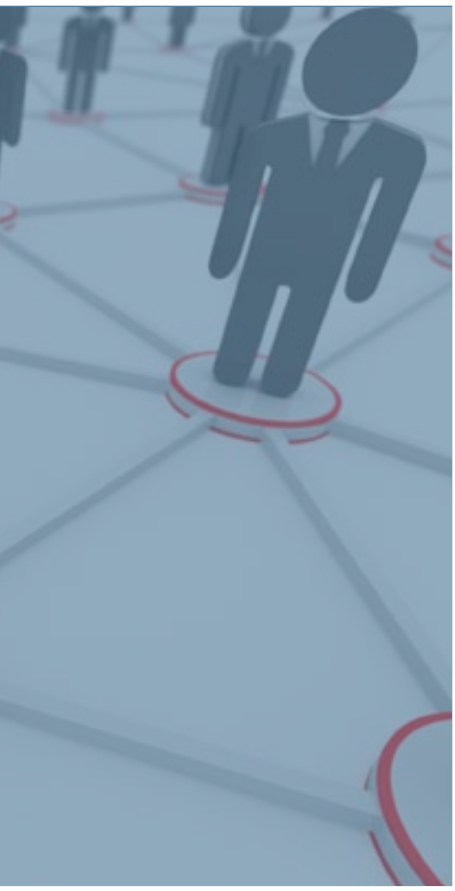
IT Manager's Guide to Social Networking



an internet.com® IT Management eBook

Contents…

This content was adapted from Internet.com's InternetNews, Datamation, and eSecurity Planet Web sites. Contributors: Alex Goldman, Sean Gallagher, Kenneth Van Wyk, David Strom, and Ed Sutherland.

Businesses Lack Social Media Policies

By Alex Goldman

More than one in three businesses have no policies concerning the use of social media sites such as Facebook and Twitter in the workplace, according to a new survey from advertising firm Russell Herder and law firm Ethos Business Law.

The survey, "Social Media: Embracing the Opportunities, Averting the Risks," was compiled from interviews of 438 executives across the United States who were interviewed during July 2009.

Executives are aware of social media and are clearly concerned about the risks it poses, but many have chosen not to create written policies to govern the use of social media in the workplace, according to the report.

"Rather than bypass the social media opportunity, organizations should embrace it while taking steps to educate their team about internal guidelines and best practices," said Carol Russell, CEO and co-founder of Russell Herder, in a statement.

Eighty-one percent of those interviewed said social media is a corporate security risk, 51 percent added that it could reduce productivity and 49 percent feared it could harm a company's reputation.

However, 81 percent also said that social media can be positive for business by enhancing relationships with customers and clients and by building a company's brand reputation.

Seventy-three percent of those surveyed said they plan to increase their use of social media. Most are already using it; 80 percent use Facebook, 66 percent use Twitter, 55 percent use YouTube, 49 percent use LinkedIn, and 43 percent use blogs.

Among the less popular social media sites were MySpace (eight percent), Delicious (seven percent), Digg (three percent), and Second Life (one percent).

So why do so few companies have company policies in place? Twenty-five percent of those who have no such policies said they weren't sure what to put in them, 13 percent said that issue has not yet been addressed, and nine percent said it's not important.

"Ignoring the need for responsible guidelines can impede an organization's ability to protect itself, while at the same time hampering efforts to effectively compete in the marketplace," the report said.

Best Practices in Social Media

The report said that every IT organization should have social media policies and that existing IT policies are unlikely to cover the issues that social media raises.

Fundamentally, companies need to decide whether their policy is open to embracing the technology or closed to it, the report said. The policy should apply to everyone in the company, the report said, not just to employees of the marketing department, for example. Other policies on conduct, such as those governing ethics and harassment, must apply in social media as well, the report said.

The policy should address managers' fears concerning productivity and security. The social media policy should be very explicit about reinforcing existing policies concerning confidential information, the report said.

In addition, companies will need to decide whether or not employees are allowed to use social media during the work day, and whether they can use such Web services during their personal time, such as during a lunch break.

The report's recommendations are a good place to start, but are not a complete list of what to do. They are "a starting point to develop a strategy and policy around social media that can serve to protect corporate interests, yet allow employees to further an organization's overall social media goals," the report said.

