Beaconing.** Turn off Wi-Fi, turn off Bluetooth when not in use.
- **Find My Mobile.** Settings>Biometrics and Security>Find my Mobile. More information is here.
- **Disable Debugging.** Settings menu>Developer Options>Turn off the USB Debugging option>wait a few minutes for changes to be registered on your device.
- **Mac Address Randomise.** Settings>Wi-Fi>Advanced>Mac Address Type>Randomised Mac.
- **Theft Detection Lock.** Activate this feature to automatically lock the phone if it detects that someone has taken it from you or if it goes offline. You can also set up the ability to remotely lock it with just a phone number.
- **Private Space.** Setup a Private Space or use the App-Lock feature to keep sensitive applications secure.

2.3 Mac

- **Anti-Virus.** Avast, Avira, Sophos Home, Malwarebytes and AVG are free.
- **FileVault & Firewall.** Both are installed but turned off by default (system preferences>Security & Privacy>Firewall On>FireVault). FileVault>create recovery key>save in Password Manager or print and hide.
- **Encrypted Partition.** Put sensitive documents in a encrypted container on your computer.
- **Firmware.** Set a firmware password to prevent a cold boot attack.
- **File Encryption.** Encrypto is a free encryption tool.
- **Admin Account.** Avoid working from an Admin account. You should be using a Standard User account

2.0 Device Specific Advice cont.

to avoid a hacker getting admin access. Here is how to set up a guest account.

- **Forget Known Wi-Fi Networks.** Before traveling, especially if they are identifiable as a company or home.
- **Find My Mac.** Check it's turned on. System Preferences>Internet Accounts>iCloud>Find My Mac>Turn on

2.0 Device Specific Advice cont.

2.4 Windows

- **Whole Disk Encryption.** Windows Pro and Enterprise come with BitLocker installed. Windows Home does have some encryption, but it needs to be enabled. VeraCrypt (replaced TrueCrypt) is free. Here is how to use VeraCrypt.
- **Install Patch My PC.** Update vulnerable software on your Windows machine.
- **Autorun.** Disable autorun to prevent infected USB device attacks.
- **Anti-Virus.** Windows computers already have Windows Defender installed, just make sure it's turned on.
- **Privacy Settings.** Apply privacy settings for Windows 10.
- **File Encryption.** Free file encryption tools include Encrypto, AES Crypt and VeraCrypt (see above).
- **Erasing Files.** Just deleting a file could still leave the file on the computer, write over it using Eraser.
- **Bios Password.** Set up a Bios password.
- **Admin Account.** Avoid working from an Admin account; you should be using a Standard User account to avoid a hacker getting admin access. Here is how.
- **Mac Address Randomise.** Windows Settings > Wi-Fi > Random Hardware Address > On.
- **Forget Wi-Fi.** Before traveling, especially if they are identifiable as a company or home.

3.0 What to do if you get Hacked

3.1 If Personal Documents are Leaked

- **Passport.** Call HM Passport Office +44 300 2220000.
- **Driving License.** DVLA (can place an administrative marker on your record which will prevent unauthorised activity with your driving license details) write to: OFT, D13, DVLA, Swansea, SA6 7JL. Also call DVLA: +44 300 790 6801.
- **Birth, Marriage, Death, Adoption Certificates.** Call the General Register Office on +44 300 123 1837.
- **Bank.** Call your bank, ask them to monitor your account, and order replacement cards.
- **Report Fraud.** Report to Report Fraud.

3.2 If Something Personal is Posted

- **Report to / Remove:**
  - Facebook
  - Twitter
  - Instagram
  - Snapchat
  - Remove from a Google search
  - Google copywrite complaints to have picture removed
  - Reporting fake profiles on LinkedIn
  - Report to Report Fraud

3.3 If Your Account is Hacked

- **Gmail**
- **Microsoft**
- **Facebook**
- **Twitter**
- **Instagram**
- **LinkedIn**
- **Your Bank.** Regularly ask your bank for a progress report. If you are unhappy with their progress, then you should complain. Find out how to do this by checking their website. If it's been 8 weeks since you complained, and you haven't got your money back, contact the Financial Ombudsman.
- **Police.** Report the scam to the police by calling 101. Remind them to pass the email address to the ISP who might be able to identify the account holder. Ask the police whether they will (or if there is a need to) report the scam to:
  - Citizens Advice Bureau who will pass to Trading Standards for investigation.
  - Report Fraud by calling 0300 123 2040 Monday to Friday 8am - 8pm or using their online reporting tool after creating an account.

