Small Business Security Guides

How malware can sneak into your company networks & how to deal with it

AVG | AT WORK

How Malware Can Sneak Into Your Company Networks and How to Deal With It

There are myriad ways that viruses, trojans and other types of malicious code can get into your business and it pays to be up on all of them

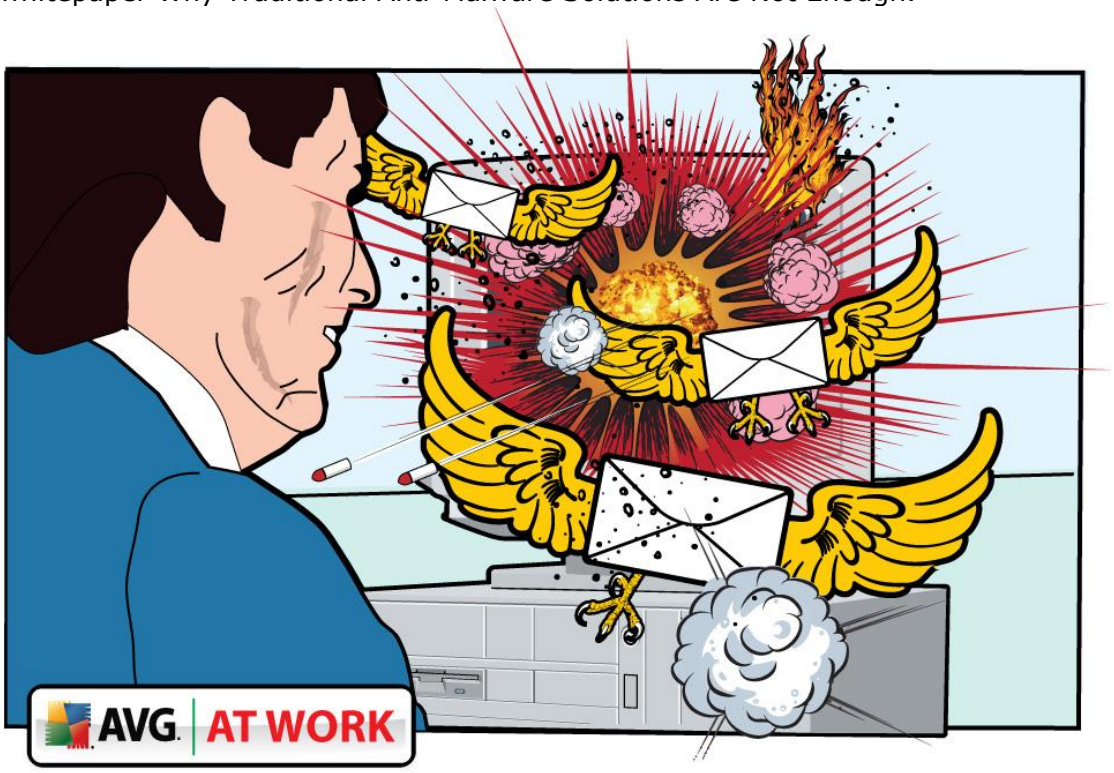
Did You Know:

- Forty percent of companies allow access to social networking technology but only 23 percent have specific security policies
- Seventy percent of the top 100 web sites have hosted malicious code or linked to malicious sites
- War driving is the practice of hunting and exploiting unsecured wireless networks

Taking a fire-axe to your broadband connection might sounds like the only really effective way to keep viruses and other so-called malware out of your business. But even if rolling the clock back to typewriters and snail-mail was practical, there are still a host of other ways for malicious code to worm its way onto your network.

Here's an overview of the main threats and how to protect against them.

1. Email and Spam - Oldies But Baddies
The method of choice for early virus writers was bundling up their wares in email attachments. Although still a popular method of attack, levels of awareness around email-based malware, together with more effective scanning-technology, means it is no longer as effective as it once was. "Email was the primary attack vector and simply installing an anti-virus and exercising caution when opening attachments mitigated the majority of threats," explains AVG in the whitepaper Why Traditional Anti-Malware Solutions Are Not Enough.



