GFI White Paper

Social networking and security risks

By Brad Dinerman

The popularity of social networking sites has increased at astonishing levels. There is no arguing the usefulness of sites such as Facebook, Twitter and LinkedIn. They can be used for professional networking and job searches, as a means to increase sales revenue, as a tool to keep the public informed of safety and other issues or as a way to reconnect with friends from way-back-when.

GFI®

Contents

Introduction

However, as with any new tool or application, it is always important to keep a close watch on its security implications. Each of these tools comes with its own set of security concerns which can put your information systems and/or personal data at risk. This white paper will look at some of these risks and identify possible solutions to help protect you, your personal information and your company data.

Of the three social networking sites mentioned, Facebook is generally considered the most casual; Twitter and LinkedIn are typically used for professional purposes. LinkedIn allows you to add Connections, Twitter creates Followers and Facebook has Friends.

Facebook

Three of the most popular features of Facebook are the ability to add Friends, update your status and run applications such as games and quizzes. A "Friend" is anyone on the Facebook network whom you allow to see various levels of personal information, such as job, birth date, photos, group membership, comments and list of other Friends. You can even play online games and keep others updated on your daily life.

Friends can also see Friends of Friends, meaning individuals, whom you have officially befriended and may never have met, may have visibility into your personal information and whereabouts.

Updates

At the top of the user's Facebook profile is the Update field, which allows the user to post a sentence or paragraph regarding any topic at any time (See Figure 1). LinkedIn has a similar field, but it does not allow as much text, and it's not possible to connect links, photos or videos with the update.

Here are some examples of updates that my Facebook friends have recently posted. These are very typical:

- "Just received a job offer. Hooray!"
- "I'm tired of all the rain."
- "Looking forward to the family vacation next week at Disney World."

Although these might seem relatively harmless, the third bullet point could raise some concern. You have just told all your friends, as well as all their friends, that you will be away from home for a full week. This is comparable to putting a sign on the main road that shouts "Empty House" for passers-by to see. Even if you have a burglar alarm or neighbors keeping an occasional eye on the home, you still don't want to create the temptation for strangers (Friends of Friends) to consider helping themselves to that wonderful, new 52" flat-screen TV you just purchased.

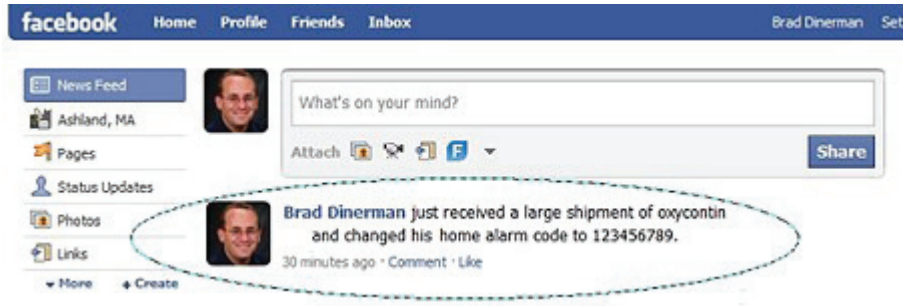

Figure 1: Users must be aware of how the information they post can be used by others. Note: This profile update was exaggerated for effect. The author neither received oxycontin nor set his alarm code to 123456789)

Twenty things you didn't know about me

Not long after I joined Facebook, I received a message from a Facebook Friend who had just created a list called "Twenty Things You Didn't Know About Me." I was then invited to read it, create one for myself and then notify others in turn. The list had questions I needed to answer so that my Friends could learn a little bit more about me.

I had some initial concern as this seemed very much like a chain letter, and I never forward those. Yet, it also seemed harmless enough; I wasn't being asked to send money or forward a false virus alert.

I decided to give this a try and went through the bullet points. Here are some of the items that I was supposed to identify about myself:

- What was my most embarrassing moment?
- Have I ever played hooky?
- What was the name of my first elementary school?
- What was my favorite pet's name?

