



TECHNOLOGY INSIGHTS

These are our own opinions.

We have no commercial
arrangements with vendors.

For more reviews, please
contact TECHNOLEDGE.

T +61 2 9909 0246
E info@technoledge.com.au
W www.technoledge.com.au

Driver Training

A survival guide for the internet highway

PART 2 - SCAMS AND SPAMS

Common Scams

Let one simple rule be your guiding light: **If it sounds too good to be true, it usually is.**

When you come across sites that say you can make money while you sleep, or make thousands of dollars a week for a few hours' work, don't stop to have a closer look. If you get a mail that says you've won a trip around the Caribbean or a prize in a Spanish Lottery, ask yourself if you bought a ticket for either before you jump up with joy. It's hard enough to win the lottery, but it's impossible without a ticket.

Here are a few simple rules:

1. When you get emails from people you don't know offering you wonderful things for next to nothing, delete them. Never open the attachments, no matter what they promise, and don't follow any of the web links in the email.
2. If you see a hot deal that looks legitimate, **be sceptical**. Do a Google search on it to see what others say. That's the beauty of the Web: you're not alone.
3. Whatever you do, don't give your bank account number, credit card details, passwords, pin numbers, or any other personal information to people you don't know.
4. Make sure that the phishing filter on your browser is enabled, the firewall is turned on and your antivirus software is up-to-date.

For an overview of the latest scams, please check **The Security Landscape**.

A detailed rundown on the most common scams in circulation is provided here: <http://www.bankrate.com/brm/news/advice/20021025b.asp>

Spam – More than a Nuisance

Much of it is harmless adware but some spam carries a dirty payload. There are plenty of spam blockers to choose from but it's better to avoid the stuff in the first place. With some basic **Spam Evasion Tactics**, you can keep most of it away.

1. Don't give your email address to all and sundry on the web. Many sites offer useful content but some will only part with it after you give your contact details, and soon you'll find more mail in your inbox. You can unsubscribe from most sites, but it's best to ask yourself if you really need that info before you sign on.
2. Often you'll get mail from associated sites as well because you've missed the little box (already ticked) that says: 'Yes, I want to be contacted by select third parties concerning products I might be interested in.'
3. Set up a **separate email address** for subscribing to newsletters or posting on forums and other public places. You can set up a Hotmail or Google mail account or an additional mailbox with your ISP. Once the spammers latch onto that address, you can simply set up a new one.
4. The more complex you make your e-mail address, the less spam it will attract. That's because the bots trying to harvest email addresses throw mostly simple word and letter combinations at the Web when they're trawling for addresses.
5. Never respond to spam. Your reply only serves to inform the spammers that that they've hit a genuine target.
6. Use passwords that are hard to crack. Here are some guidelines: <http://articles.techrepublic.com.com/5102-1035-1047939.html>

And here's a simple, free utility that stores your passwords and fills them in for you when you complete forms online - <http://www.roboform.com/>

Dealing with Spam

If you're overwhelmed by spam, it might be time to change your email address. That's a pain since you have to inform all your important contacts, but you only need to endure it once or twice. Spam is a pain every day, and even the best spam filters only get it right 95% to 99% of the time (the high rate is for enterprise-class filters that cost thousands of dollars). You can always check the spam folder if you're worried about missing an important email, but you'll soon wonder why you bothered with a spam filter.

The good news is that they're getting more accurate. Still, they slow down your email traffic in proportion to the amount of spam they have to filter, so it still pays to reduce spam in the first place.

Tools for Dealing with Spam

One of the best spam filters is **Cloudmark** - <http://www.cloudmark.com/homeoffice/>
It only works with **Outlook**, but **Thunderbird** comes with its own Bayesian filter, the kind that learns on the job. Bayesian filters can make a poor impression at first but tend to improve as they learn the ropes..

Mailwasher is a free spam filter available here <http://www.mailwasher.net/>
SpamBayes is another popular free choice - <http://spambayes.sourceforge.net/>

If your business makes you an obvious target for spammers, you may want to read this piece, which describes how to use Gmail as a primary spam filter and another product as a secondary:
http://www.techsupportalert.com/how_to_reduce_spam.htm

Both Google's and Yahoo's email services do a fair job of filtering out spam, and they're free services.

Another option is to let your ISP filter your email for a small fee. For a somewhat bigger fee, security services like **MessageLabs** will scan your company's email for malware and spam before delivering it to your network. **MessageLabs** also offers a number of useful resources for SMBs here:
<http://www.webbuyersguide.com/landingzone/messagelabs/>

There is a catch: you have to register before you can download these documents.

[PART 1 - STAYING OUT OF TROUBLE](#)

[PART 3 - AFTER AN ACCIDENT](#)