Malware Checklist

Malware (short for malicious software) causes a computer or device to perform unintended operations, often unknown to you.

It is often hidden in websites, apps, online advertisements, and pop-ups, but most commonly sent via fake emails or SMS designed to look and sound like a legitimate company or person. Fraudsters want you to act on the hidden threats within a message by opening an attachment, clicking on a link or downloading the image(s).

Signs and symptoms of malware can vary significantly. Some forms of malware will be obvious (e.g., ongoing pop-up ads, browser redirections or general system slowness etc. while others will be completely undetectable and generally not identified until something has gone wrong.)

What to do if you think your device may have malware:

Identify your impacted technology

- ❑ Ensure you have appropriate anti-malware software on your devices. Speak to an IT Professional for a suitable recommendation
- ❑ If it's a laptop or desktop, remove anything connected to it, such as USBs or Bluetooth connectors
- ❑ If it's a mobile, iPad or tablet, disconnect from Wi-Fi, hotspots or mobile data
- ❑ Remove any suspicious apps, and factory reset the device. Resetting the device is usually found in the settings app of your device
- ❑ You may wish to engage an IT provider to remove the malware for you. In this case, leave the device completely turned off until you have had it cleaned. By cleaning your device, you're removing threats that might potentially further compromise your information and security.

Speak to St.george or your Bank

- ❑ Report your personal details as potentially compromised
- ❑ Review and report any suspicious or unusual transactions immediately, particularly recent payments that you did not authorise
- ❑ Request Security Keywords be added to your account, along with any additional security measures your Bank may offer
- ❑ Change the password on your Internet Banking, on a different device (not one you suspect has malware) and enable Two Factor Authentication (2FA)
- ❑ Review and update any alternate sign in options you may use.

Malware Checklist

Protect your devices from malware:

❑ Be cautious before clicking on links in emails and SMS:

- Before clicking, hover over links in emails to show the actual address of the website and confirm the link is directing you where you expect to go
- Be wary of requests to open attachments, or download images within an email
- Validate through a verbal conversation that the sender is legitimate before opening or enabling any files or programs.

❑ Don't download unauthorised or illegal software copies – these can adversely affect your device/s

❑ Always download apps from trusted sources (such as the Apple App Store and Google Play) and read the reviews before downloading

- Keep your apps and operating systems up to date – these updates protect you from the latest malware and security threats
- Use Two Factor Authentication (2FA) everywhere it's offered - this provides a way of 'double-checking' that it's you accessing your accounts by requiring multiple forms of validation on sign in, e.g., sign in credential and password plus a secure code.

❑ Regularly back up your data including your photos and store it separately and securely

❑ Avoid Wi-Fi connections that aren't password protected and never conduct sensitive transactions on non-secure or public Wi-Fi connections

❑ Secure your devices with anti-virus software and run regular virus scans. Anti-virus provider McAfee has a great offer for our customers - get 6 months free subscription at stgeorge.com.au/mcafee

Protect your Personal Information

❑ Contact IDCARE - Australia and New Zealand's national identity & cyber support service. IDCARE provides free, confidential support and guidance to people who have been targeted by fraud, scams, identity theft or compromise. Visit idcare.org or call 1800 595 160

❑ If you are a small business, you can check out our Cyber Response playbook available at stgeorge.com.au/incident-response

❑ Change your passwords on all online accounts straight away, including any social media, apps, or emails, etc. on a different device (not the one you suspect has malware)

❑ If you think someone may have accessed your online accounts, report it to the relevant company

❑ Check your email account and ensure there are no suspicious emails in either your inbox or other folders e.g., deleted or sent items. Check for mailbox rules that you may not be aware of

❑ Report suspicious emails or emails you believe may be linked to the malware to cyber.gov.au/report

❑ Alert your family and friends if someone has taken over your social media accounts, your email account or is impersonating you in any way. Tell them to report the account and block any further contact.

For more helpful information, visit:
stgeorge.com.au/security

st.george