



From: www.csoonline.com

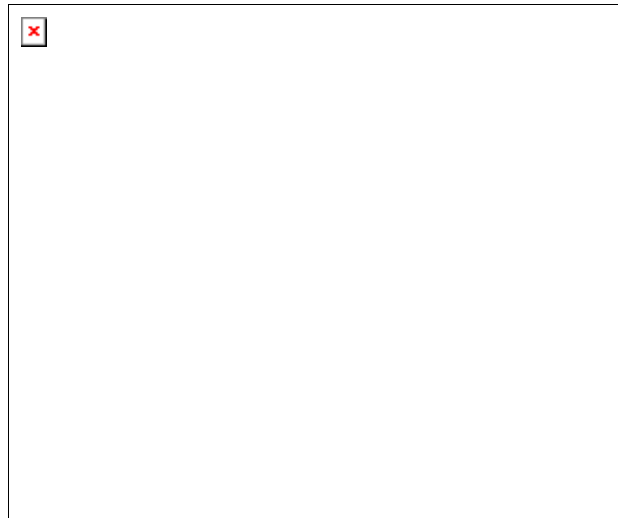
The Top 5 Stupid Things People Do With Mobile Phones

A lost mobile device can be just as bad as a lost laptop - Mformation's Matt Bancroft takes a look at the careless errors that make it so.

Matt Bancroft, Mformation, CSO

November 20, 2008

Mobile devices get smarter every day, and more of us than ever depend on them. But there is a drawback to our increasing dependence on smart mobile devices—they have the potential to be even more risky than laptop computers. This risk is due to two key factors. First, users tend to be as careful with their mobile devices as they are with their laptops, and second, security solutions (encryption, [antivirus](#), etc.) are not as pervasively deployed on mobile devices as they are on laptop computers. A recent survey from [Credant Technologies](#) found that a staggering 94 percent of the IT security professionals surveyed now believe that mobile devices pose more of a security risk to companies than mobile storage devices (88%) or laptops (79%).



To add to that, a recent series of online workshops and surveys conducted by IT research firm Freeform Dynamics, which gathered input from both IT and business professionals, revealed that the attitude of mobile users to security is either poor or variable in 80 percent of organizations. Only one IT security professional in five indicated that users have a consistently good attitude towards mobile security.

A 2007 study commissioned in part by the National Cyber Security Alliance appears to bear out the above. The study was based on interviews with 700 mobile workers in the United States, United Kingdom, Germany, China, India, South Korea, and Singapore. Among the findings:

- 73 percent of the mobile workers surveyed said they aren't always aware of security threats and best practices when working on the go.
- Nearly 30 percent of the mobile workers admitted that they "hardly ever" consider security risks and proper preventative behavior.

With an increasing number of smart mobile devices playing an ever more important role in businesses of all types, it is time that we considered some of the "stupid" things people do with their mobile phones—some of which they would never consider doing with their laptops—and what companies can (or cannot) do to protect users from themselves.

#1: Disabling the lock feature on the phone and/or not establishing a password to unlock an idled phone
This is how lost mobiles become dangerous mobiles. Because they are so small and so portable, mobile phones are easier to misplace or steal than laptops. The numbers are staggering. According to a survey commissioned by [Pointsec](#), 85,000 mobile phones and 21,000 PDAs and smartphones were left on taxis in Chicago over a 6-month period in 2007. The survey also found that more than 63,000 mobile phones and 5,800 PDAs and smartphones were left in London taxis during the same 6-month period.

According to the Credent Technologies survey mentioned earlier, even given these types of loss statistics, over half of the supposedly security-conscious respondents (56%) surprisingly confessed to 'not bothering' to use a password every time they used their own mobile device or smartphone. This is the most basic security precaution for mobile devices and often the first line in defense. Billions of dollars are being spent on information security, yet companies are leaving their back doors and windows wide open by allowing uncontrolled mobile device access, risking sabotage, hacking and exploitation. Management software that can remotely lock/wipe high-risk content from lost or stolen mobile phones can protect users from themselves. A more proactive approach is to put in place management software that enables enterprises to establish security policies for their mobile devices and applications—policies like requiring the use of [a strong device password](#) for unlocking an idled phone—to ensure consistent protection for all mobile employees.

