Symantec Consumer Guide to Wireless Device Security

The deployment of wireless mobile devices – including personal digital assistants (PDAs) such as Palmtops and BlackBerrys, cell phones, smartphones, and laptops – is growing faster than the Internet. The number of smartphones worldwide, for example, is expected to reach 49 million by the end of the year (a 150 percent increase over 2004), and nearly 130 million by the end of 2008, according to IDC.

Wireless Device Security

There are specific information security issues that users of wireless mobile devices need to deal with, partly technological but primarily human: wireless technology frees you from the wires of the desktop computer, enabling you to work in ways that suit you, and where, when and how it suits you. This is what is propelling the dramatic increase in the deployment of wireless technology. However, wireless technology is extremely insecure and therefore exposes information to significant risks, ranging from loss or destruction of confidential personal data to identity theft. And as wireless mobile devices become multifaceted and more ubiquitous, carrying more and more valuable and important information, so the risks and threats to information stored on them will increase.

Owners of small businesses face additional risks: failure to properly secure important customer and user data can expose them to legal and regulatory action, loss of reputation, and commercial failure. In their own interests, individuals and small businesses need to make a personal, pro-active effort to combat the current and emerging risks to the information they store and work with everyday on their Palmtops, BlackBerrys, cell phones, and smartphones.

WIRELESS TECHNOLOGIES

As wireless communication becomes an increasingly substantial part of the economic infrastructure, it's also becoming an increasingly worthwhile target for hackers, virus writers, and organized crime. Information is at even greater risks because more and more of the technology in which it is stored and communicated is vulnerable and insecure.

As an individual user of a wireless mobile device – either in the home or using a public hotspot – everything on your computer may be accessible to an outsider; it's as easy as simply opening and reading any of your folders and files without you being aware of it.

There are three primary wireless technologies, deployed in cell phones, PDAs, and smartphones:

- Bluetooth
- Mobile telephony
- Short message service

BLUETOOTH

Bluetooth is a short range wireless technology. It is a radio frequency standard that allows any sort of electronic equipment to make its own short range connections, without wires, cables, or direct action of any sort from a user. It is an inexpensive, wireless and hassle-free technology that is being deployed in a wide range of digital equipment.

Bluetooth is not restricted to line-of-sight, but its effective range is about 10 meters or 40 feet; this short range is a result of its very weak signal, selected to avoid the danger of interference with other devices that use the same range of frequencies.

When two Bluetooth enabled devices encounter one another, they can automatically communicate with each other to establish whether or not they should form a personal-area network. This simple facility creates the opportunity for Bluetooth attacks. Bluetooth devices, particularly cell phones and smartphones, are at risk from three types of attack by nearby or passing devices: bluejacking, bluebugging, and bluesnarfing.

What is Bluejacking?

A bluejacking exploits the key Bluetooth functionality that allows users to exchange business cards electronically with one another. It means that third parties can send text messages anonymously to the smartphones or PDAs of any users who are within range (usually 10 to 20 meters, or about 40 to 80 feet), and it could be used maliciously (for instance to hassle or bully someone) and for "bluespam." Bluejackers look for a response from the receiving phone or its user before sending a more personal message.

Phone owners should refuse to add senders of bluejack messages to their address book and, better still, should remain "hidden" from Bluejackers by keeping their Bluetooth settings in non-discoverable mode. Non-discoverable mode will not affect devices that have already been paired, but it will protect you from blue attacks.

What is Bluebugging?

A bluebugging attack is a hack attack on a Bluetooth enabled device. While the hacker must be within 10 meters of the phone that is being attacked, the attacked phone's user will not be aware of the attack. Bluebugging enables the attacker to initiate phone calls on the victim's phone, to read and send short message service (SMS) messages, read and write phonebook contacts, eavesdrop on phone conversations, divert incoming calls, and surf the Internet.

A bluebugging attack requires advanced hacking skills and freely available hacking software. The situations in which it is most likely to occur are those in which a number of Bluetooth users are within easy range – a coffee shop, train station, or airport lounge are ideal locations.

What is Bluesnarfing?

A bluesnarfing attack is as serious as bluebugging because it can involve the theft of all contact information stored in the cell phone. It is illegal, but that doesn't stop criminals. Some of the information could be particularly confidential and/or valuable to a third party. However, not all cell phones are vulnerable and, as manufacturers respond to the discovery of these vulnerabilities, there will be security improvements.

