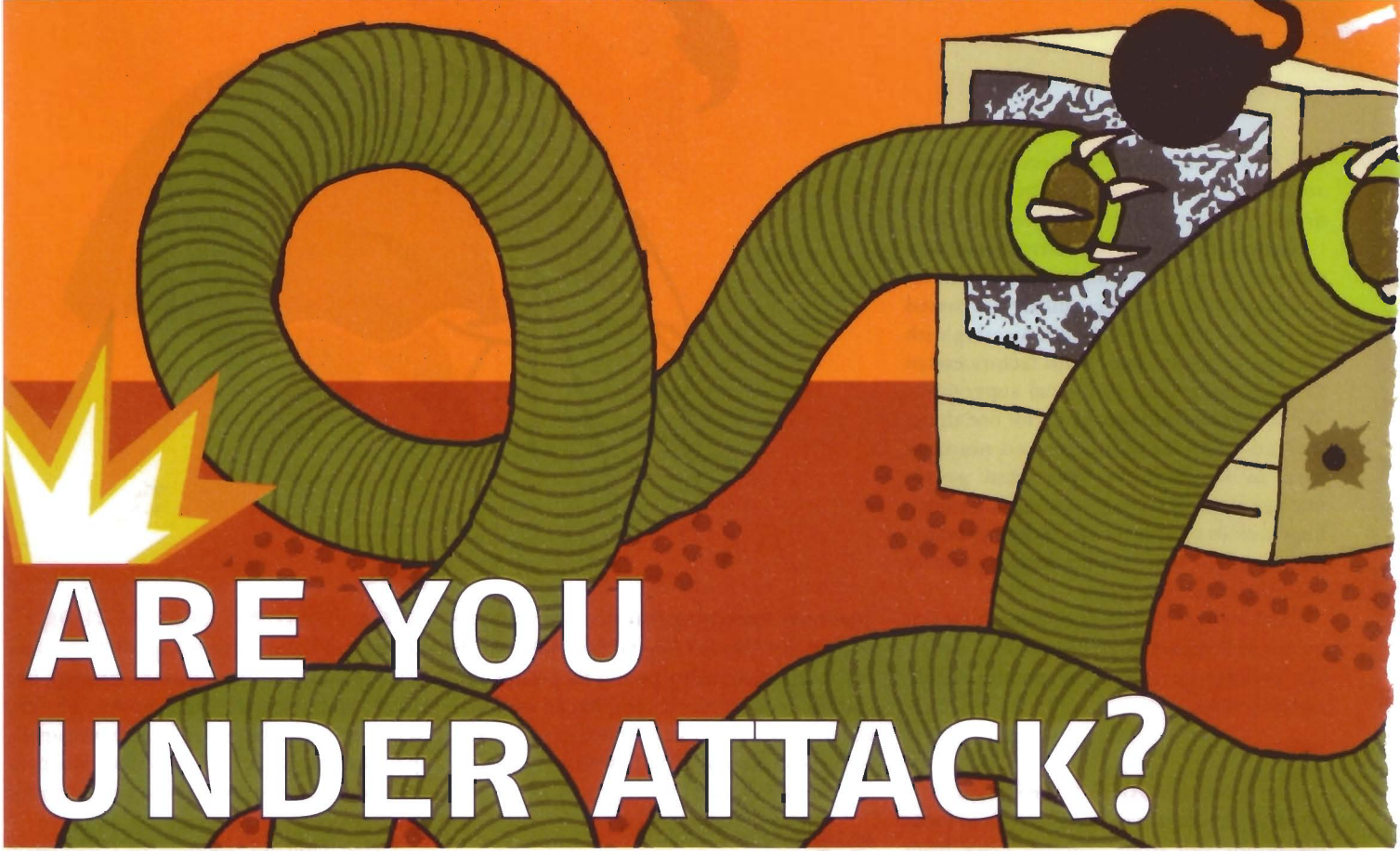


ARE YOU UNDER ATTACK?

There are some nasty, twisted people out there, wreaking havoc on computers. In the first of a two-part series, *Matthew Stibbe* explains how to make sure they don't get at yours.

If you use a computer, chances are you've already had a virus attack and received spam e-mail. You've probably lost some important data. A stolen laptop or a misplaced file will do it. If you have a broadband Internet connection, your system will almost certainly have been probed by hackers. These are the most common risks but a determined hacker can do a lot more damage through fraud, vandalism or theft.