In ordinary conversation with friends and colleagues, these are questions that we aren't typically afraid to answer. But look more closely at the last two questions, and now think about the way that you may have set up your online bank account, Amazon.com profile or the access to your work's Human Resources system.

When setting up online accounts, in addition to creating a User ID and a password, you often provide answers to a set of "secret questions" that you need to answer if you forget your credentials. If you can answer the questions, you will receive the password (or a new one) and have full access to the system which likely contains very personal and sensitive information. Now consider what "secret questions" are often asked: "What was the name of your first elementary school?" "What was the name of your favorite pet?"

By providing the personal information asked in these Facebook questionnaires, you may unwittingly be providing an easy channel for identity theft. Is it worth compromising your online bank account for the bit of amusement that Facebook provides? Probably not. If you still want to have fun with these questionnaires, then by all means do so. But be very careful about the type of information that you provide and how that information could be used if it fell into the wrong hands.

Applications

Facebook offers thousands of applications that its users can install and run. These applications include calendars that allow Friends to be reminded when it's your birthday, tools to send Friends online greeting cards, quizzes on myriad topics and much more. (See Figure 2.) Many of the applications were designed by Facebook end-users.

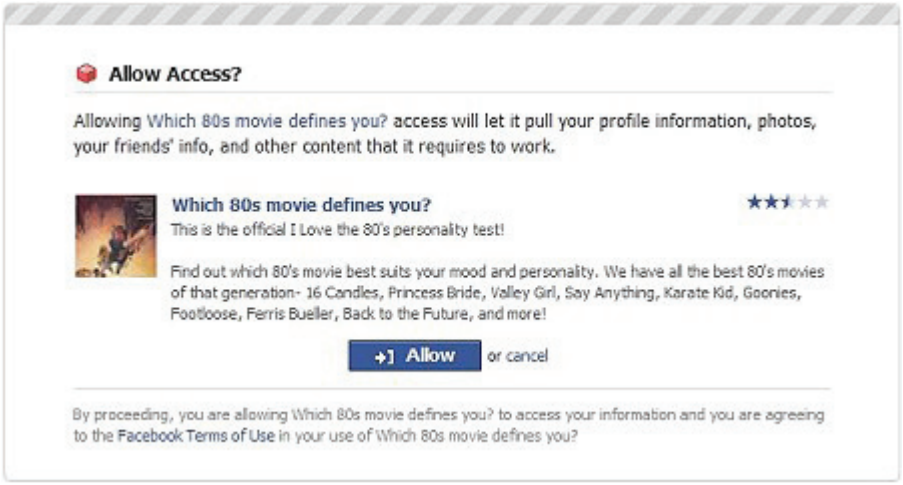

Figure 2: Even though applications provide warning messages, many users still install and run them, unaware of what they may do to your system.

Although the applications on Facebook may look harmless, and in fact most probably are, there are always some that may deliver malicious content to your computer. This holds true not only to Facebook, but also to other social networking sites and to the Internet in general, when downloading from the web or opening attachments in email messages. Therefore, make certain that your computer has a proper and functional firewall, as well as up-to-date antivirus/anti-malware software, and only install or run these applications if they are from a trusted source or approved by your corporate IT department.

Twitter

Twitter is an online application that allows you to post brief comments (tweets) on any topic. Other users on the Twitter network can become followers of your tweets, such that they receive the updates whenever you send them.

Figure 3: Users can post a "tweet" on any topic, as well as receive the tweets of those they are following.

Both Twitter and Facebook users must be very careful about the personal information that they tweet and how it may be used. Employers must be especially attentive to the information that is posted and how it can affect their company. For example:

- "The boss just laid off 32 employees. I hear there may be more coming on Wednesday."
- "Rumor has it that the Acme Widgets acquisition fell through."
- "Working to troubleshoot a major software bug we just found."
- "I just posted a funny video of myself frying a rodent at the restaurant where I work."