Beware of Pairing

If Bluetooth is on, it should be a basic rule of self defense that you don't "pair" with any unknown devices. If an unknown device flashes up on your cell phone screen, and you are asked whether to pair or not, DECLINE. Similarly, you should not download or install suspicious or unknown software onto your cell phone and if, during installation of new software, your device produces a safety warning, you should have very strong reasons for ignoring it.

Wherever possible, you should upgrade your cell phone PIN to an 8-digit code from the standard 4-digit code with which it is issued. Never share the PIN with unknown devices or individuals. The truly security conscious users will only pair devices in a secure or confidential area, where they can be sure that no hackers are within 10 meters and capable of capturing the PIN.

The other defense is to avoid buying any phones that are at risk of bluesnarfing and learn to live with the problems of bluejacking – you simply need to move more than 10 meters away and, unless the perpetrator is following you, you will be out of range. Bluebugging remains a threat, however.

Losing a Bluetooth device

If you lose one of your Bluetooth devices, you need to protect all your remaining devices by immediately unpairing (deleting) the lost device from those that remain. This will make it impossible for the lost or stolen device to be used to access all the services of your paired devices that are still within range.

MOBILE TELEPHONY

The mobile telephony universe has two originally distinct but increasingly overlapping categories of devices: cell phones and PDAs. Smartphones are devices that have features of both categories.

Cell phones

The biggest information security risks relating to cell phones come from the tendency of users to speak about confidential or sensitive matters in public places. There's always a chance that someone will hear what is said and will be able to make use of the information; and conversely, the fact that people can use cell phones to bypass security installed on corporate telephone networks, whether call recording, call blocking, or anything else. Cell phones (particularly privately owned ones) are the simplest and easiest way for someone in possession of confidential information to pass it beyond the organization's secure perimeter.

These, though, are issues for the organization to deal with – and it requires a combination of clearly stated policy, clearly written and understood employment contracts, straightforward staff training, and an uncompromising disciplinary policy.

Risks to cell phones

There is a small, but growing number of cell phone security issues that individuals and small businesses need to consider. These risks are larger on smartphones, because of their greater functionality and the amount of data they carry.

There are essentially three principal cell phone risks:

- Blue attacks (dealt with in Bluetooth, above)
- Loss of essential data (through accident or theft of the cell phone)
- Viruses, worms, Trojans, and malware

Cell phone loss

Loss or compromise of cell phone data is a far greater issue. Millions of cell phones are lost or stolen every year. When a phone is lost or stolen, two things happen, apart from the cost and inconvenience of the loss: someone else can use the phone to make calls, and all data (all the stored contact information and telephone number details, etc.) is lost.

There are obvious precautions cell phone users should take:

1. Don't use the phone in areas where it could be stolen, and keep an eye out for possible attackers.
2. Ensure that the phone, when not in use, is secure – in a briefcase or purse (itself kept within eyeshot) or in a pocket, but not just lying on the table or seat next to you where anyone who distracts your attention can then grab it.

3. Lock your cell phone. There are several locking methods and, in each case, you should change the default manufacturer's code (because criminals also know the defaults):

- Key lock: this locks your keypad, to prevent accidental number keying
- SIM PIN code: this locks your SIM card, protecting your account, even if the SIM is transferred to another phone
- Phone security code: this locks your handset, as distinct from the SIM card or the keypad
- Network PIN/call barring code: this enables you to change network level call barring options
- Voicemail PIN: this secures your voicemail service

4. Back up your cell phone. Your phone should have come with a CD-ROM that enables you to back up contact data to your desktop computer. You should run this backup routine on a regular basis if you change your contacts' details frequently. Otherwise, you should do it every few months, or at least once a year. Then, if you lose your phone, it is relatively easy to reload the data onto a new cell phone – and it is equally easy to alert all your contacts that the phone has been stolen.

Malware

Mobile phone malware is an increasingly important issue. The possibility of spreading mobile phone viruses, worms, and Trojans has been proven and only the relative simplicity of phones and their limited range of functions have so far prevented this from becoming endemic. In 2005, cell phone malware is still at a developmental stage. At the moment, not all cell phones are vulnerable, and malware is only just starting to spread. As cell phones become increasingly powerful, this will worsen. You should keep informed about the development of these threats and take appropriate action as and when necessary.

