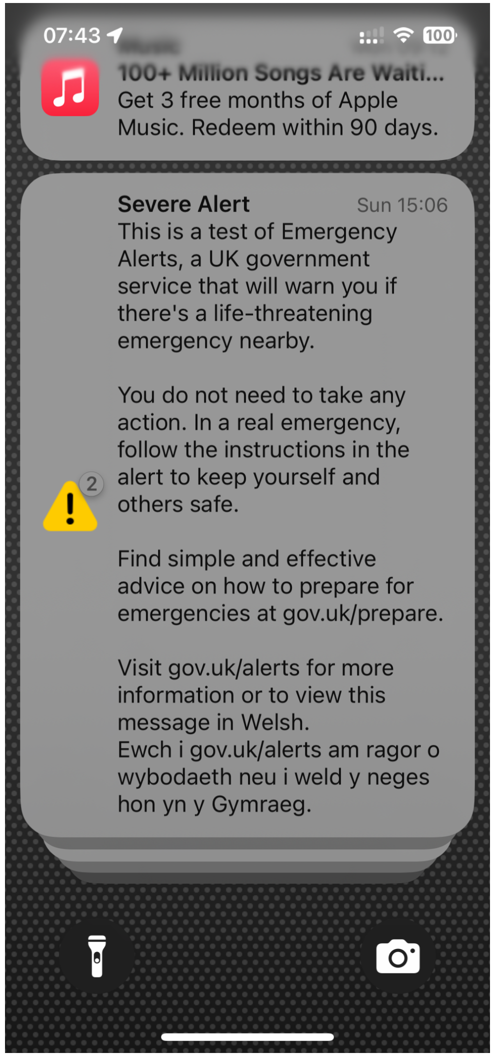
# Smartphone and Tablet Security

Mendlesham Computer Club

By Giles Godart-Brown

# Emergency alert test



Music

**100+ Million Songs Are Waiti...**
Get 3 free months of Apple Music. Redeem within 90 days.

**Severe Alert** Sun 15:06

This is a test of Emergency Alerts, a UK government service that will warn you if there's a life-threatening emergency nearby.

You do not need to take any action. In a real emergency, follow the instructions in the alert to keep yourself and others safe.

Find simple and effective advice on how to prepare for emergencies at gov.uk/prepare.

Visit gov.uk/alerts for more information or to view this message in Welsh.
Ewch i gov.uk/alerts am ragor o wybodaeth neu i weld y neges hon yn y Gymraeg.

# Introduction

- Smartphones are essential tools for communication, work, and personal use.
- They store sensitive data: contacts, emails, financial details, photos.
- Security is crucial to protect against threats like malware, theft, and data breaches.

# Common Security Threats

- Loss or Theft of the device.
- Fraudulent messages to steal information.
- Spyware and Tracking Apps.
- Malicious apps or links.
- Accessing non-secured sites on Public Wi-Fi.

# Things to do
# before
# it is lost or stolen

Mendlesham Computer Club

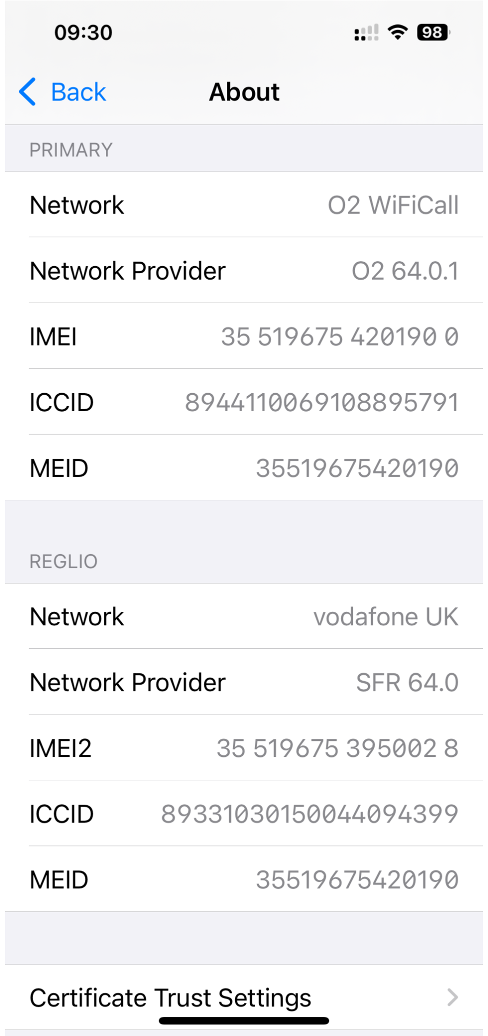
By Giles Godart-Brown

# Best Practices for Smartphone Security

- Use Strong Passwords and PINs - don’t write them down!
- Enable biometric authentication (fingerprint or face).
- Enable Two-Factor Authentication wherever possible.
- Update Software whenever a new version is available
- Only Download Apps from Trusted Sources - Google Play Store or Apple App Store.