Educating employees on good email security etiquette is fundamental while US government site US CERT recommends that users be wary of unsolicited email even if it's from a known contact. "Many viruses can "spoof" the return address, making it look like the message came from someone else. If you can, check with the person who supposedly sent the message to

make sure it's legitimate before opening any attachments," the organisation advises.

Other must-dos to impart to staff include turning off options to automatically download attachments wherever possible. "To simplify the process of reading email, many email programs offer the feature to automatically download attachments. Check your settings to see if your software offers the option, and make sure to disable it," US CERT recommends.

2. Instant messaging - Chatting Your Way Into Trouble

While not as ubiquitous as email, instant messaging has some of the same security risks for those companies that have adopted it. As with email, viruses and other malware can be hidden in files sent via IM. Some staff may be unfamiliar with the IM which can increase the risk that infected attachments will be clicked on so training is a must. Microsoft has some good advice to offer on the issue and warns users never to click on a file sent by someone they don't know. Other advice to close the door on IM malware includes making sure that users email cannot be easily identified by their IM username. "Some IM services link your screen name to your e-mail address when you register. The easy availability of your e-mail address can result in an increased number of spam and phishing attacks" warns Microsoft.

3. Websites/social networking - Why It Pays To Be Antisocial

As awareness of the dangers of clicking on a suspicious email attachment has increased, cybercriminals have sought new ways to spread malicious code. Hosting malware on websites which can infect with a single visit now poise a growing threat to consumers and businesses alike.

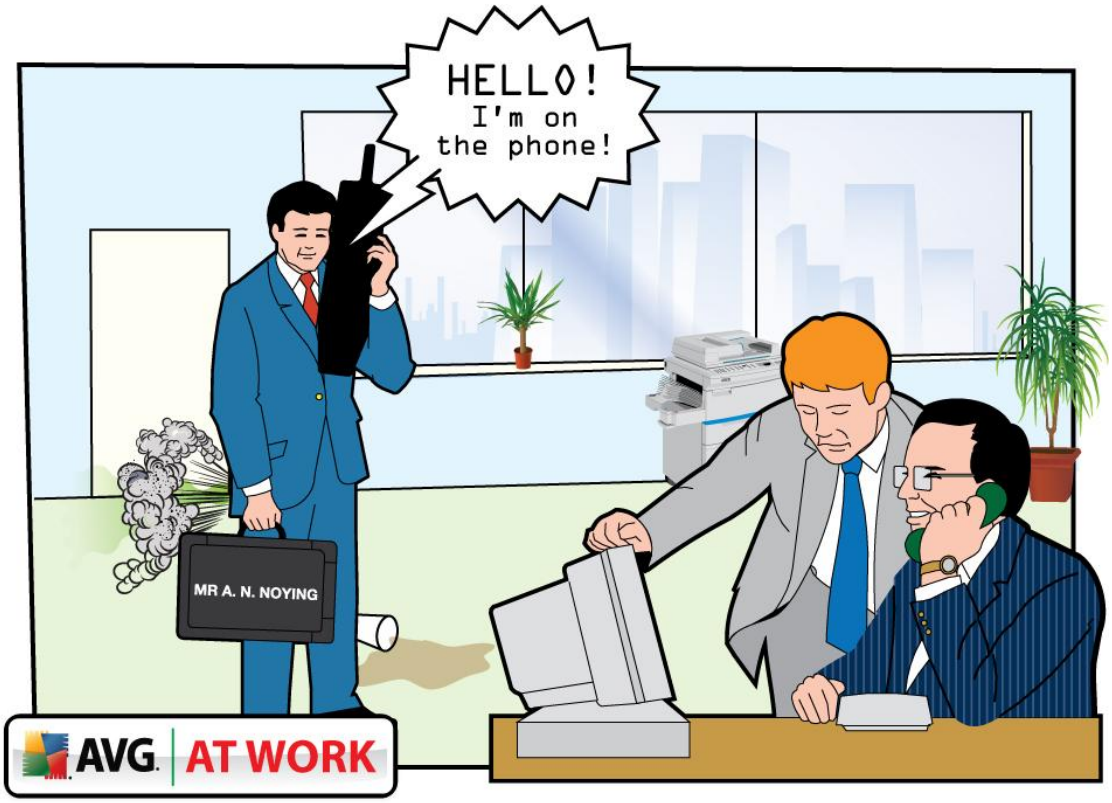
Browsers and their associated add-ons provide a huge variety of ways to compromise websites and deliver malware to unsuspecting surfers. Research carried out in 2008, revealed that seventy percent of the top 100 web sites either hosted malicious code or contained a link to redirect surfers to a malicious web site. "The Web has become the attack vector of choice. With email, attackers had only a limited number of ways to a computer: either with an infected attachment or with a link to a website which would deliver attackers still use email, they have discovered that the Web in general – and social networks in particular - provides them with a much broader range of options" the AVG paper Why-Traditional-Anti-Malware-Solutions-Are-No-Longer-Enough explains.