The report added that companies need to implement ongoing training regarding the benefits and challenges that social media brings to the enterprise.

"A well-defined strategy, coupled with clear policies and effective training will place your company in the best position possible to take full advantage of social media's potential," the report concluded. ■

Social Networks a Magnet for Malware

By Sean Gallagher

The "clickjacking" attack on the Twitter social networking service early in 2009 was part of a growing trend of social engineering attacks via social networks, according to experts.

"We've seen a lot of these social networking and peer to peer sites targeted in general for a bunch of different reasons," said Sam Curry, the vice president of product management and strategy for RSA. "It's a law of large numbers in many ways."

Curry calls the attacks through social networking attacks "orthogonal attacks." As users have become aware of phishing attacks and other efforts to get at their personal data, hackers have turned to social networks and "brand attacks," like the CNN.com-spoofing Cease-Fire Trojan to spread malware that goes after the same information once installed on the victim's computer.

In the case of Twitter, the service moved to block clickjack exploits, according to Biz Stone, co-founder of Twitter. He said in an e-mail to InternetNews.com that the company is serious about blocking such attacks.

"We've found that proactive security reviews, quick reaction time when there is an incident, and communication with our users in a timely manner are effective techniques in dealing with exploits," he wrote.

While the Twitter clickjack only spread itself and had no apparent malware associated with it, social engineering attacks on other social networking sites have hardly been so benign.

Scareware links on Digg.com and the Koobface virus spreading across Facebook are both examples of social-engineering based attacks that are tailored to the habits of social networking users, with a much more significant security threat attached.

Because of the nature of social networks, they're particularly attractive to hackers, according to Craig Schmugar, a threat researcher for McAfee. "The nature of user interaction within social networking sites is being exploited by malware authors and distributors, and that's definitely on the rise," said Schmugar.

"Unfortunately, a lot of it is just straight social engineering," he said. "They're not exploiting any security vulnerabilities, but they are crafting messages like 'don't click me' to capture users' attention and take them to completely different sites."

That sort of attack puts social networking sites in a difficult situation, he says. "Even if you test as much as you practically can to validate user input, you've got millions of users out there, a small subset of which are trying to poke holes in the application, but it still is a lot of people, and you can't assume your QA is 100 percent. So if you at least on the back end do some additional scanning you have a better chance of catching it."

While social networking services are being more proactive about scanning downstream sites, that can be a fairly expensive undertaking in terms of resources, "especially when you're talking about Facebook which has millions of posts a minute, and Twitter, in trying to isolate the ones you really have to be worried about and keeping the rest of the traffic going," said Schmugar.

While the risk of malware is certainly growing on social networking sites, Curry thinks that the risk is tied directly to the benefit the sites offer. "The risk is greater (in social networks)," he said. "But why do people do this? They want a richer social life, they want to interact with more people, have more engaging types of interacts with people, and want to push out the cultural and social boundaries of their lives, and that creates more risk.

"The question is, is that necessarily a bad thing? Most of us want to hire the people who are interactive in those ways. The value of people who use these is probably far greater to an employer than people who don't do that sort of thing."

How to Use Facebook Safely

By Kenneth Van Wyk

Love them or hate them; social networking sites are here to stay. And your users are going to find ways to use them from home, from work, from smart phones, from shared computers, or from anywhere else they care to.

The whipped cream is out of the can. Now what can we do about it?

Like so many millions of others, I've found Facebook and Twitter in the last few months, in addition to the more traditional professional networking sites I've used for years, like LinkedIn. But what started as idle curiosity soon grew into addiction.

Yes, my name is Ken and I'm addicted to…

But gosh darn it, they're fun! I've re-connected with many old friends, and I like knowing what they've done with their lives. OK, we're not likely to become best friends again, but I still value that connection we've made again.

So how secure are these sites?

I've experienced several classic Web security issues in each of the sites I frequent, and without a doubt there remain many vulnerabilities to be discovered. But that hasn't stopped me from using them.

Like any decision involving risk, I've studied the issues, minimized my own exposure, and I'm getting on with what I care to do.

