

Network Box white paper: Securing social media series

Part 5: Guide to secure use of IM (instant messaging)

We are often asked by clients how to block a particular application, most notably one that includes instant messaging (IM), such as Facebook, Skype, MSN etc. But the problem with blocking an application is that it will often find a way through a firewall – either using ‘tunnelling’ software, or by searching through all available ports until it finds one open (a problem that can be solved through security systems such as Network Box). So securing the application, and creating user policies on how and when to use it, may be a more effective solution than simply blocking IM altogether.

How secure is IM?

This really varies by IM provider. A survey by CNET News in June 2008 showed that only half the major IM providers use full encryption: AOL Instant Messenger, Google Talk, IBM's Lotus Sametime, and Skype (http://news.cnet.com/8301-13578_3-9962106-38.html). It is worth noting that MSN offers full encryption since version 8; and Pidgin provides a secure https version of IM. Most IM providers use encryption for log in authentication, but many do not encrypt the messages themselves. The same survey found that Facebook's IM was the least secure platform; it appears not to protect login details or conversations. (It is worth saying that IM applications versions are updated regularly, so IT Managers researching IM use should check the latest specifications of each application provider.)

Privacy is the other consideration. As with any social medium, there are privacy holes in most IM platforms. An IM application's default setting (which can be changed by each user) usually allows the user to be contacted by someone they don't know. This invites spammers to use IM, bringing with them all the associated risk of spam, such as sending links to malware-infected websites.

According to the CNET survey, Microsoft is the only IM provider currently that keeps no connection logs, though Google and Skype state that their logs are deleted after a short time.

Is there a business case of using IM?

Increasingly, we find that there is. Many businesses use IM to communicate with customers, colleagues and clients. Skype in particular is commonly used by businesses, and it has an inbuilt IM system.

What are the risks of using IM?

The most common risk from using IM, is of receiving spam. Because IM doesn't come through the email system, spam IM will not be filtered in the same way that emailed spam would be. Spammers over IM will often send infected web links, so having up-to-date security (anti-virus, firewall etc) in place is crucial. But the most effective way of avoiding downloading malware from a web link is not to click on the link in the first place – so educating employees on the risks of IM, or other peer-to-peer applications, is vital.

Other risks from IM include:

- Malware that can be delivered unintentionally through links, files or applications shared between friends, such as songs, photos, games and so on. This malware can be used to create backdoors – openings in the corporate network – through which hackers can attack
- Eavesdropping (a third party accessing your IM, which could give them access to private information about you or your company)
- ID theft
- Data security leaks (information from the company being sent out through an unmonitored 'line').

Company response: securing IM

The first step for an IT manager is to agree with business managers whether to allow IM use: whether it is important for your business overall, or for groups of employees. If you decide to allow IM access, consider the following:

1. **Agree what IM platform you will use**, and make sure your employees only use that platform. Ban use of all other platforms.
2. **Agree which employees should have access to IM**, and set your access policy accordingly. For example, your customer services team may need to use IM, but not your product development team.
3. **Ensure that the IM service is updated regularly**. Often IM providers will include enhanced security in new versions of the application.
4. **Ensure your security policy is set to secure all outgoing communications**, including IM, as well as incoming communications. If you simply block an application, it will often find a way through a firewall – either using 'tunnelling' software, or by searching through all available ports until it finds one open. It is more effective, therefore, to configure firewalls to block all outbound connections except those to secure proxies, which forces all web access (including IM) through a gateway security system.
5. **Educate all employees on the security risks of IM**, and give them clear guidelines on how to use it (see below for an example of these guidelines). Consider including a section on IM in your company security policy, and if you hold security seminars, include IM within these. IM can seem a much more personal form of contact than email, and so the temptation to click on a link within an IM can be greater than within an email. Don't assume that employees understand the risks.
6. **Keep your security systems up to date**, to protect against employees clicking on infected web links, for example. Ensure you are using a secure, recently patched browser, ensure your firewall and anti-virus systems are up to date and correctly configured, and keep your operating system patched to ensure you're operating the latest version. If you have any doubts, talk to your security provider about configuring security to cope with IM.
7. **Monitor IM use**. We're not suggesting that you read every IM sent by your employees, but it is important to ensure employees understand that this is a company system, in the same way that the telephone or email systems belong to the company. IM shouldn't be abused by employees any more than email or telephone should be. Set clear guidelines as to what IM use is acceptable; and write this into your usage guidelines, alongside your email / telephone / Internet policies. Chatting over IM can be time-wasting for employees – monitor productivity.
8. **Ensure employees understand that they are representing the company**, whether it is over IM or any other platform.

Educating employees

In our previous guides to securing social media, 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 IM within this seminar, alongside other social applications (such as Twitter, social networks and so on).

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.

Explain the following guidelines for secure IM use to all employees who use IM:

1. Never accept a contact from someone you don't know. The chances are they'll be a spammer, with an agenda other than being friendly.
2. Set your privacy setting so you can choose who adds you to their contacts list, and block other users than those you specify as contacts. Note: the default setting of your IM provider is probably low security. Don't accept the default setting.
3. Create a screen name – don't use your email address as your IM name; you're inviting spammers.
4. Don't share files, even if you think you know where they're from. Don't click on links, or open a document, or watch a video sent via IM.
5. Set a strong password, and change it often. Don't use personal details as your password.
6. Don't give out personal details or confidential company information on IM. Assume that your IM can be seen and is not secure.
7. Update your IM software when prompted. Updates often include security upgrades.
8. Don't use computers that you don't trust; applications like Apeve Pro are designed to steal your username and password without your knowledge.
9. When using a public computer, ensure that you disable any features that retain login information to prevent other users from gaining access to your instant messaging once you leave.
10. Protect personal and confidential information when using IM. Revealing confidential or personal information in these types of conversations can make you an easy target for Internet predators.
11. Don't download third party plugins from unverified sources – don't click on a link claiming to take you to the source, go to it by typing the link into a browser.
12. Remember that all conversations you have about company business, over any medium, mean you are representing the company. Ensure that you are as professional over IM as you would be over any other platform.
13. Never use the 'remember my password' feature.
14. Don't forget to log out, completely (don't just click 'close', as this will leave the application running). Staying logged in to IM leaves a connection open for hackers to exploit.

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