# Netzwerkgruppe KaWo1 e.V.

## Security sheet

2007/12/01

This paper should give you a short overview about the ways to keep your computer secure from viruses and malware (malicious software) and protect your data against unauthorized access.

### Worms and other malware

Worms are harmful programs, which spread across computer networks. They cause damage in various ways and unfortunately many users don't know that a great deal of spam (unwanted emails) is being sent from private computer's while the user does not even know something about it. In other cases your surf-behaviour is monitored and/or additional popups are created for example. In extreme cases a worm grants other people access to your computer so it can be remotely controlled over the internet. *In most cases the user does not recognize this!*
Especially an *unpatched* Windows system can be infected over the internet without any userinteraction within minutes. Therefore frequent security updates for your pc are indispensable.

### Security updates

For newer windows versions an automatic update program informs the user frequently about new updates and installs them. Those notifications must not be ignored *in any case*! If you miss those update notifications for a longer time period you should check the settings concerning Windows Update in the control panel. For an effective protection against worms and attacks on your system security updates are essential!
Apart from that for most Windows versions there exist so-called Service Packs which represent a collection of all updates and program fixes until the release of the Service Pack and in case of Service Pack 2 for Windows XP even offer additional security functionality. The known „Personal Firewall“ programs are *not suitable* for protecting your system against worms and hacker attacks. Before connecting your computer to the internet you should check whether you have installed the latest Service Pack for your Windows version. If and which one is installed can be looked up in System of your control panel. A CD with the newest Service Pack for your Windows can be borrowed from the association.
For Windows 2000 currently Service Pack 4 and a Rollup-package 1 with additional updates is available. For Windows XP Service Pack 2 is up to date and for Windows Vista don't exist and Service Pack until now.
We strongly advise against the use of older Windows versions because Microsoft is not supporting them anymore.

### E-mail

Worms often spread as attachments of e-mails in which for example is told you about a bill, a price of a lottery or even a reminder to pay money or a complaint. But also other text try to move the reader to open the included attachment. You should open attachments only if you expect them and can be sure they contain no malicious software. Unfortunately knowing the sender is not sufficient because this can be forged easily. *It is irresponsible to let your e-mail program open attachments automatically!* Often for infection of your computer low security settings of your software or security holes are used, too. We advise against the use of MS Outlook or Outlook Express for reading your e-mails. As an alternative we recommend Mozilla Thunderbird
(`http://www.mozilla.com`) which is described in our documentation.
Another thing are so-called chain letters which should never be forwarded. They often travel through the internet for years, unsettle users, cost them time and even make people send postcards to specific adresses or calling specific telephone numbers for a very long time. You may want to read more about such Hoaxes on the german website `http://www.tu-berling.de/www/software/hoax.shtml`.

### Passwords

Be aware of the fact, that other members of the network can easily login to your computer and control it if you decided to choose a bad password or even no password. Therefore it is recommended to use *good passwords*. A strong password consists of at least eight symbols, containing capital letters, minor letters, numbers and special characters. So a name for example is a poor password, „Nd!bw4np“ would be a strong password. A common trick is making up a sentence, and using the first (or last) letter from each word, while replacing some of them with numbers or special characters. Passwords should never be written down or send by mail. Writing them on a post-it taped to your screen is simply asking for it. Passwords are *never* to be passed on to another person, not even to the administrator.

### Further information and contacts

Further information can be found in the installation manual and on our web pages:
`http://www.kawo1.rwth-aachen.de/kawo1-net`
Feel free to pose your questions in our newsgroup `kawo1.computer`. Alternatively, you can drop in on the administrators office hours or send an e-mail to `admin@kawo1.rwth-aachen.de`.