Let's start by looking at the issues briefly.

Web Apps

Well, for starters, they are Web applications, and as such they're potentially vulnerable to a plethora of issues, from the OWASP Top-10 and beyond – and yes, there are far more than 10.

And don't think for a moment that all Web application vulnerabilities solely place the application at risk. Many also put the app's users at risk: cross-site scripting (XSS), cross-site request forgery (CSRF), and others can be used to attack the users quite easily.

As a user of a social networking site, you're placing your (and your employer's) data at risk.

Active Content

My long-time readers (hi Mom!) have heard me talk about the dangers of active content many times. JavaScript, Java applets, Flash, ActiveX, and many others are all examples of active content. And guess what? Every popular social networking site in existence – or at least with a significant population of users – absolutely requires active content in order for the site to function.

The bottom line: by allowing active content into your browser, you trust someone else's code to run on your computer safely. Well, what's the big deal? We do that all the time. Well, now the code is dynamic and maintained somewhere else, and you're trusting it every time. Gulp!

Domain of Trust

Some of the HTML, JavaScript, etc., that arrives in your browser comes from (say) Facebook. Fair enough, if you're going to use Facebook, you'll need to trust that content.

But your browser isn't so discerning. Some of the stuff that comes into it while you're on Facebook might be provided by someone else: another Facebook user; an attacker; a third

party application on Facebook. If your browser trusts Facebook, chances are it's also going to trust that code. This extends the active content exposure pretty substantially.

User-Supplied Content

Users put all sorts of content into their own profiles" URLs pointing to cool sites, photos, etc, and if they link to something dangerous—perhaps inadvertently—and you click on it… Well, you get the drift.

Third-Party Applications

Most of the popular social networking sites have a third-party application interface for companies to generate their own content. Most of it is pretty innocuous and in the spirit of good clean fun, like a little app that lets you "throw" a virtual snowball at someone else. But, again, it extends that trust boundary in ways you might not want.

All of these things come with levels of risk. The "double whammy" that I see is the active content combined with the expanded domain of trust. There's a cross-site scripting launch pad in that combination if ever there were one.

When I've written about browser security, I've advocated browser plug-ins like NoScript to give the user a level of control over active content. The problem is that it only provides a partial solution on social networking sites.

For example, if I tell my NoScript to allow scripts to run from Facebook, I'm allowing all Javascript coming at me from facebook.com to run. As I said, that may or may not be actual

Facebook Content

NoScript either trusts a domain or it doesn't. Clearly, it's not granular enough for all issues.

What can we do to protect ourselves? Here are a few tips to consider:

Continue to Run NoScript and Follow Browser Security Steps

They're far from obsolete!

Be a Bit Choosy About Your Friends

Easier said than done, but at a minimum, I suggest only accepting friend connections from people you directly know. Of course, they'll come with varying levels of technology "cluelessness," but it's still not a good idea to be friends with anyone who figures out how to send a request to you.

Be More Than a Bit Choosy About Your Apps

If you have the ability to decide what apps you run and allow within your social network's site, be choosy. Do you really need every cutesy app that comes along?

Wait for a couple days to see what people (and the media) say about an app before deciding to dive in. If the app has problems, often it's the early adopters who will find them.

Turn up the privacy controls: Pretty much all the social networking sites allow you to tune your own privacy controls. Turn those up to "high." Only allow people in your ring of accepted friends to view your information.

Don't Click on Links Willy Nilly

When friends send you links to sites, apps, etc., don't just click on them. Hover your mouse over the link, look at it in its entirety, see what data is going to be passed to it, and then decide. You might even cut-and-paste the URL into another browser and go there separately.

Log Out of Other Apps and Sites

To the extent possible and feasible, don't run other Web apps while you're on your social networking site. Shut down your browser completely, re-start it, do your social networking for the day, and then log out.

That should arm you with a few tips to consider. There's still risk involved with using these sites, and there always will be. You need to decide for yourself if the risks are worth whatever value you perceive in using the sites.

As for me, I sure wouldn't give up my Facebook account without a fight. ■

Top CEOs 'Miserable' At Social Networking

By Ed Sutherland

Only two Fortune 100 CEOs use Twitter and no top business leaders maintain a personal blog, findings that show "a miserable lack of social engagement," according to a new study.

