

The Academy of Plumbing 25 MacHygiene

What? You think you have a virus and haven't been anywhere near a schoolchild or hospital? With the Mac marketshare and online crime in general growing inexorably it's time to exercise a bit more hygiene than we're perhaps accustomed to.

There are millions of viruses, worms, Trojans and other malware in circulation on the Internet, almost all of which target Windows PCs and are entirely ineffective on a Mac. Those that can sting you can be divided into around five types:

- Microsoft Office Macro viruses
- Malicious JavaScripts
- Phishing emails
- Spoofed domains
- Trojan Horses

Come on, I can see your eyelids drooping already. What on Earth am I on about? I'll explain.

MICROSOFT OFFICE MACRO VIRUSES

A 'macro' is a set of instructions that tell a program to automatically perform a certain sequence of operations. Photoshop Actions are macros. Microsoft Office has very powerful macros, and so of course various toerags have gone and written malicious Office macros that attempt to go behind your back in order to wipe your hard disk, throw away your documents, auction your granny on eBay, etc. Defence against them is simple. By default, on a Mac, Microsoft Office has macros disabled. You'll be warned if you try to open a document containing macros and asked if you want to enable them. Just Say No, and then go ahead and open it anyway. It's very rare to come across a document that actually requires macros

enabled to be of any use, and opening it with macros disabled allows you to check whether or not it's pukka. If it's dodgy, delete it.

The real problem with Office Macro Viruses is that although they're unlikely to do much real damage, if you run a viral macro you'll probably find that any new Office document you create will be infected. This document will then bounce back at you when you try to send it by email to someone who uses virus filtering on their email server. Clean up infected files with Norton Antivirus (<http://tinyurl.com/5tbfzz>), and then when you've done that, turn it off.

MALICIOUS JAVASCRIPTS

These originate from nefarious websites and also from legitimate websites that have been nefariously hacked. There are lots about. They'll try to do all sorts of things, most of which involve redirecting you to spoofed domains (see below) or downloading and installing useless Windows malware. To protect yourself, browse with Safari, which is highly resistant to most of this rubbish, or Firefox equipped with NoScript (<http://noscript.net/>). Ditch Internet Explorer.

PHISHING EMAILS

"Warning!! Your account has been suspended because of false login attempt from IP address 87.269.13.67!! Please to click on the below link to reactivate your account!" – it says here, in this email purporting to be from the Abbey National. As it happens, I don't have an account with the Abbey National. This is an attempt to get you to go to a spoofed Abbey National (or insert other bank name here) website and enter a whole load of personal information into a web form, so that it can be sold on for all kinds of purposes. Two things to

remember here:

- 1) Even in this day and age, bank employees generally have a better grasp of grammar than the average composer of phishing emails
- 2) Banks, other financial institutions and most large organizations never send these kinds of warnings by email, for precisely this reason.

If you think your bank account details might have been compromised, ignore email and *phone your bank*. Telephones are still useful in the 21st Century.

SPOOFED DOMAINS

These are website addresses that are either plausible variants of proper domains (e.g. abbeynationalsecurity.com, nothing to do with abbeynational.com) or hidden misspellings of legitimate domain names, created by using international letters that appear to be English letters in your browser's address field. None of them are things you'd be likely to type yourself; they'll all be accessed as a result of clicking on a link. Some are extremely convincing. Your best defence here, apart from not clicking on that link in the first place, is to use OpenDNS.com for your DNS, because their DNS servers automatically protect you against spoofed domains. Don't know what that lot meant? Don't worry: go to <https://www.opendns.com/start> and follow the extremely simple instructions. If you also set up your router to use their servers you protect all of your computers at once. Job Done.

TROJAN HORSES

Those of you of a classical bent will know that a Trojan Horse is something nasty pretending to be something benign, a.k.a. a wolf in sheep's clothing. It appears to be

The Digital Plumber

By Paul Ellis

a very attractive thing and attempts to con you into running it, so that it can go about its real work. So, that pre-release copy of 64-bit Photoshop CS4 you've just downloaded from LimeWire is likely not to be the real thing, but a Trojan. The only real defence here is common sense: if it looks too good to be true, it probably is.

THE REST: YOUR MAC

You can make your Mac much more secure in general by doing the following:

- Set up the Security System Preference as illustrated



- Set up the Firewall section of the Security Preference as illustrated, then allow or deny incoming network access to applications as requested



- Use the excellent Little Snitch (<http://tinyurl.com/6mwf7>) to control which processes running on your Mac are allowed access to the outside world
- Assign a firmware password. Boot from the Installer DVD that came with your Mac, or a Tiger or Leopard Installer DVD, and then click past the first Installer screen until you see a menu bar. From the Utilities menu select Firmware Password... and follow the instructions.
- Don't run as an Admin user. Go to the Users System Preferences and add a user. Call it whatever you like. Check the box that says "allow user to administer this computer". Log out, log back in as the user you've just created, then go to the Users System Preference again, select your usual account (most probably named after you) and uncheck that "allow user to administer this computer" box. Log out again, and back in as you. Now, whenever you need to authenticate to install software, change preferences or whatever, you'll have to enter the username and password of the admin user you created. This is a solid line of defence against anything trying to subvert your Mac behind your back.
- Also, while we're at it, enable Leopard's Guest user but don't allow it to connect to shared folders. That way, if your computer gets stolen, the thieving toerag will be able to log in, allowing the wonderful Undercover (www.orbicule.be) to go about its work.
- Whatever you do, use a strong password. As I said last month, a short word plus a car registration number is easy to remember, and secure enough in computing terms.

- Get into the habit of shutting down your laptop when traveling, rather than just putting it to sleep.

EMAIL AND THE INTERNET

- Use OpenDNS (<https://www.opendns.com/start>).
- If you're going to do some dirty browsing or deep research, consider using Firefox equipped with NoScript (<http://noscript.net/>).
- Use an email provider that runs a virus scanner and spam filter on their mail server. Hotmail, Gmail and Yahoo Mail all do; so do Ultrasign.com (my provider for years now) and Simply Mail Solutions (www.simplymailsolutions.com/). If your current email provider doesn't run antivirus, move to one that does. This is the single most effective way to keep your Mac clean.

If you do all of the above you'll have no need to run irritating, CPU-grabbing, expensive anti-virus software.

Next month: MacBook Pros are surprisingly fast, powerful computers hobbled by relatively slow hard drives. Add a few choice peripherals to create a lean, mean location machine that gives a Mac Pro a run for its money.

Those of you still hungry for information can keep up by periodically checking my blog at www.thedigitalplumber.co.uk, where you'll also find my contact details. © Paul David Ellis, 2008. All Rights Reserved.

