Hardening your computer, defending against malware and spam

No more Spam!

When I switch on my computer in the morning, it seems that the red light district has taken over my mailbox. The Internet is full of hackers, viruses, Trojans, and miscellaneous malware. BY PATRICIA JUNG

Is it really a good idea to set up a computer "outside your door"? Just like in real life, the answer is yes, assuming that you are well-informed and have the right kind of protection. Even so, there is no such thing as 100% protection against unexpected attacks.

Although you can drown in the bathtub, most normal people feel safe enough leaving their homes and venturing out into the streets, although there is always the danger of a murderer hanging around on a park bench, a pickpocket in the subway, or an inattentive driver not braking in time. The situation in the virtual world is quite similar. If you surf the Web, there is the danger of malware infection. If you have an email account, you are bound to be spammed sooner or later. Also, if you connect your machine up to the Internet, you might be hacked.

Bad enough, but no reason to condemn the Internet, ignoring its advantages and hankering for the good old days before the rise of public networks. Malevolent and criminal activity seems to be inevitable wherever people meet. It does not make sense to bury your head in the sand. Instead, you should work on developing self-defense and self-assertion techniques.

In the case of viruses, worms, and Trojans (see page 20), simply using Linux may be the answer. On the one hand, the Linux operating system provides a certain degree of protection, assuming that you use a non-privileged account to access the Internet. On the other hand, Linux, and the software applications that run on Linux, are not the most attractive of targets to malware authors (or have not been thus far). The article on page 20 tells you how to harden your system sufficiently to safely surf the Internet.

Immune, but not inactive

Although Windows viruses cannot attack Linux software, responsible Internet citizens will try to avoid exposing unsuspecting Windows users to nasty surprises. There are many approaches to doing so: regularly scanning the Windows file servers on the local network for viruses, checking the message from your neighbor for infection before you forward the MS Word attachment to another Windows user (page 35).

Finally, that leaves us with the exasperating subject of spam. Proactive approaches are typically beyond the reach of mere mortal network users, but at least you can react. On page 26, we reveal the techniques that can help you keep your own mail address hidden from spammers for as long as possible, without having to do without email entirely. Just to keep your adrenalin level as low as possible while checking your mailbox, you might prefer to be more circumspect about the type of messages you download (page 30). ■

COVER STORY

Protection 20
Hardening your computer and minimizing the risk of attacks from intruders who are intent on harm.

Spam-proof Homepages...26
How to design and implement spamproof homepages. Avoid the email address harvesters, and reduce your spam load.

POP3 Antispam 30
Save your hard disk space for your needs. Kill the spam on your ISP's POP3 server before it ever gets downloaded to your machine.

Clam AV Antivirus 35
Fight Windows viruses on your Linux box and safguard your entire network with the antivirus tool ClamAV.