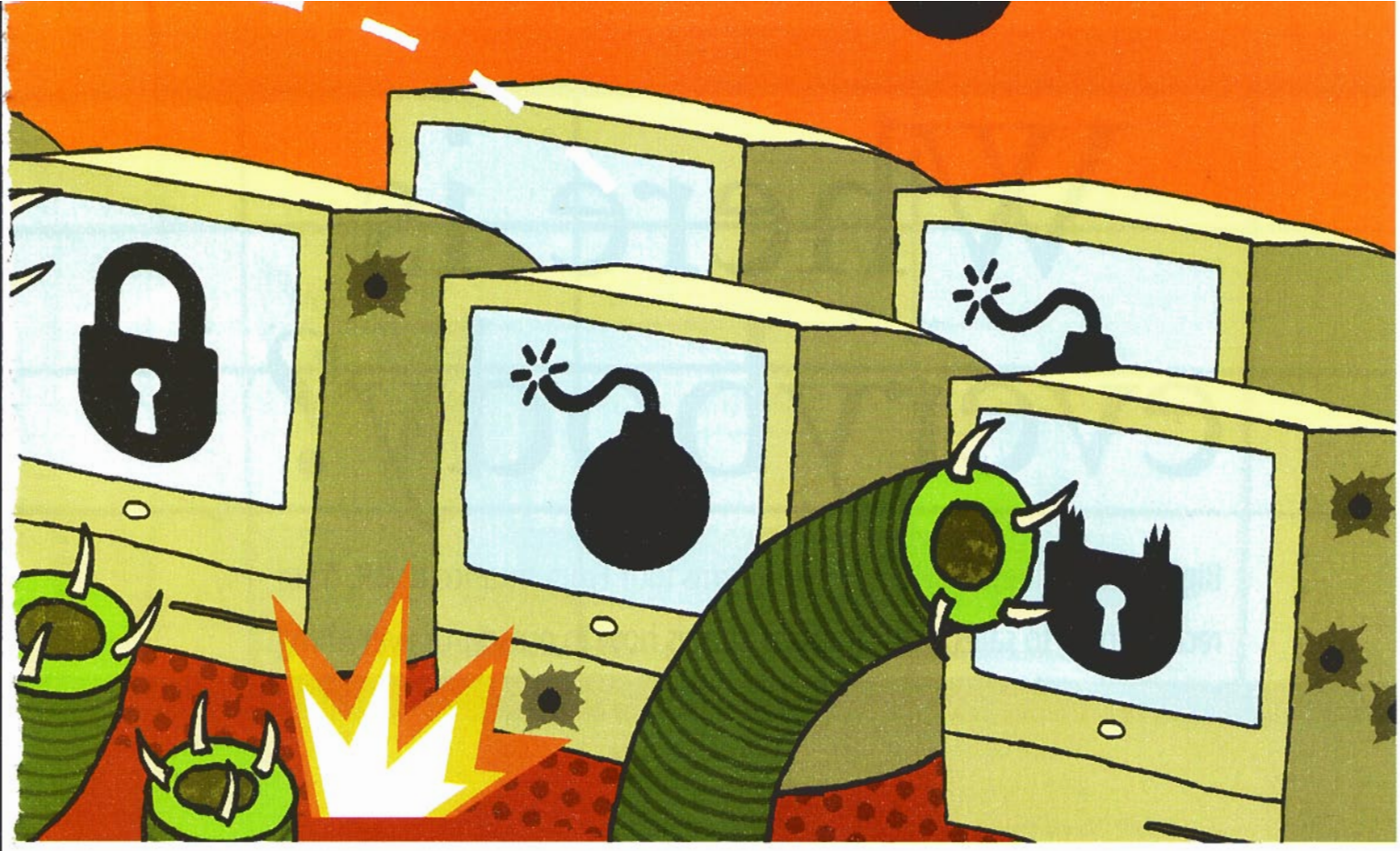
It isn't only sinister hackers and criminals that cause trouble. Sometimes, it's your own employees. Fancy a sexual harassment claim? Over two-thirds of Internet porn traffic occurs during office hours. What about two years in prison? Directors face personal liability for copyright theft and yet three quarters of company networks unwittingly host some form of illegal file sharing software. How about losing all your e-mail and data? Nearly half of all medium-sized firms have no data backup plans at all, according to a recent survey, and most firms have lost a laptop.

No-one's immune. Microsoft recently announced that portions of the source code for some older operating systems had been illegally posted on the Internet. In 2000, an MI5 agent had a laptop stolen at Paddington station and an MI6 agent left his computer in a cab after a pub crawl. Famous companies, including Intel, Gateway, Disney and The New York Times have had their websites defaced by hackers.

These examples show that the problems require a joint effort by software developers and by end-users. Like it or not, we're all geeks now. There are lots of risks, but luckily, the remedies are relatively painless and straightforward. The first three – firewall, software updates, and virus protection– are mandatory and urgent.