Each of the four statements can have serious public relations and financial consequences for the company whose employee tweeted or posted the information. The impact can be even more serious if that company is publicly owned. The first two statements will create a public perception that the company is doing poorly or will continue to experience loss, and shareholders may begin to sell off their stocks, reducing the value of the company. The third statement will raise concern amongst the company's customers who have purchased the software, possibly tempting them to investigate competitors' solutions. And the fourth statement, which actually occurred to a well-known, nationwide fried chicken company in 2008, will certainly give customers second thoughts about going to visit the restaurant, even if the video wasn't real.

Acceptable use policies

Unfortunately, there is no simple solution to manage these issues. Certainly a company can implement technical barriers to prevent any use of Twitter, Facebook or similar applications, but then the company may have lost a valuable sales and marketing tool in its effort to protect its security or privacy.

Alternatively, the company could (and should) have an Acceptable Use Policy, a document that details how these applications and the Internet in general can be used. The policy also defines consequences for failure to comply, which might be as simple as a written reprimand or as heavy as termination of employment and legal action. You can find some excellent Acceptable Use Policy templates at the System Administration, Networking and Security (SANS) Institute, but just know that you will need to customize them to fit your company's culture and HR needs.

Beyond Acceptable Use Policies, however, companies will still have a difficult time restricting what employees do at home. Employees will have their own Twitter and Facebook accounts, set up websites like AcmeWidgetsSux.com and put all levels of derogatory and inflammatory comments, whether true or not, onto those sites. Although the company may have legal recourse when this occurs, the damage may already have been done and the cleanup can be a very expensive and involved undertaking.

Facebook, Twitter and LinkedIn spam hoaxes

Whether you use Facebook, Twitter, LinkedIn or any online site for social networking, online banking or day-to-day purchases, be aware of emails that claim to be from these sites but are actually hoaxes and may contain malicious content. I have received numerous emails that allege to be from my bank, yet are actually sent by a spammer in the hopes of obtaining my online username and password. Similarly, emails claiming to be Twitter and Facebook invitations are now commonplace. (See Figure 4.) The messages may even contain an attached ZIP file that recipients are asked to open to see who invited them. The attachment actually contains a mass-mailing worm, which can cause damage to both your computer and your reputation.

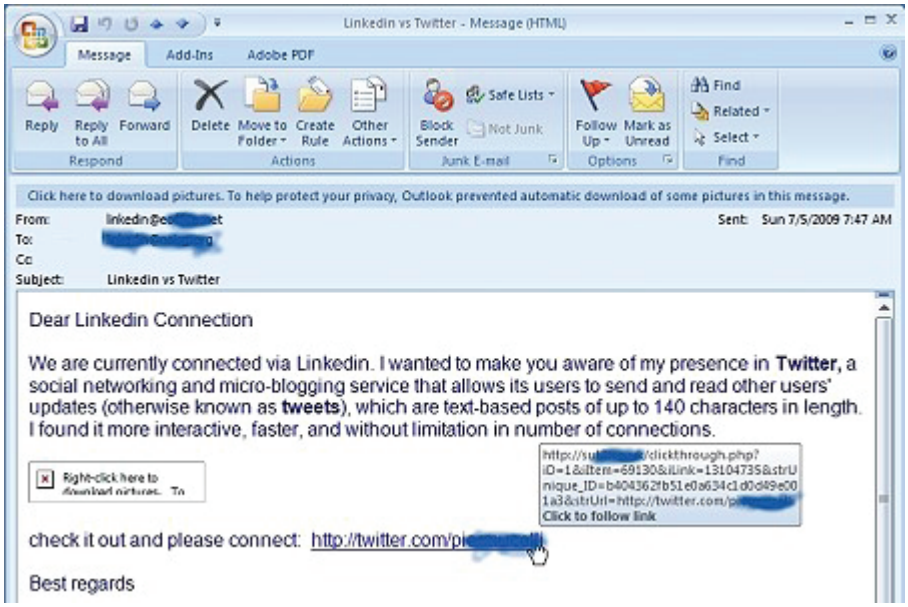

Figure 4: The message claims to be from a LinkedIn connection, inviting the recipient to also connect on Twitter. Yet, the sender and the recipient do not actually know each other, and their respective addresses and names were likely gleaned from a spam database. Hovering the cursor over the link near the bottom of the message reveals the URL to the actual spam site; it also contains information that identifies the individual who received this message.