The three practical counter measures are:

- Never accept or install any program on your cell phone that you don't recognize or which you are not expecting. Currently, known cell phone viruses need to be accepted or installed by the phone user, so DON'T DO IT. This is particularly important if you are downloading games or files from file sharing or freeware sites, or if they are sent by a friend.
- Download, install, and keep up to date a cell phone anti-malware software package. Companies that currently supply such software are: Symantec, for PDAs and smartphones, McAfee, also for PDAs and smartphones, and F-Secure, for some cell phones.
- Keep your operating system up to date. Malware exploits software vulnerabilities; as vulnerabilities are identified and patched, threats are removed. You should therefore check the Web site of your cell phone supplier every few months to see if a patch or upgrade for the operating system on your cell phone has been released and, if it has, install it.

SHORT MESSAGE SERVICE (SMS)

SMS flood attacks, which occur when an attacker sends SMS messages in sufficient volumes to represent a Denial of Service (DoS) attack, are less important than they used to be, because service providers have largely dealt with this threat on their SMS gateways. A DoS attack is one in which your device and/or service (your e-mail inbox or your SMS inbox) are flooded with messages from another device, making it impossible for you to continue using the service and, often, exhausting your battery power and costing you money.

The rise of SMS capabilities in Web site marketing tools will make SMS spam a major challenge for 2006. Provider SMS gateways should identify and stop a substantial portion of spam, but spammers will get more cunning and will succeed in bypassing these controls. You will need to keep up to date with developments on this front.

Only you, as an individual user, can deal with the most obvious security risks where SMS messaging is concerned: a message can easily go to the wrong person or if it's not delivered within a short time, it expires; you can't get a receipt, so you don't know if it arrived anywhere; you don't know who else might be reading the

screen when the message arrives; and you certainly don't know who might later access the SMS memory and find your message. The guidance is simple: use SMS only for unimportant, non-confidential communication. If you do use it for something confidential, phone and get confirmation of its arrival, and make sure confidential texts are deleted from the phone's memory.

SMARTPHONES AND PDAS

Smartphones, PDAs, and other handheld devices are ubiquitous; they improve productivity and flexibility for individuals and employees. Almost everyone who has a smartphone or PDA uses it for both personal and business purposes. Personal use includes storage of confidential personal data (identity information, contact lists, bank account details, user names, PINs, credit card details, etc). Business information includes confidential data about your employer, co-workers, clients, suppliers, and about problems and issues – much of which may also be subject to privacy or data protection legislation.

A recent survey by Symantec found that:

- 60 percent of respondents store confidential business or client data on their phones and send or receive confidential business or client e-mails from their PDAs and smartphones
- 55.7 percent of PDA and smartphone users said they store confidential personal data on their devices
- 54 percent said they send/receive e-mails on their devices that include confidential personal data
- 41 percent said they access bank accounts; 31.3 percent said they access credit card accounts; 19.7 percent access mortgage statements; and 17.7 percent access stock portfolios.

Theft or loss of a Smartphone or PDA

This could be a huge problem for users as the theft of confidential information on computers continues to increase exponentially and wireless mobile devices appear to be the next frontier for such attacks. There are specific security risks, much greater than those related to ordinary cell phones, which need to be considered because thieves and criminals all know how much confidential information is stored on smartphones and PDAs, and how poorly they are secured.

Apart from the sensible practices that users can take to avoid having a smartphone or PDA stolen or lost, the one practical step that might lead to the return of a lost PDA is to have all the information on the device protected and inaccessible. No one will be able to use it, which means they will also be unable to access anything, including your contact details.

Malware

The risk to a PDA or smartphone from viruses, Trojans, worms, and other malware is zero if the device is only operated in stand alone mode. However, as half the benefit of the device comes from its wireless connectivity, it is vulnerable to malware. The risk is both to the PDA or smartphone and to any computer or corporate network to which it connects, in that the malware could be uploaded through the HotSync/ActiveSync function or through its direct connection to the network. The only practical solution is to download, install, and keep up-to-date anti-malware software.

