

Network Box white paper: Securing social media series

Part 3: Guide to secure use of Twitter

It seems you can't open a newspaper or look at a news site without seeing Twitter all over the headlines. From Barack Obama's use of Twitter during his election campaign, or reports that the primary school curriculum will include teaching children about Twitter, to growing concerns about identity theft on the site, it is clear that the micro-blogging platform is in a phase of enormous growth.

Opinion varies as to whether Twitter and other micro-blogs are here to stay, or just a phase in our obsession with social and online media and communication. Whichever camp you fall into, the fact remains that use of Twitter is currently growing at breakneck speeds. Nielsen Online reports that the number of people using Twitter grew by 1,689 per cent between 2008 and 2009; with around 1.8 million people using the site by February 2009.

Is there a business case for using Twitter?

A clear business use for Twitter is emerging. Increasingly, it is being used as a communications tool between companies and their customers, to address customer service issues, market new services, share information, or monitor and research what's being said about a company online.

What are the risks of using Twitter?

Twitter is a classic case of a tool that was built with users in mind, but not security. As a result, there have been a number of reported security flaws to date on Twitter. The main ones seem to focus on spamming: either flooding the system with spam by creating false user accounts or by hacking into existing user accounts (or mimicking the 'from' address of a Twitter account) and creating false spam posts. There were a number of significant breaches last year, including a scam where hackers created an auto-follow tool that exposed victims to links containing malware; and a series of attacks on high-profile Twitter users' accounts including Barack Obama and Britney Spears, when hackers accessed administrative tools used by Twitter to edit log-in details (*source: <http://news.bbc.co.uk/1/hi/technology/7813558.stm>*). There have also been a number of 'Twitter-jacking' cases: people creating false accounts, posing as a celebrity or company.

These cases have obvious risks of reputational damage, and as Twitter integrates further into other social networks (Friendfeed, Facebook etc) there is a greater risk that these spam messages will travel further afield.

But as with any early-stage technology, there is the potential for more malicious damage to be done.

The main risk is similar to that of social networks such as Facebook: trusting networks of people who are unknown to us in 'real' life. Twitter is often used to share information and links – mostly shortened using tools such as bit.ly or tinyurl, which disguises their true address. This could be exploited to link to a website containing malware, and as with any media, a user should not click on a link unless they trust the source.

There are also an increasing number of Twitter applications that have taken Twitter and adapted it for different media (iTweet, Twitterberry etc); or increased the usability of Twitter (Tweetdeck, Twirl, Twitterlicious etc); or provide followers or analysis (Mr Tweet, Twittersion, Twitterbuzz and so on). Many of these will ask for your Twitter password, given on trust and in turn increasing the users exposure to potential security vulnerabilities.

Company response: creating a user policy

Much of the security on Twitter comes down to applying the same principles as in other media: create and apply a clear user policy; educate employees to use with caution; and keep tight controls on and update your existing security systems to reflect new kinds of use.

It is our recommendation that companies should explicitly reference Twitter and microblogs in their Internet and social media user policies. These should include:

1. **User access:** Agree whether your company policy is to allow access to Twitter. As mentioned above, there is a clear business case for using Twitter; be realistic about whether users should be using it. It may be that don't feel comfortable allowing blanket access to Twitter to all employees, so you could consider granting different access rights to different groups. For example, it may be important for customer-facing or product development staff to use Twitter to communicate with customers or test groups. If you do allow universal access, consider recommending Twitter tools that should and shouldn't be used; and stay up to date with development and use of those tools. Review this policy regularly – this is a fast-changing world.
2. **Productivity:** As with any interactive media tools, keep a close check on productivity. Make clear to employees that wasting company time on personal activity is not acceptable, whether this is spending time on Twitter, Facebook, personal email or the telephone. Give clear guidelines, such as:
 - a. Limiting the amount of time on personal activity.
 - b. Monitoring personal communication – one or two personal contacts a day may be acceptable, whatever the medium, but no more.
 - c. Talk to HR teams and line managers about enforcing these policies, and encourage them to set clear objectives and targets. If targets are met, then productivity is not an issue.
3. **Personal security:** Educate your employees about the risks of giving away personal details on Twitter, as on any other media. Don't give away your Twitter password, or information on Twitter that could expose any of your other personal account passwords. Commonly, these include: date of birth, mother's maiden name, father's first name, pet's name, key home address details and such like.
4. **Downloading malware from unknown sources:** Twitter is often used to share information and web links, photos or video links. Make it clear to employees that they should never click on a link they don't trust, or that is sent by someone they don't know personally. This may sound obvious, but with the rise of the 'social web', it is a point well worth re-iterating. URL-shortening tools as mentioned above can cloak websites that are being used for malware downloads or phishing attempts. Some of these URL shortening tools (tinyurl and bit.ly on Firefox) have a 'preview' function, which allows you to view the URL before you click through – these have been developed as a result of increased security concerns and are worth using.
5. **Associated reputational risks:** As with other social media, make it clear to your employees that they have a contractual duty not to bring their company into disrepute. This includes talking about company business on public conversation networks such as social networks or microblogs.

Educating employees

In our last guide to social networks, we suggested holding an annual seminar to explain to employees what is, and what isn't acceptable at work. We recommend including the use of Twitter within this seminar.

Make sure that your employees have access to your user policy, and are clear about what it means. Don't leave any room for confusion.

Stay up-to-date

Finally: make sure you know what systems your staff need to use to do their jobs. Your security systems should adapt to work for your company, not against it. Make sure your security networks and systems are up to date; if you have any doubts, contact your security provider.

For the latest security information, visit www.network-box.co.uk, or read Simon Heron's blog at <http://blog.network-box.co.uk>.