Firewalls stop the bad guys accessing your computer over the Internet. Think of a firewall as a Klingon cloaking device and a Star Trek shield rolled into one (I told you we're all geeks now). Like randomly dialling telephone numbers, hackers randomly try to connect to computers over the Internet. A firewall will cloak anything it protects. Even if someone does find your network, it will prevent any unauthorised connections, like a shield. Microsoft Windows XP has a firewall built in. If you use an older version of Windows, consider upgrading. There are also commercial software firewalls, such as McAfee's Personal Firewall Plus v5 and Symantec's Norton Personal Firewall 2004 which cost less than a tank of petrol. And ZoneLabs is free (for personal use only). Industrial-strength firewalls suitable for businesses cost more: for example Symantec's 25-user small business firewall is £1200. Some broadband routers come with hardware firewalls built-in. Ideally, you should have two different firewalls for belt and braces, for example a hardware firewall and a software firewall or XP's own plus a commercial product. Setting up a personal firewall and learning how it works will only take a couple of hours.

Software updates. Just as locksmiths and burglars are engaged in an endless game of attack and counter-attack, so manufacturers constantly try to make their software safer and less prone to attack and hackers look for new vulnerabilities. For this reason, it is vital to keep operating systems (e.g. Windows, Mac OS™ etc.) and application software (e.g. Microsoft Word™, Excel™ or Outlook™) up-to-date with the latest versions. In part this means upgrading to the latest version when appropriate. Newer versions of software products, including Windows™ XP, Small Business Server 2003 and Office 2003 include enhanced security features, making them stronger than the versions they replace. It also means downloading patches and updates for your existing software. As well as security benefits, they often bring performance and feature improvements. For Microsoft products, it is easy to do this. Simply go to www.windowsupdate.com and www.officeupdate.com and follow the instructions. Downloading the patches may take a few hours if you don't have a fast connection but don't let this put you off. Check regularly for new updates.



Virus protection. Viruses are insidious computer programs that people inadvertently download via e-mail or browsing the web. The majority of viruses are dangerous. For example, some are used to forward spam and can clog up your e-mail system; others open backdoors into your network for hackers to exploit. Even the most innocuous take time to clear up. The first line of defence: don't open suspect e-mails or attachments, even if they promise nude pictures of Britney or Brad. The main defence is anti-virus software. This scans all incoming mail, website downloads and programs already installed on your computer for known viruses. There are some free programs for personal use, but businesses should expect to spend around £25-35 per user. Hundreds of new viruses appear each year but anti-virus software can only scan for viruses it knows about, so you have to update them at least weekly so that they can detect the latest nasties.

Anyone who goes online without virus protection, a firewall and up-to-date software (and you need all three working together) may be unwittingly making the problem worse for everyone else. They are also taking an unnecessary risk themselves. These basic steps are the equivalent of locking the office at night and making sure that everything is insured. Next time, I'll look at physical security, passwords, wireless networking, how Microsoft's new Small Business Server can improve security and how to prepare a business-wide security plan.

WANTED: FRIENDLY HACKER

Peter Wood is chief of operations at First Base Technologies, a security consultancy. His job? Companies hire him to hack into their networks (and tell them how to fix any problems he finds). He's been doing it for fifteen years and he is good – very good. But he rarely gets to use his full skills. Hacking is that easy.

One of his favourite tricks is to walk in from the street, bluff his way past reception and hook up his laptop at an empty desk. "We only need one valid user id and password to access a network. In the trade we call that 'Game Over'."

He has software that can break a quarter of passwords on a network in two minutes. Most people use obvious words: password, football, friday or their own name.

Sometimes he doesn't even bother to visit. "Just ringing people up and asking them for their passwords, providing you have a semi-plausible story, works quite well."

He reckons that 50-70 per cent of the risks to a business come from within. Only a very small fraction of the population has the skill to hack in through a firewall. A disgruntled employee or a salesman in exit mode is a more plausible risk.

Most small business owners respond "well, we're not the bank of England, who wants to attack us." My response is "duh! You've only got to upset one employee (and SMEs are not exempt on that score) and they have a motivated would-be hacker. Hackers are not just a weird underground class of misfits, they're you and me."

Where next?

Go to www.microsoft.com/security/protect/default for a step-by-step guide to setting up virus protection, software updates and a firewall.

For fortnightly security newsletters, an online quiz and detailed advice, go to www.bcentral.co.uk/security and www.microsoft.com/uk/security

Order a free copy of the British Chamber of Commerce's Guide to IT Security from:
www.bcentral.co.uk/technology/security/guide

Check out the Government's site:
www.ukonlineforbusiness.gov.uk/informationsecurity

To find a local IT firm to help you, visit:
www.bcentral.co.uk/technology/buy/findpartner

For an extensive list of anti-virus software manufacturers see:
www.microsoft.com/security/partners/antivirus