3.0 What to do if you get Hacked cont.

3.4 If Your Computer is Hacked

- **These are the main signs that your computer may be compromised:**
  - Your computer crashes at random intervals and being unusually slow.
  - New icons appear on your desktop.
  - Programmes run without your commands.
  - Your contacts receive spam from your email address.
  - Notifications informing you that a program is trying to access the internet without your commands.

3.4 Protect your computer

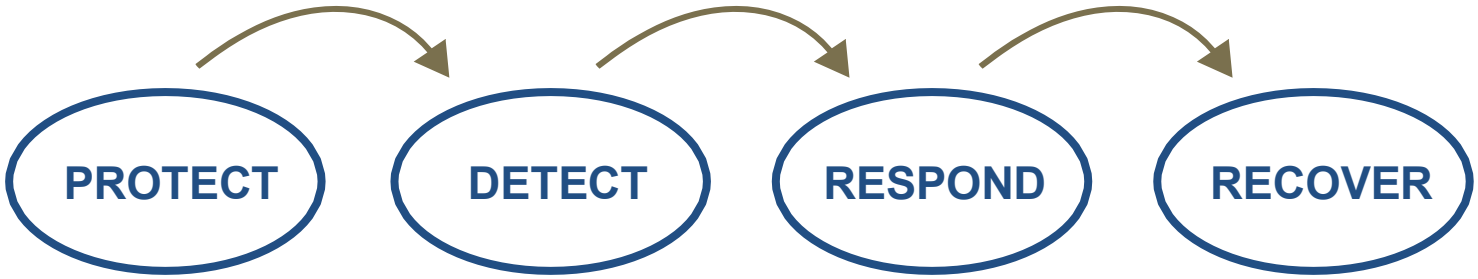
The best way to avoid your device from being infected with **malware,** or a virus, is to install **anti-virus** and **anti-malware** software - and ensure that your computer's operating system and applications update **regularly.** Set a reminder to check for updates **every week.**

Be **suspicious** of websites that offer to automatically download software, or which pop up a window suggesting that your computer is **infected** with a virus or malware. Always update your personal computer using a built-in App Store or software update function.

AVOID SHARING DEVICES, SUCH AS USB MEMORY STICKS, AND PLUGGING IN UNKNOWN ITEMS.

Some free software designed to attract users with the promise of **optimising** their computer contains **malware** and is used for capturing **credit card** information.

Protect, Detect, Respond, Recover



Protect Avoid becoming infected:
- Ensure all software updates have been downloaded and installed.
- Applications should be updated.
- Devices should be **backed up regularly** to at least one other location.

Detect Identify when you are a victim of malware or a virus:
- Unwanted **pop-up messages** may appear requesting card details.
- Your system may run **slowly,** or applications may crash.

Respond If you believe you have been infected with malware:
- **Immediately** disconnect from any network.
- Do not power down the device as an investigation may be required.
- **Contact IT Support.**
- If it is a personal device, scan with anti-malware **and** anti-virus software.

Recover Recover from the cyber incident:
- Contact IT Support or trusted contractor.
- A fresh operating system may need to be reinstalled.
- Previous backups should be scanned for malware and viruses.
- A safe, uninfected, backup of data restored to the computer.

If you believe that your work computer has been infected or there has been a data leak - the best thing to do is to let someone know, so the negative impact of the breach is reduced, and experts can begin the steps to save your data. It is not a good idea to attempt to solve the problem yourself if you are unsure about the steps and protocols.

3.6 If Your Signal or WhatsApp Accounts are Hacked

- **Warn your friends and family.** If you no longer have access to your account, the first thing you should do is to let your contacts know. You should warn them not to trust any messages they receive from your account.
- **Unlink Devices.** If you do still have access, you should open the app on your phone, tap on Menu, then Linked Devices. This will show you all your active sessions with the last active time. Log out from each device individually.
- **Contact WhatsApp/Signal.** WhatsApp and Signal do not have a phone number you can call but you can report the hack using these websites for WhatsApp or Signal

torosolutions.co.uk
info@torosolutions.co.uk
+44 (0) 208 132 9267