Although 76 percent of corporate heads have a Wikipedia entry, 81 percent of 2009 business chiefs do not have a personal Facebook page, said Sharon

Continued on Page 9

How to Be Safer on Twitter

By Kenneth Van Wyk

"Twitter is insecure. Twitter is the root of all evil."

Right. Much has indeed been written about Twitter's security – or lack thereof– in just the past couple of months. In taking in what others have to say, though, I can't help but think it's being unfairly attacked.

Let's take a fair and objective view of some of the issues, and see what, if anything, a user can do to reduce her risk.

Twitter, the wildly popular micro-blogging Web site, has roared onto the scene in an amazingly short time, even by Internet standards. Twitter users can post short (140-character) messages known as "tweets" to all their followers. Pretty much anyone can follow anyone else's tweets on Twitter, although there are some minimal privacy settings and such for those who want to limit the scope of where their tweets go and who can see them.

It's through this simple matrix of followers and writers that communities of like-minded people have joined one another in reading and posting their tweets.

But several articles and blog entries have been published declaring Twitter to be insecure. A common theme among the naysayers has been Twitter's use of TinyURL, a site/service that encodes long URLs—we've all seen them—to be just a few characters long. No doubt this is used so that people can post tweets with URLs and still fit within the 140-character tweet limit.

The problem with TinyURL and similar encoding mechanisms is that the end user really doesn't know what's in the original URL itself. Thus, a tweet could be pointing the reader to a hostile site containing maliciously formed data that could quite conceivably attack the reader's browser.

All of this is true, of course, but so what? The truth is that any URL we click on or enter into our browsers manually can take us to sites that contain malicious data. Granted, some sites are going to seem more trustworthy than others: a respected news outlet is likely to be more trustworthy than (say) www.click-here-to-infect-your-computer.com—which, by the way, I think is not a registered domain.

Even still, I again ask the question: so what? There is an inherent risk in pointing your browser to any Web site. We've discussed numerous ways of shoring up your browser so that you're less likely to have your system compromised, even if you visit a site containing malicious data. All of these things are entirely relevant in the context of Twitter, of course.

Another common complaint is that there's no verification of a Twitter user's identity, so someone could trivially pose as (say) a celebrity and the public would be none the wiser. This too is quite true, but it's nothing new with Twitter.

Anyone still remember the old "kremvax" April Fools' joke from 1984? Spoofing an identity was as true then as it is now. In the absence of a trustworthy cryptographic signature, digital identity must not be trusted.

Now, to be fair, there have been a few published coding vulnerabilities on Twitter, including some cross-site scripting problems, "clickjacking" problems, etc. But from what I can tell as an outsider (and a Twitter user), the folks at Twitter have fixed these problems on the server as they've been reported. I don't have data on how rapidly they've been fixed, but they do appear to be addressing them.

All of these security and privacy concerns are valid, but they're by no means new or unique to Twitter. No, it seems to me that Twitter is being unfairly attacked for whatever reasons. I've heard many folks complain about Twitter's 140-character tweet limit, saying that nothing of value can be communicated in such a small message, therefore Twitter must be without merit.

I won't get into a debate of whether one can say something valuable on 140 characters or not, but suffice to say that I've seen many 140-character tweets that were of value to me. But let's get past that and consider some positive recommendations on how to safely use twitter, assuming that you also want to hear what some of your colleagues want to say in 140 characters.

- Don't click on encoded URLs if you at all doubt them. If they point to something you feel you do want to read, direct message or e-mail the tweet's author and ask for the full citation, and then decide whether it deserves your trust.
- Harden your browser anyway, just like I've suggested many times.
- Follow people who post things you're genuinely interested in. Follow people you trust. Verify their Twitter identities via a trustworthy channel like, for instance, an encrypted or cryptographically signed e-mail.
- Avoid twits. There is a lot of noise on twitter. Life is too short for that blather. Shut it off.
- If you're concerned about the privacy of what you post, set your own account to "protect my posts," which restricts your tweets to only your followers. Approve (or disapprove) your followers. Block followers you don't know or otherwise don't want reading your tweets.
- Avoid posting URLs, or post really short URLs so that your tweets don't automatically invoke TinyURL. If you want to point to a URL, tell your followers to direct message you to request the full URL.