#2: Keeping information that could compromise company security in "plain sight" on the phone (e.g., keeping server or other passwords in Notes or Contacts, keeping detailed/sensitive information on an unsecured device)

Many of us are starting to use our mobile phones as tiny computers, and are keeping all sorts of data on these devices. According to a survey of global-500 CIOs conducted by [Coleman Parkes](#) for Mformation, more than half of companies surveyed reported that technical product, sales and/or customer details are being kept on employees' mobile devices, many of which are personal devices rather than company-issued devices. The same Coleman Parkes survey also found that only 12 percent of enterprises have a full record of the data being stored on their employees' mobile devices.

To make matters worse, this critical company data is being kept on unsecured devices. According to the McAfee 2008 Mobile Security Report, 79 percent of consumers are knowingly using unprotected devices, with another 15 percent unsure of their devices' security levels. All sorts of information is being kept in "plain sight" on mobile devices and could be devastating to an enterprise if it fell into the wrong hands. Consumers, operators and especially enterprises are finding that they need remote management capabilities that can enforce security policies on mobile devices, and keep the data on those devices safe, even when individuals aren't as careful as they should be with it.

#3, Opening an application from an unsecured/unknown source

Without mobile applications and content—from messaging and email to games, business applications, productivity software, educational content, and even health and fitness systems—a mobile device is basically just a phone. Every day, more applications and content are being developed specifically for mobile devices. But not all applications are created equal. Downloading/opening a "bad" &mdash or even just poorly constructed—application can cause all sorts of problems. Users of mobile Web and other mobile applications are very concerned about the lack of protection from "bad" mobile applications and content. In McAfee's 2008 Mobile Security Report, 64 percent of mobile Web users surveyed expressed worry about surfing on the mobile web/downloading content.

Enterprises in particular want to be able to establish and enforce security policies that ensure only authorized applications can be loaded onto employees' devices. They also need to be able to ensure that employees have the correct versions of key applications. Consumers also need quick resolution to any problems they might have as a result of a bad application or service being downloaded.

#4: Using the phone to access dangerous/risky Web sites and Internet locations

Most mobile devices provide Internet access, making it just as easy to access risky Web sites and Internet content on a phone as it is to access this content on a computer. We all know what sort of havoc some Web sites and Internet locations can wreak on a computer—from crashes due to viruses and malware, to unsolicited content that affects performance. This issue is now a problem for mobile phones as well.

According to McAfee's 2008 Mobile Security Report, more than 86 percent of mobile users worry about receiving inappropriate or unsolicited content, getting fraudulent bill increases, or suffering information loss or theft. In addition, one in seven global mobile users report that they have already been [exposed to mobile viruses](#), either directly or through knowing someone whose phone has been infected. Consumers and enterprises alike need to be able to protect themselves from these problems with the ability to block unsolicited content and to recover quickly and completely if a mobile device is infected.

#5: Leaving the device open to access (e.g., leaving [Bluetooth](#) or WiFi on, visible and unsecured)

Some of the most prevalent mobile viruses and worms use an unprotected Bluetooth connection to get into mobile devices or to spread to other devices. This includes two of the most common mobile device viruses, both with a number of variants, Cabir and CommWarrior. As yet, there have not been reports of attacks on mobile phones via open WiFi connections, but experts say that with more mobile devices connecting via WiFi, they are

susceptible to the same types of attacks as any computer on an at-risk network might be.

In addition, it is possible for external sources to hijack an open, unsecured connection such as Bluetooth or WiFi in order to enter into corporate networks, where they could cause harm to corporate systems or data. One way to minimize the risks these open connections can present to an enterprise is to establish and enforce policies about restricting access to certain mobile device functions, such as WiFi or Bluetooth, under certain circumstances, protecting corporate data and assets from outside attack.

Mobile devices are changing the way we all live, work and play. Most of us wouldn't think of leaving home without our mobile devices, and more of us are using mobile devices—whether they're our personal devices or issued by our employer—for work every day, even if it's just to check our email when we're not in the office. We need to start treating our mobile devices in much the same way as we treat our laptop computers. Implementing security solutions and policies, as well as remote management support for all mobile workers—whether they're using personal or company-issued devices—are big steps in the right direction toward protecting these increasingly powerful devices and the critical data on them. ##

Matt Bancroft is chief marketing officer for mobile device management provider Mformation.

© CXO Media Inc.