Minimising the Mobile Threat

pcadvisor.co.uk [London, UK] Malware is bad, but it's not bad for everybody.

Cyber crooks are partial to the odd web threat as their income depends on it. Many criminal gangs operate like legitimate businesses - recruiting bright young adults, training them and benefiting from their developing skills.

More legitimately there is a multi-billion dollar industry in combating malware. Security software vendors love to destroy web threats but they'd be out of business if they no longer existed.

Fortunately for them that's unlikely to occur - as soon as one threat vector is closed down, the criminals move on. Where 10 years ago cyber crooks spent time coding elaborate malware, now relatively unskilled salaried crims simply tweak existing threats to evade signature-based antivirus. If you know where to look you can buy malware kits for just a few pounds, which is only a few pounds less than the cost of a hacked ID. That's why we all need to add in behavioural- and heuristic security software to our Windows PCs - traditional antivirus, anti-spyware and a firewall is now just the first line of defence.

The mobile threat

Malware exists only to make money, and criminals by and large prefer to pick the low-hanging fruit. This is why the threat to your mobile is real, and set to explode. We increasingly spend and bank via our smartphones - and crime follows the money.

Because mobile devices are so much more personal and portable than your PC you have more to lose. I'd rather have my wallet stolen then my phone hacked or nicked. My phone has a physical value, offers access to the contents of my wallet, and gives up enough of my data to make spoofing my identity as easy as drawing a face on a beachball. (This is a decent physical description.)

But the mobile threat is very different to that faced in the desktop world. Social engineering is a growth area in all computing, but by and large the Windows bad guys are trying to install software on to your PC, the good guys stopping them.

There have been a few live viruses in the iOS ecosystem, and a ton in the Android world. We can expect Windows Phone 8 to be a big target just as soon as it is big enough to deserve the attention. But the real danger rarely comes from rogue software trying to install itself on your device.

The two major modes of attack in the mobile world are fiendishly simple: physical theft or loss of your phone, or a legitimate looking app mistakenly installed by you. You have noticed the weakest link in your smartphone's security setup – it’s you.

Security software can definitely help. As with Windows security you should definitely have antivirus protection, but only to filter out the background threat. Much more important is to be able to physically track your device if it is stolen. Good security software will let you wipe and brick your phone as soon as you know it is gone, so that even as you are lamenting the cost of replacing your favourite toy, your bank account is not being emptied - preventing you replacing it. It’s like insurance – a sensible investment to minimise loss.

But the most important way to stay safe is to adopt an attitude of suspicion – act on the web as you would on the street. If something looks wrong, it probably is.

So when you buy any security software look out for a mobile component – ideally one that helps reduce the impact of loss or theft as much as it claims to keep your phone from being infected. And do yourself a favour and stay savvy when surfing on your smartphone.

Matt Egan is Editor of the UK's best-read technology magazine and website, PC Advisor. Follow Matt's Twitter account, @MattJEgan, and visit pcadvisor.co.uk

to keep up with the latest tech news and reviews.

Mobilesecurity