Social networking sites are particularly worrisome when it comes to harbouring malicious code according to the recent Trial By Fire survey by consultants PWC. Around 40 percent of companies reported that they allow access to social networking technology but only 23 percent said they had any security policies that specifically address the potential problem. "Today a new generation of employees worldwide is accessing social networks from work in great numbers, often without the knowledge of the IT department—and in circumvention of the traditional countermeasures employed by many," the PWC report states.

Aside from updating the organisation's IT security strategy to include the threat posed by social networking sites, companies can obviously simply opt to block the sites altogether. Companies looking for a more subtle response are increasingly turning to web scanning tools. AVG's LinkScanner (http://linkscanner.avg.com/) technology for example checks each site for infections prior to access.

4. Insider threats - Know Your Enemy, You Might Be Employing Them

While companies might rightly be concerned about shadowy cyber-criminals, employees poise a similar or even greater threat when it comes to malware. This so-called "insider threat" attracts a lot of debate in the IT security industry but whether malicious or accidental, staff are responsible for introducing the majority of malware onto company networks.



Education around secure practices can help cut reduce accidents but stopping staff that might want to introduce destructive malware is more challenging. There have been recorded cases of employees installing malware on their company network out of pure malice or with an eye on turning a profit at a later date. One famous example, is that of Michael John Lauffenburger a worker at General Dynamics Corporation who installed a so-called logic bomb on the arms company's network hoping to be hired on to fix the resulting damage at a later date.

While keeping anti-virus and other security software up to date is vital, another way to stop staff purposefully planting malware in the company is not to hire them in the first place. For companies dealing with very confidential information, background checks on staff - especially technical staff - are worthwhile. Psychometric testing which might help weed out personality types capable of sabotaging their own company are another option. Obviously, staff cut-backs and redundancies might provide motivation for staff to plant malware on the company system so staff's IT privileges - especially IT administrators - should be limited or revoked as soon as practically possible.

5. Remote workers - Security that's Out of Sight

While preventing staff from leaking malware into a business has its challenges, staff that are allowed to access the company network remotely are even harder to control. Consumers usually have a laxer approach to updating anti-virus software and system updates than businesses. Allowing staff to use their own machines for work ups the risk that malware may get onto the company network.