# Keep a record  the Phone’s IMEI number

- If your Phone is lost or stolen you need to know its unique serial number - the IMEI
  - iPhone
    - go to Settings > General > About, and then scroll down to find the IMEI/MEID information
  - Android
    - dial *#06# on your phone, or
    - go to Settings > About phone, then scroll down to find the IMEI



PRIMARY

| | |
|---|---|
| Network | O2 WiFiCall |
| Network Provider | O2 64.0.1 |
| IMEI | 35 519675 420190 0 |
| ICCID | 8944110069108895791 |
| MEID | 35519675420190 |

REGLIO

| | |
|---|---|
| Network | vodafone UK |
| Network Provider | SFR 64.0 |
| IMEI2 | 35 519675 395002 8 |
| ICCID | 89331030150044094399 |
| MEID | 35519675420190 |

Certificate Trust Settings

# Extra protection - iPhone/iPad

- Enable FaceID or TouchID
  - Go to Settings > Face ID & Passcode, enter your passcode> Set Up Face ID and follow the on-screen instructions to complete the two-part facial scan
- Enable Find My on your device
  - Go to Settings> Apple ID> Find My> Find My iPhone and toggle the switch to on. You should also turn on Find My network to locate your device even when offline and Send Last Location to send its location to Apple when the battery is low
- iPhone Stolen Device Protection - This is an iOS (Version 17.3 or greater) security feature that adds an extra layer of protection against theft by requiring biometric authentication (Face ID or Touch ID) and delays for sensitive actions when your iPhone is away from familiar locations, like your home or workplace. It is enabled by
  - Go to Settings > Face ID & Passcode> Enter your device passcode> Stolen Device Protection, then turn Stolen Device Protection on or off.
- Enable Data wipe to erase all data after too many passcode attempts

# Extra protection Android -

# Instructions may differ on some devices

- Enable face protection
  - Go to Settings>Security and privacy (or Security) > Device lock (or Biometrics and security)> Face Unlock (or Face recognition).
- Enable Theft Protection features
  - Go to Settings> Security and privacy > Device unlock > Theft protection
    - Theft Detection Lock automatically locks the device if it senses it's being snatched,
    - Offline Device Lock protects data from thieves who might disconnect your phone from the internet,
    - Remote Lock allows you to secure your phone from any device with your verified phone number at Android.com/lock.
- Enable Find My Device
  - Go to Settings > Google > All services > Find My Device

# What to do if
# it is lost or stolen

Mendlesham Computer Club

By Giles Godart-Brown

# What to do if you lose your device or it is stolen

- Try to Locate It with Find My iPhone (iOS) or Find My Device (Android) from another Phone /Tablet/PC.
- Put the phone in Lost Mode or erase it - Lost Mode disables Apple Pay or Google Wallet automatically.
- Lock the Device Remotely to prevent access.
- Erase Data Remotely if recovery is unlikely.
- Contact Your Network Provider to suspend the service or block the IMEI.
- Change Passwords for accounts linked to your phone.
- Report to Authorities with IMEI for recovery/insurance.

# What to do with your wallet

- Suspend or Remove Payment Cards
  - For Apple Pay: Log in to iCloud.com> Select your device> Remove cards from Wallet.
  - For Google Wallet: Go to Google Pay > Choose the lost device>Remove cards.
  - For Samsung Pay: Sign in to your Samsung account> Lock or erase wallet cards.
- Contact Your Bank or Card Issuer immediately and freeze or cancel cards linked to your phone’s wallet and ask for replacements if necessary.
- Notify Your Mobile Carrier, they can help suspend SIM-based services, which adds another layer of protection.
- Monitor Your Accounts - keep an eye on your bank statements and transaction alerts for suspicious activity.

# Find My demos

Mendlesham Computer Club

By Giles Godart-Brown

# Other Security Concerns

Mendlesham Computer Club

By Giles Godart-Brown

# Advanced Security Measures (Unlikely to be needed)

- Check App Permissions when installing new Apps
- Consider installing Antivirus software.
- Have a plan for recovery of key photos or files in the event you cannot access the Cloud.
  - Access the cloud from a PC Browser and download to its disk or a USB drive

## Things to remember

- Though unlikely, phones are not fully immune from threats.
- Beware of phishing attempts, notably emails and texts from bad addresses
- Be “street savvy”