

Viruses, they're not just for PCs anymore

By [Sean Cocks](#)

5 Dec 2011

Viruses, malware, spyware and spam are all common terms in today's connected world and most users who access the Internet using a PC, laptop or notebook would not dream of doing so without some sort of security solution. Cyber-crime has become the world's most profitable underworld "business" and users are now aware of the need to protect themselves from falling victim to any number of threats.

New avenues for cyber-criminals

However, the world has become increasingly mobile over time and technology has evolved so that cellphones have become smartphones, along with tablet PCs and other mobile devices allowing always-on connectivity. While such devices have revolutionised the way we work and have grown exponentially in popularity in recent years, this also opens up new avenues for cyber-criminals with malicious intent to exploit users.

In the cyber-crime industry, as with any profitable business, the smart enterprise goes where the customers are. As more users migrate onto a variety of mobile platforms, from BlackBerry to Android, Windows Mobile, Apple Mobile OS and even tablet devices, cybercrime is increasingly targeting these platforms as methods for the perpetration of a variety of malware, including viruses, spam and spyware, all with the express purpose of making money.

Mobile security becoming increasingly important

Users are now vulnerable to viruses that can shut down their smartphones; identity theft as a result of spyware and the entire gamut of threats that were once the exclusive realm of computers. As a result, mobile security is becoming increasingly important for users to protect themselves from falling victim to malicious activity.

Aside from the threat of malware, the increasing trend towards mobility, along with tools such as push email functionality, also means that more and more personal and business information is now stored on highly portable devices. The greater the levels of portability, the greater probability that the device, and the information it holds, may be lost or stolen. Having personal and business-critical information falling into the wrong hands is undesirable for obvious reasons, and the ability to wipe the device remotely in the event of it being misplaced is another strong reason as to why mobile security is so important in today's world.

Features to look out for

When looking for a mobile security solution to protect devices, such as smartphones and tablets, from malware and to ensure personal information does not fall into the wrong hands, there are several features to look out for, which take care of security in the event of loss or theft and also help to prevent malware attacks from causing problems on the device and prevents cross-infection of other devices.

Remote locking capability is one crucial feature, which lets you remotely disable a lost or stolen phone to prevent strangers from accessing private information. It also prevents thieves from actually using the device, so that they cannot run up large phone bills at your expense. This, combined with SIM card-locking capability, which instantly locks your phone if its SIM card is removed, so thieves cannot use it with a different SIM card, ensures that even if your phone is stolen, the thieves will not profit from it as the device is effectively rendered unusable.

Wiping your phone's memory

Remote wipe is also critical, as this lets you actually erase all of the information contained on your phone if it is lost or stolen, including contacts, text messages, call history, browser history, bookmarks, and any data on the phone's memory card. Mobile threat protection will detect and remove malware such as viruses and other threats without affecting phone performance, and download threat protection will automatically scan all files and app updates for threats.

Aside from these now-vital security components, a comprehensive mobile security solution also lets you block calls and text messages from specific phone numbers, perfect for getting rid of annoying spam SMS' and unwanted callers.

Mobile devices are increasingly common, which makes them more and more vulnerable to attack. Protecting all of the personal information stored on your mobile device is of the utmost importance to prevent all-too-common issues, such as identity theft, and mobile security is no longer just nice to have, but a necessity for both consumer and business users in the modern world.

ABOUT THE AUTHOR

Sean Cocks is Norton and PC tools retail product manager of Drive Control Corporation.

For more, visit: <https://www.bizcommunity.com>