General Security Principles for PDAs and Smartphones

- PDAs and Smartphones must be password protected, preferably with a strong password (eight digits, alpha-numeric)
- Devices must not be left unattended (while charging, for instance) – unless secured in a locked device or room, or with an appropriate alarm

- The wireless port on PDAs and smartphones must be disabled (to prevent transmission of confidential data to unauthorized individuals)
- Appropriate anti-malware software must be installed and kept up to date
- Device operating systems must have the latest patches installed (which means keeping in touch with your supplier's Web site(s), as automatic updating is not yet a big feature of PDA and smartphone operating system support)
- Any confidential (including corporate) information stored on a device must be encrypted, perhaps stored in an encrypted database
- Back up regularly – by synchronizing the device with a linked computer

Wi-Fi LAPTOPS

802.11 Standard

"802.11" is a group of standards for wireless local area networks or LANs, segmented into a number of different versions, and adopted at different times. 802.11b is the wireless standard that was originally known as Wi-Fi. It has been widely adopted and is the most widely available and used; it is compatible with 802.11g and has a maximum outdoor range of about 120 meters (approximately 480 feet) and 50 meters indoors (200 feet).

802.11g is compatible with 802.11b, but is usually several times faster. An 802.11g device can access an 802.11b hotspot, but will run at the slower speed. Most laptops today provide both b and g Wi-Fi.

Wi-Fi equipment is sold and usually installed with its manufacturer's default security settings intact. These settings are "no security." No security means that anyone, including the completely innocent, can connect to a wireless laptop or wireless network and use it for their own communication purposes, to access shared resources on the network, and even to access individual folders and files. A malicious user could use an unsecured wireless laptop or network for spam or malware releases, for cybercrime or cyberterrorism purposes.

Wi-Fi's "Evil Twin" Attack

Evil twin attacks are slowly mounting as wireless device users are increasingly conducting business over the Internet. While grabbing a few minutes of connectivity is convenient and productive, identity thieves are discovering that, through "evil twin" attacks, hotspots are a great way to steal unsuspecting users' private information and business data.

While users are connecting their laptops, PDAs, and smartphones to a wireless network or hotspot, a hacker may be in the area sending out his own Wi-Fi signal, with an exact replica of the sign-in Web page of a legitimate service – hence the name "evil twin."

The damage from an evil twin attack can have many consequences. An intruder can degrade network performance or deny service completely. An evil twin may offer fake login prompts to steal user names and passwords, which can then be used for later access by the hacker or a third party. The hacker's goal is to have unsuspecting surfers log on to the page and dole out private, sensitive data including credit card numbers, passwords, and confidential business information.

As new wireless technologies appear, hackers will devote more and more time to discovering and exploiting new vulnerabilities – paralleling what has occurred in the wired world. However, unlike the wired world where there is an obvious physical connection between the attacker and the victim, in wireless environments, locating the source of the attack is much more difficult. This difficulty reduces the risk to the attacker, thus increasing the attraction.

False Sense of Security

There are several measures already in place by most Web browsers to warn about unencrypted Web pages. However, various security flaws still exist in these browsers.

- Pop-up warnings: Web browsers often use a pop-up dialog box to indicate that information being sent is not encrypted. However, these boxes offer the option to users to "turn off" the dialogue box so it never appears again. Even when enabled, many users are prone to simply clicking through such warnings without paying much attention.

- The "lock" icon: Most Web browsers display a small lock icon to indicate an encrypted Web page. Though users should be diligent about looking for them every time they log on to a new Web page, they often are not. Additionally, hackers often register commonly misspelled domains names or ones that closely resemble legitimate sites. When a user is redirected to that page it will display the lock icon, and the user may not notice the changed domain name. While the connection to the site may be encrypted, the user is not communicating with the site they believe they are.

- HTTPS and unfamiliar links: Many financial services advertise the unencrypted version of their Web pages (https indicates a secure version; http, however, is easier to remember). When a user logs on to that page and clicks to enter the encrypted version, he or she can be redirected to a page with a domain name that is different than the company's normal home page. If users don't recognize the name, however, it is difficult to know if they have been redirected to a page operated by the company or a hacker.

Security basics for Wi-Fi laptops

The biggest risk associated with Wi-Fi activity is, in fact, the loss or theft of the Wi-Fi enabled laptop or other devices. Before taking any action to secure Wi-Fi communication, it is important to establish the physical security of the device itself. The risks associated with the physical loss of a laptop or wireless mobile device include (but are not limited to):

- Loss of confidential or proprietary information, which might expose you or your employer to litigation, loss of competitiveness, loss of reputation, loss of clients, loss of suppliers, breach of M&A information, stock exchange regulations affecting confidential information exposure, etc.
- Loss of irreplaceable information, which might expose you or your employer to severe interference or disruption
- Loss of confidential access information (user names, passwords), which might enable a malicious acquirer of the laptop to access and compromise (or plunder) your or your employer's resources

In the office, physical security means using computer locking cables during the day to ensure that laptops that are in use on desks cannot simply be picked up and removed. In theory, laptops are safer at home than they are in an unattended office (i.e., don't leave your laptop or other wireless mobile devices on your desk overnight), as long as the home is secured from theft.
The real challenge is in transit: it's what happens to the laptop in the coffee shop, in its bag on the bus, plane or train, or in the taxi cab. More laptops are lost in taxis than by any other means. The basic guidance (apart from paying attention) is store laptops in nondescript carry bags, or inside brief cases or luggage – anything that doesn't look like a computer case, so as to avoid encouraging a passing criminal to consider stealing it.

When in public places, hold on to the laptop at all times, especially in bars, hotels, and airport lounges. When you're not using it, keep it under your feet or better yet, on your lap. Do not leave a laptop unattended, not in a public place, not on view inside a vehicle, not anywhere. Keep a close eye on it when you go through a security checkpoint – someone might grab it while you're distracted by something or someone else.

Even as new vulnerabilities are identified and exploited, users can mitigate or eliminate many of the wireless security risks with careful education, planning, implementation, and management. Some of the following measures are not specific to wireless networks. However, when connecting to a public wireless network such as a hotspot, a user's device is arguably more exposed to threats than when at home or at work (and behind a firewall), it becomes more critical to consider such basic measures. The following tips will aid this process:

1. **Check Your Wi-Fi Settings**. Many laptops are set to constantly search and log on to the nearest hotspot. While this option might seem convenient, it does not allow you to monitor which hotspots you are logging on to and determine if they are legitimate. Turning off this option will prevent your computer from logging on to a hotspot without your knowledge.
2. **Download only from reputable sites.** While it's tempting to download freeware or shareware on a wireless device, it is risky as well. These types of programs can potentially contain malicious code masquerading as legitimate programs.
3. **Use one credit card on the Web**. Open a credit card account that is used solely for the purpose of shopping on the Web. Ideally, you should be able to access account records online so you don't have to wait for monthly statements to monitor account activity. Also verify the issuing company's policy for dealing with fraud.
4. **Do not store authentication credentials.** Although it requires more work to log in when passwords and other authentication criteria are not automatically saved, it also makes unauthorized access more difficult.
5. **Use passwords that are not easily guessed, and change them often.** This remains one of the most overlooked but effective and easy deterrents to security breaches. While not specific to wireless networks, due to the increased risk of eavesdropping in such environments, it becomes more important.
6. **Configure your device to prevent the indiscriminate sharing of resources.** Consider the range of your wireless device and the potential hacking opportunities a simple misconfiguration can present to users with malicious intent; then lock down your device. Turn off unused services such as file sharing.
7. **Use a virtual private network (VPN).** This software creates a secure tunnel into a remote network and provides both encryption and authentication. Users connecting to corporate networks from public locations such as hotspots, hotels, and conferences should always employ a VPN to limit risk.
8. **Back up often.** While this certainly doesn't *prevent* a security breach, a complete and recent backup makes recovery from a security incident a great deal easier—but only if the source to which you back up is secure.
9. **Keep apprised of the latest wireless security offerings, standards, and breaches.** Find a handful of online wireless security sources that offer current, concise, and clear information about developments in the wireless arena, and check them regularly. In a market that is as complex and dynamic as today's wireless environment, information is key to not only maintaining but increasing the value of your wireless capabilities.

By employing a complementary combination of security solutions and common-sense best practices, wireless device users can significantly reduce their exposure to security threats. And, as security standards and products evolve, users can prepare to embrace next-generation wireless devices and services that will help ensure their continued success in the wireless future.