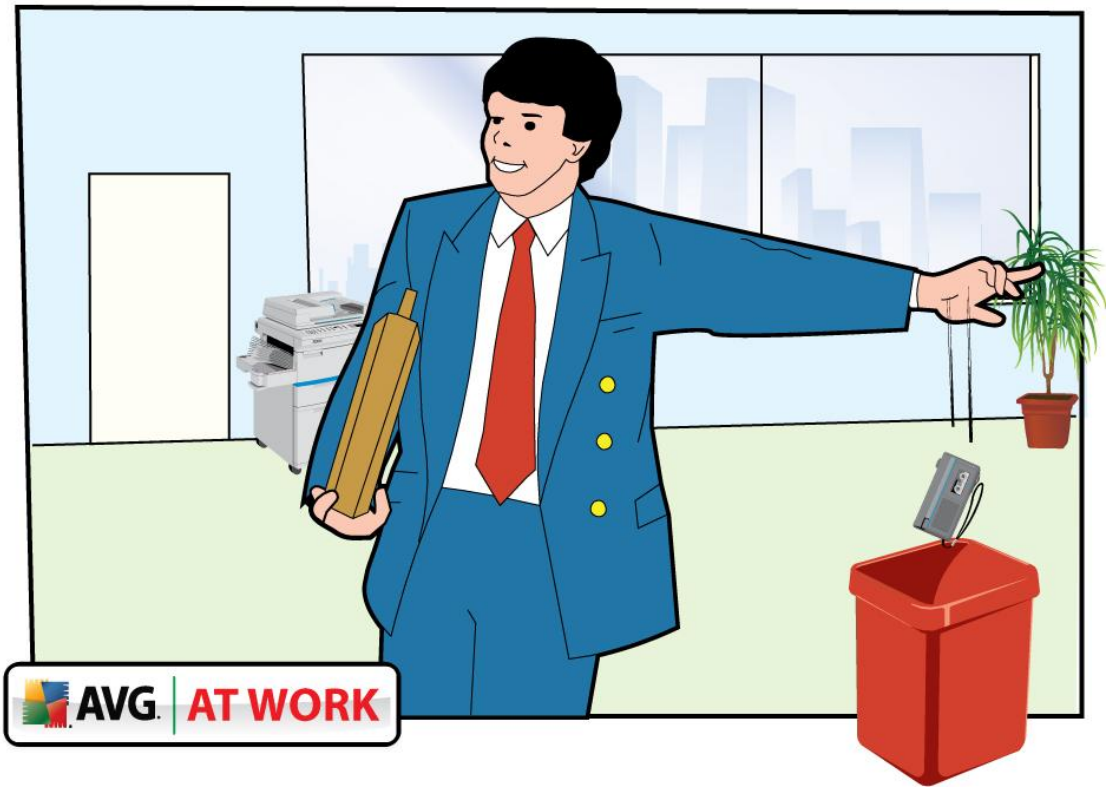
An obvious way to close this particular security hole is to prevent staff from using their own machines. But some companies such as virtualisation specialist Citrix has shown letting staff buy and manage their own devices is a cheaper long-term option than providing company-owned machines. Citrix has got around the problem thanks to its virtualisation technology which effectively creates a virtual safe-zone within the hardware - like an embassy in a foreign country. The use of hosted or cloud applications is another way to ring-fence employee machines as everything is hosted on a central server rather than downloaded locally.

6. USB Sticks - Plug N Play Malware
Memory or USB sticks are particularly good at spreading malware. They appear innocuous compared to a laptop or smartphone but can hold several gigabytes of code. "Because USB drives, sometimes known as thumb drives, are small, readily available, inexpensive, and extremely portable, they are popular for storing and transporting files from one computer to another. However, these same characteristics make them appealing to attackers," US government security organisation CERT advises.

Recent examples of organisations falling foul of USB sticks include Greater Manchester Police which had its computer systems brought down for several days when a USB stick containing the Conficker Worm. Tony Anscombe, AVG's head of free products, explains that removable devices can be automatically checked using AVG software or users can choose to run a manual scan before accessing any of the files on the stick. "The moral of this story is that you should never let your guard down," he says.

CERT's advice on how to avoid malware infection via USB sticks includes the obvious warning not to use any unknown devices but also to keep personal and business drives separate. "Do not use personal USB drives on computers owned by your organization, and do not plug USB drives containing corporate information into your personal computer," the organisation claims.