How is it possible to identify the legitimate messages from the hoaxes?

- Use an up-to-date email client such as Microsoft Outlook 2007, Outlook Express or Mozilla Thunderbird which have spam filtering enabled and checks for "phishing" messages (phishing messages are falsified emails that use these tactics to obtain your username, password or other personal information).
- Never open an attachment unless it's from someone you know, and you are expecting to receive it. If you have any doubt, then contact the individual and ask if he/she actually did send it.
- Use up-to-date antivirus/anti-malware software on your computer to block any harmful files that you may have accidentally opened.
- Always use common sense on the web and in email; take an extra moment or two to think about what you have received or are about to do. For example, would Twitter really email an invitation in a zipped attachment? Not likely.

URL shortening (obfuscation)

Another form of hoax involves the obfuscation, or shortening, of URLs in email messages or on websites such as our favorites: Facebook, LinkedIn and Twitter. The posting of hyperlinks is obviously not specific to these sites, but the frequency with which we let down our guard when using them is a big concern.

Often times, the links that we want to post can get very long, making them unwieldy or impossible to type in the small space allotted by the network sites. To get around this, third-party services such as http://tinyurl.com/ or http://bit.ly/ will "encode" the URL into a much shorter version. For example, the URL of this article, http://www.fieldbrook.net/TechTips/Security/SocialNetworking.asp, has a length of 64 characters but can be shorted by TinyURL to have only 25 characters: http://tinyurl.com/m34rkp. Which URL would you rather type when you have a limit to the number of characters that you can enter?

Although the benefit of URL shortening is obvious, there is also a security risk associated with it, in that the shortened URL really does not tell you the true destination of the link. You only find out once you get there, which may be too late if that site happens to contain drive-by malware or content which should not be viewed by "sensitive" eyes. Therefore, make certain that you click on shortened URLs only if you trust the sender. Never click on them if they are contained in spam messages or on sites that you have any reason to consider suspicious.

Also consider obtaining a third-party browser or mail client add-on that will reveal the URLs' full path so that you know where your browser is actually directing you. Examples of websites or software that will perform this task can be found at http://longurl.org/ and http://www.longurlplease.com/.

Conclusion

Social networking sites can be valuable sales and marketing tools, as well as fun diversions. Inherent in these applications are security risks that can put the individual or a company in a compromising position or at serious risk. Aside from not using these sites at all, end-user education, alongside documented policies and procedures, is the most fundamental protection that exists. A well-informed user will not only help to maintain security, but will also educate others on these issues and establish best practices which can be standardized and updated as applications mature or as new applications come along.

About the author

Brad Dinerman is the president of Fieldbrook Solutions LLC, an IT, MIS and security consulting firm in the Boston, Massachusetts area. He is a Microsoft MVP in Enterprise Security as well as a Microsoft Certified Systems Engineer (MCSE), a Certified SonicWall Security Administrator and a Certified 3Com IP Telephony Expert. He even earned a Ph.D. in physics from Boston College, which he claims was "to calculate how long it would take me to launch my frozen computer over the local highway."

Brad maintains his own TechTips site at http://www.fieldbrook.net/techtips/, which has been used by IT support personnel from organizations including NATO, the US Department of Homeland Security, the Department of Energy, the Department of Justice, the US Geological Survey and the Office of Naval Intelligence.

Brad is the founder and president of the National Information Security Group (NAISG, http://www.naisg.org), a member of the FBI's Infragard Boston Members Alliance and a member of the Microsoft IT Advisory Council.

About GFI

GFI Software provides web and mail security, archiving, backup and fax, networking and security software and hosted IT solutions for small to medium-sized enterprises (SMEs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMEs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at http://www.gfi.com.

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com