

Network Box: a guide to secure blogging

Technorati now tracks more than 112 million blogs and more than 250 million pieces of social media. More than 175,000 new blogs are created every day. Of these, 58 per cent are corporate or professional blogs, with the vast majority being both personal and professional – ie written by a personality within a company. (source: Technorati.com).

Blogs are now a mainstream form of communication for most companies, and are a trusted source of information: Technorati reports that 37 per cent of bloggers have been quoted in traditional media, based on something they've included in a blog post.

And yet, as the numbers grow, so do the potential threats. As blogging pervades our lives, so too do reports of malware delivered via Blogspot, Google's blogging platform, or malicious code embedded in Wordpress, for example.

So what are the pitfalls for bloggers? And how can they be avoided? Most bloggers won't be expert in Internet security (though they're likely to be aware of security issues). This short guide from Network Box aims to help business bloggers avoid common mistakes that can cost them the security of their blog; and take some important steps to ensure their security.

What are the threats bloggers face?

Blogging software is still relatively young. It is designed to be simple to use and so it is not surprising that there are still many problems such as SQL injection vulnerabilities which let them become infected.

The most common issues faced by bloggers are:

1. Comment spam. This is where a spammer posts content advertising a product (typically health or finance products), with a link to a website that may contain malicious code. Increased exposure also helps these spammers increase their search rankings for a short time. Some research claims that as many as two in three comments left on blogs are spam (blogsecurity.net puts the figure at as high as 93 per cent – www.blogsecurity.net).
2. SQL injection attacks. This exploits a vulnerability in the blogging platform that lets a hacker 'inject' malicious code into the blog itself, that can be used to put malware onto a reader's computer; or to spam subscribers with a product website. Both Blogger and Wordpress have been vulnerable to SQL injection attacks, and don't provide enough care when validating SQL queries.

At best, the effect is to damage the reputation of the blog (and the blogger) and to have your blog closed down; at worst, you could be responsible for infecting the computers of loyal subscribers. The impact on a company's reputation can be extremely negative.

A blog takes a lot of work to keep up – coming up with new and engaging content, writing regularly, creating dialogue with other bloggers and link-backs to attract readers – and now it is important that bloggers put some of this effort into making sure their blog is not open to attack.

How easy is it for a hacker to use a blog for their own purposes?

As blogging is a relatively new phenomenon, we tend to be naïve in the way we behave with them. Although most people who use the Internet regularly are aware of basic security issues, with new communication tools – such as social networks and blogs – people are surprisingly lax with security. (*For information on how to avoid compromising your personal security on social networks such as Facebook, see our Facebook guide for companies: <http://www.network-box.co.uk/whitepapers>*).

Organisations like Technorati are doing a huge amount to encourage bloggers to take steps such as updating their blogging software, but it still requires action from the bloggers themselves. Blog security is still, to an extent, uncharted water – and hackers are taking advantage of this.

Hackers are using variations of the same basic techniques as they've been doing for years with spam and phishing campaigns. But the motivation is more sophisticated. Comment spam can hike a spammer's website up the search rankings, until the search engines cotton on and ban the site (and your blog, for promoting it). So even without people clicking on the link within the comment spam, there is a value to the spammer.

User trust is a key ingredient, too. Blog readers are more likely to trust something they read in a blog they subscribe to, and this applies to clicking on unknown links. Most of us are pretty used to sharing links to unknown sites – YouTube videos, or photo albums shared between friends, for example – and this can lead to complacency that hackers exploit.

What are the solutions?

I'm a blog user – what should I do?

From the blog user's perspective, the usual rules apply: never click on a link in a blog if you don't know or trust its source (in the same way you wouldn't in an email); make sure your security is up to date (network protection should prevent company employees clicking on a blacklisted link but there is no alternative to keeping your system's software up to date); and always keep your wits about you – common sense is often the best protector.

I'm a blogger, what should I do?

If you are a blogger and you want to keep your blog safe from being hacked, there are a number of technical solutions springing up to help bloggers protect their blogs.

Use Captcha (www.captcha.net). It is a free and commonly-used tool that checks the person posting comment is human, thus blocking automated comment spam. It is a simple, but reasonably effective tool and is a good starting point for blog security.

Also worth checking is Aksimet (www.akismet.com) – a free web-based tool that personal bloggers can use free, to protect their blogs from comment and trackback spam. It works by submitting all blog comments to a central service that analyses the comment and blocks or allows it as appropriate.

Another interesting service is Spambam:

<http://www.thespanner.co.uk/2007/02/12/spambam/> a Wordpress plug-in that blocks comment spam and is free to users.

But there are some other practical steps you can take before you start using these services. The list below is a good checklist for bloggers:

- Make sure your blog password is hard to guess. Don't use your company name, for example. Password strength is absolutely crucial. Use numbers, upper and lower case and where possible punctuation. Make sure your password is 16 characters or longer. Change your password periodically.
- Restrict access to the admin account to your IP if you are a single-user blog. If you have multiple users, try to restrict remote access. Changing the name of the administrator account makes life a bit more difficult for the hacker.
- Use Captcha before allowing a comment post (see above).
- Use some form of anti-spam software on the site. Your blogging platform may offer this. Make sure your 'comment' settings don't allow comment without authentication or moderation.
- Consider user authentication before you allow a reader to post a comment – registering on your blog, for example.
- If you are setting up a database of users for the blog, make sure you set the right permission levels. Make sure access to files and directories are restricted to authorised users only. Your blogging application installation guide should lead you through this but be sure to pay attention to these details.
- Make sure the admin account is the only account able to control the more powerful functions of the blog settings, such as enabling and disabling plugins, importing and uploading files.
- Ensure your day-to-day account has the minimum access possible to changing blog settings – the less they can do, the less damage is likely to be done! All new users should have the absolute minimum you can get away with. Usually, blogging software will provide different account levels. Use them!
- To reduce your blog's vulnerability to SQL injection attacks, don't use default prefixes for names when you set up tables in a database (Wordpress, for example, uses a default setting to prefix user names with 'wp', which makes it easy for hackers to guess). Change the default names to make it harder for hackers to guess.
- Only log in to your blog over a secure link like https, not http. Use scp rather than ftp if uploading files.
- Once you have your blog working, disable any error messages. This will reduce the amount of information hackers can glean about your blogging software.
- Importantly, ensure your blogging software is up to date and that you're using the latest version.
- Check your blog at the weekend. The most common time for a hacker to infect a blog is over a weekend, when the effects won't be seen until the following Monday. This gives the maximum 'window of exposure' to the hacker.
- Protect your blog with a firewall, ensuring that only the ports required are open to the public (usually you will only need tcp port 80 for http and 443 for https).

- Finally, don't forget to backup your blog regularly. It would be shame to do all this work, and for a server failure to mean you had to do it all again.

Written by Simon Heron, Internet Security Analyst, Network Box (www.network-box.co.uk).

Network Box Limited (NBL) is an international managed security services company, specialising in unified threat management (UTM). It continuously defends the networks of its customers using PUSH technology to instantaneously update protection, from 12 Security Operations Centres spread around the globe. NBL's customers in Asia, Australia, North America and Europe include companies such as BMW, Nintendo and Toyota, as well as banks, utilities companies and government organisations.

For more information, see www.network-box.co.uk / www.network-box.com.