7. Mobile devices - Smarter Phone Security
Email-equipped smart phones poise the similar risks to company networks as desktop computers. Although the phones themselves are rarely hit by viruses or worms, they can help to spread malware onto other susceptible devices on the network. Hackers and criminals have also been known to use text messages to guide unsuspecting users onto websites containing bad code according to US CERT. "These messages, supposedly from a legitimate company, may try to convince you to visit a malicious site by claiming that there is a problem with your account or stating that you have been subscribed to a service. Once you visit the site, you may be lured into providing personal information or downloading a malicious file," the organisation warns.



Other risks with smart-phones are related to downloading content. CERT's advice is to warn employees not to download games or other unnecessary applications onto work mobiles. “There are many sites that offer games and other software you can download onto your cell phone or PDA," the organisation states. "This software could include malicious code. Avoid downloading files from sites that you do not trust. If you are getting the files from a supposedly secure site, look for a web site certificate. If you do download a file from a web site, consider saving it to your computer and manually scanning it for viruses before opening it."

Aside from email and web access, other ways criminal code could gain access to a mobile device is the short-range networking technology known as Bluetooth. CERT's advise when it comes to Bluetooth it so to make sure employees know to keep it switched-off when it is not needed. "Make sure that you take advantage of the security features offered on your device," the organisation states. "Attackers may take advantage of Bluetooth connections to access or download information on your device. Disable Bluetooth when you are not using it to avoid unauthorized access."

Another issue with mobile devices such as smartphones is that they are increasingly being used as a way to pay for goods and services. This fact means that while some obvious viruses will emerge from time to time, the real concern is more subtle malicious code according to AVG's chief technology officer Roger Thompson. "Viruses have, and will continue, to make it onto mobile devices from time to time," he says. "Just last month, we had a couple of iPhone viruses (or, more correctly, worms), but a virus is really only a virus if it spreads, and the malicious software we're going to see infecting mobile devices will be much more subtle than your typical virus."

Mobile malware will log keystrokes and snoop out user ids and passwords according to AVG's Thompson. "There will also be malware that transmits information about our browsing habits to its masters, who will use that information to decide what ads to serve us," he says. "It's quite likely that the more nefariously-inclined will build up databases of background information about us, to be used to profile us for future criminal activity.

8. Wireless networks - What You Can't See Can Hurt You

As they have the potential to spill outside the physical confines of an office building, wireless networks offer a tempting route for hackers. Some criminals specialise in targeting unsecured wireless networks warns US CERT. Shutting this loop-hole means paying attention to the security settings of the network, the organisation advises. "A practice known as wardriving involves individuals equipped with a computer, a wireless card, and a GPS device driving through areas in search of wireless networks and identifying the specific coordinates of a network location. This information is then usually posted online," US CERT warns.

US CERT also has advice on how to manage firewalls to block wireless attacks. "While it is a good security practice to install a firewall on your network, you should also install a firewall directly on your wireless devices (a host-based firewall). Attackers who can directly tap into your wireless network may be able to circumvent your network firewall—a host-based firewall will add a layer of protection to the data on your computer."


AVG SMB group at:
bit.ly/avglinkedin


Become an AVG Fan at:
facebook.com/avgfree


Read our blogs at:
blogs.avg.com


Follow us at:
twitter.com/
officialAVGnews


Become an AVG
affiliate at:
avg.com/affiliate

Watch our Channel at:
youtube.com/officialAVG

AVG Technologies CZ, s.r.o.
Lidická 31, 602 00 Brno
Czech Republic
www.avg.cz

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
USA
www.avg.com

AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
United Kingdom
www.avg.co.uk

AVG Technologies GER GmbH
Bernhard-Wicki-Str. 7
80636 München
Deutschland
www.avg.de

AVG Technologies CY Ltd.
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosia, Cyprus
Fax: +357 224 100 33
www.avg.com