

PDA misuse threatens security

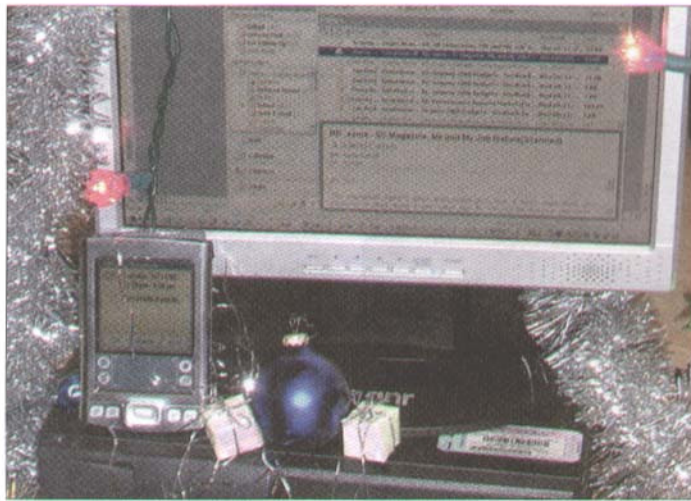
The growth in the number of personal mobile devices such as PDAs and smartphones being attached to corporate networks is raising concerns for IT managers.

Handheld PCs, PDAs and digital cameras can be connected with a USB cable and as they do not have virus protection, they open up systems to virus, spam, spyware attacks and security breaches.

"The problem is usability - modern devices are so easy to install that anyone who knows one end of a USB cable from the other can quickly join their PDA or iPod to their PC," said Robert May, managing director of IT solutions provider, Ramsac. "Unfortunately, their PC usually means the PC they spend the most time in front of, which more often than not is a computer at work."

There are few problems with attaching a device to an office PC, but unchecked hardware and software linked to corporate networks can create serious problems.

"Companies spend a lot of money on firewall protection, e-mail block-



Danger signs: unauthorised PDA use on networks is a security risk

ers and other preventative measures designed to keep e-mail inboxes and file servers free from distracting and destructive files, yet people are unwittingly jeopardising that investment by installing a personal gadget, which has nothing in the way of anti-virus protection, on a business computer without notification or agreement.

"There is no doubt that these gadgets have made modern working life more flexible and accessible, but they have to be used appropriately," added May.

Companies need to issue guidelines on peripheral use, establish access privileges and clarify the type of devices which can be connected to their networks.