Smartphones are the most intimate form of computing we have ever had, and permeate many people’s lives day in and day out. Securing these devices is now more important than ever, as a compromised device can lead to the loss of personal and professional data. This project compares the security posture of Google Android and Windows Phone 7 smartphones against each other using a set of practical experiments and then provides recommendations for users and network operators to help improve device security.

### Problem
Users want to know what is the most secure platform to protect themselves from smartphone security threats – Google Android or Windows Phone 7.0?

### Solution
Both users and network operators can take a number of measures to secure Google Android and Windows Phone 7 devices

### Generic Risks
- Data loss/leakage
- Poor disposal
- Unintentional data disclosure
- Phishing
- Spyware
- Network spoofing attacks
- Surveillance
- Dialware
- Financial malware
- Network congestion

### Comparative Experiments
1. Data loss and data leakage – examining the possibility that physical access to a device could result in data being accessed or retrieved
2. Unintentional data disclosure – exploring the way in which each device manages downloaded applications and prevents private data such as location data being inadvertently disclosed
3. Detecting phishing emails – how does each platform provide protection to the user from phishing emails
4. Network spoofing attacks - how a device can be spoofed into connecting to a fake mobile phone network
5. SMS message attacks – how easy is it to configure each device to send automatic SMS messages, mimicking the action of some smartphone malware.

### Conclusions
- Users should prevent others having physical access to their smartphone device
- Applications should only be obtained from official marketplaces and the offer of a cheap or free version of a paid for application should be treated with suspicion
- Network providers should investigate how email data is presented to users and maybe evaluate an email scanning application
- High security users and those that need to protect the integrity of their data and voice traffic should consider selecting to use a 3G signals only
- Network providers could consider monitoring sudden surges of calls to transient premium rate numbers indicating a possible Trojan infection
- ... and finally if both devices are secured and used based on the recommendations in this report they would both achieve the same approximate level of security.

---

**SMS Message Attack**

```java
// --- sends a SMS message to another device
private void sendSMS(String phoneNumber, String message)
{
    PendingIntent pi = PendingIntent.getActivity(this, 0, new Intent(this, test.class), 0);
    SmsManager sms = SmsManager.getDefault();
    sms.sendTextMessage(phoneNumber, null, message, pi, null);
}
```