fieldbrook solutions LLC

WHITE PAPER

12 Kings Row
Ashland, MA 01721
(508) 231-0931
http://www.fieldbrook.net/

Social Networking and Security Risks

Revision 4 - Draft

by Bradley J. Dinerman
President, Fieldbrook Solutions LLC

July 23, 2014
(Original publication date: July 07, 2009)

[This white paper is provided for informational purposes. No part of it may be reproduced or distributed, in part or in whole, without the express written consent of the author.]

CONTENTS

Introduction

The popularity of social networking sites has increased at astonishing levels. There is no arguing the usefulness of sites such as Facebook, Twitter, LinkedIn and a myriad of others. 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 breaking news or as a way to reconnect with friends from way-back-when.

However, as with any 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.

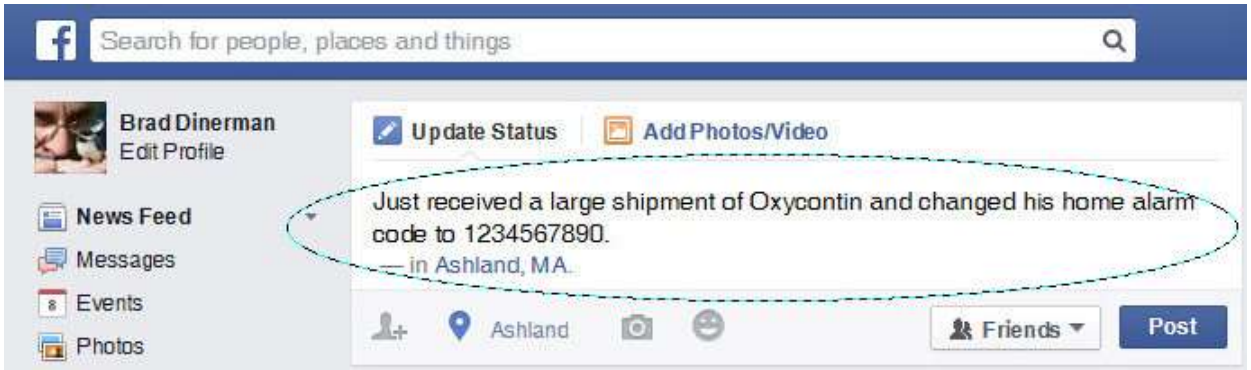
Of the three social networking sites mentioned, Facebook is generally considered the most casual; Twitter and LinkedIn are typically used for professional purposes. Facebook's interactions are through Friends, LinkedIn has Connections and Twitter creates Followers.

Facebook

Some of the most popular features of Facebook are the ability to add Friends, update your status, post photos and run applications such as games, travel planners and news tickers. A "Friend" is anyone on the Facebook network who you allow to see various levels of personal information, such as job, birth date, photos, group membership, comments and lists of other Friends. You can play online games with other users and post updates on your daily life.

Updates and Photos

At the top of the user's Facebook profile or Wall is the Update field, which allows the user to post a sentence or paragraph regarding any topic at any time, as well as post photos and videos. (See Screen Shot 1.)



Just received a large shipment of Oxycontin and changed his home alarm code to 1234567890.
— in Ashland, MA.

Screen Shot 1 – Facebook profile status update.
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 1234567890.)

Here are some examples of updates that are typical of those that my own friends have posted:

1. "Just received a job offer. Hooray!"
2. "I'm tired of all the rain."
3. "Having a great week in Paris with my family."
4. "So excited that Mona can finally babysit for younger sister Lisa. