

Suite 3  
Woodhouse Corporate Centre  
935 Station Street  
Box Hill North, Victoria  
3129, Australia  
**ABN:** 83 078 025 813  
**Tel:** +61-3-9896-7800  
**Fax:** +61-3-9896-7801  
**Email:** sales@eb2bcom.com  
**Web:** www.eb2bcom.com



## **The Notebook: Your Achilles Heel**

### **Top Tips for Securing your Data from Utimaco**

27th September 2004

- **Security leaks are not only caused by data transfer, but by the mobile device itself**
- **The only effective solution is a combination of encryption, authentication and access management**
- **Top 7 Tips for Securing your Data**

Let's be honest: is it really the fault of problems with a virus protection program, or an insecure hotspot, if notebook users lose data? A recent Gartner study showed that 86% of all security events in wireless networks are caused by the mobile devices – and not by insecure transfer. Utimaco Safeware is a specialist in mobile security. We would like to give you some tips about simple measures for securing your notebook.

The most secure method data is on your desk at home – because you cannot lose your notebook there. A survey of the town lost & found offices in the main German cities, Berlin, Frankfurt, Hamburg and Munich, discovered that more than 25 notebooks were handed in to them in the first half of 2004 alone. If the worst happens, and your computer is stolen or even lost, there is still hope that your personal data is not all accessible, provided you have taken the right precautionary measures.

Here, Utimaco recommends a combination of three protection mechanisms: "With authentication, encryption and access management, to guarantee system integrity, combined with the classic protection tools such as anti-virus systems, you can ensure your notebook is properly protected", says Ansgar Heinen, security expert at Utimaco. "This applies to professional users just as much as to users who simply store things like holiday photos and personal data on their notebook. The most important data that can be lost if a notebook goes missing is often similar for both these kinds of user: sensitive and valuable customer, product or business information on the company's notebooks."

## **Here are the Top 7 Tips for Securing your Data:**

### **1. Discipline when on the move**

The only protection against being careless is more care and discipline – but that is difficult when you are under time pressure. A survey of the town lost & found offices in the main German cities, Berlin, Frankfurt, Hamburg and Munich, discovered that more than 25 notebooks were handed in to them in the first half of 2004 alone. It might sound obvious, but if you travel with a notebook, you should always make sure that you really have the notebook case, including all its contents, over your shoulder before you leave the plane, taxi or train.

### **2. Making passwords more difficult to crack**

If the worst happens, and your computer is stolen or lost, there is still hope that your personal data is not all accessible, if the password is difficult enough to crack. A mixture of characters, numbers and letters is considered the most secure – but only if passwords and keys are not stored on the hard disk. For this reason it is better if the computer prompts for a password before booting– electronic security solutions enable this. This gives an unauthorized user no chance to somehow get access to the operating system or saved data in any way.

### **3. Supplement password protection**

Analysts working for the Meta Group have confirmed what IT managers already know: passwords alone do not provide optimum protection for data. The alternatives have been available, and in use, for years: special smartcards or tokens – which look just like a USB stick – store key information that is used in combination with a user password to unlock the computer. Only someone who has the token and knows the password can access the system and the data saved on it. Another variant, which has still to have its time, and is also a bit more expensive, is to store the user's biometric data on a smartcard. For authentication, the user's fingerprint is checked directly on the card, instead of the password.

### **4. Secure standby mode**

You can set up the system to prompt for the password again when the notebook switches back from the screen-saver or from hibernation mode to normal working mode. This means your data is still secure if you stop for a break or you are making a phone call in the train or airport.

### **5. Set up an electronic safe**

As a basic principle you should never save valuable information without protecting it electronically: important papers are kept in safes. The electronic pendant is a "virtual" disk drive that securely encrypts and stores all its contents. You can very easily set up an electronic safe of this kind on local hard disks and network directories, on the PDA, and also on mobile media such as USB sticks and flash memory cards, CD-ROMs and DVDs, and on diskettes, to provide secure storage of your electronic data.

## 6. Implement automatic encryption

While we're talking about the electronic safe: what use is the best safe, if the valuable data is simply left on the shelf next to it because no-one takes the time to think about whether a particular document needs protecting at all? Here, data transparent encryption is a big help. It runs automatically in the background, without being noticed, so the user does not even have to think about storing data securely.

## 7. Restrict plug and play

Plug and Play is convenient, but can sometimes be dangerous: if someone connects a USB stick, MP3 player or external hard disk drive to a notebook, it is recognized automatically – and it is then easy to start exporting data and passing it on to the wrong people. The alternative is to lock the computer for all memory media apart from the company's own memory sticks which cannot be used to run or read programs. This also removes the danger of accidentally loading a worm or virus on your own hard disk if you lend the data medium to someone, and get it back with a "dangerous cargo". In addition you should only use sensitive data on USB sticks when it is encrypted, as the smaller the memory device, the greater the danger that it will get lost or stolen.

**You can find more information about Utimaco Safeware AG and its products for secure work on the move at <http://www.utumaco.com>**