How do I protect my personal data and devices?

IT FAQs - 2019-08-20 - Stay Safe Online

Your online identity and personal data represents a lot of your life, study and wellbeing. The consequences of unknown &/or criminal parties getting access to it are at the very least a huge amount of hassle and worry, and at worst can adversely affect you, your contacts, and your credit rating for years. A whopping 1.3M people fall victim to identity theft annually, so to avoid being one of them make sure you get in the habit of doing this lot....

- Never leave your devices unattended and unlocked.
- Put a screen lock pattern / PIN code (ideally 5 digits) on your Smartphone
- Windows key + L locks all Windows devices
- Always sign out fully from a public PC, including NMIT ones.
- Don't 'over share' on social media & know your privacy settings
- Backup your personal data regularly
- Avoid using flash/pen/USB drives – they're very insecure and can easily fail/get lost
- Auto-sync to cloud files storage services like OneDrive or Google Drive instead
- Consider encrypting your data
- Use antivirus software and keep it auto updated
- Auto-update for Windows/Adobe/Java security updates – your device will perform better too
- Don't download files / attachments from untrusted sources
- Upgrading to a new phone/computer? Remove/wipe/erase storage on the old one.
- Follow the guidance in our how do I keep my NMIT account secure FAQ
- Use the Stop & Think before you Click techniques from other FAQs