These, of course, are just some basic precautions you could take if you wanted to use Twitter in a reasonably safe way. Above all, though, treat it for what it is—a means of posting short bursts of information to people. If you want your own tweets to be valuable to others, be concise. Very concise.

Oh, and in case you're interested, my Twitter name is "krvw." ■

Continued from Page 7

Barclay of the Blue Trumpet Group, a public relations firm. Barclay released the study's results on her blog UberCEO.

Only two CEOs -- Warren Buffet and Proctor & Gamble's Alan Lafley -- have Twitter accounts. Although Buffet has 7,441 friends, the Oracle from Omaha has tweeted just once, a Feb. 20 "coming soon" message. Lafley has never updated his 33 followers on P&G, according to Barclay.

Twitter had 19.7 million visitors in May, according to Internet measurement firm Compete. More than 8 in 10 top CEOs are also avoiding Facebook, the social networking giant with more than 200 million users.

The banking sector leads among Facebook corporate users with Bank of America CEO Ken Lewis, Wells Fargo's John G. Stumpf, and Citigroup's Vikram Pandit having the most friends. Exxon's Rex Tillerson is the sole Fortune 100 CEO using Facebook without a single friend, according to the study.

The limited use of social networking by CEOs also extends to LinkedIn, a site that caters to business-to-business interaction.

Just 13 top CEOs are listed on LinkedIn, with only three having more than 10 connections: Michael Dell, Cisco's John Chambers and Gregory Spierkel of Ingram Micro.

The results give the "impression that the 'old boys' network' is clearly the preferred method for Fortune 100 CEOs," Barclay said.

Earlier this year, Gartner published a study on CEO impressions of Web 2.0 services, such as social networks. Just 15 out of 74 CEOs questioned in the study said they had a "fairly good understanding" of Web 2.0 technology, with about 45 of the group responding they had limited understanding or had never heard of the term. ■

Four Useful Tools for Social Networkers

By Kenneth Van Wyk

What do the services Pixelpipe.com, Etherpad.com, Tr.im and namechk.com have in common? All four are tools that I can't live without these days and didn't even know existed a few months ago.

That is how fast the Internet is changing. I suggest you give each of the four a quick try out and see if you agree that you can save yourself a lot of time with each of them.

Pixelpipe is a service much like Ping.fm. It allows you to post the same piece of content to multiple sites. Whether it is a status update (which is just what Ping does), a blog entry, a video, or a series of photos, it is a very useful service and handles more than 80 different sites. Look for a review to come soon in Computerworld next month.

The downside is that you have to store your authentication credentials with the service for each site, which may make you nervous if you care. And if you mess up, your typos will be immediately sent out to the world for many of your correspondents to see, because there is no easy way to recall the messages without visiting each site individually.

I like it mainly because I post my blog entries to multiple platforms, part for redundancy's sake, part because I don't trust Wordpress to be the sole repository of my work product.

Next is Etherpad, a service that allows multiple people to concurrently edit a document using just a Web browser. You create a unique URL and then send that to your collaborators via e-mail. Once someone knows the URL, they can make changes to your document, and each author's changes can be tracked with different colored highlights.

I used this today with a client – even though we were sitting around a conference table in the same room, we were able to agree on the edits of a document within a few minutes, it was incredibly productive.

Tr.im is a URL shortening service with a twist: you can post the shortened link directly to your Twitter account. And while that is convenient, wait there is something that I really like. It will track all the people who have clicked on the shortened link and show you which client (browser, Twitter third party app, or service) was used in the process, along with time-series data on the clicks.

You can really see the immediacy of Twitter, but you can also use it to track referrals on other services too.

Namechk is a very simple service that will lookup a particular username on more than 120 different social networking, blog and video sharing sites. It will see if it is taken or available. This is a very useful tool that you can show your clients how tuned in you are to that scene.

Let me know what you think about each of these services, and if you have others that you have recently found that could be useful. ■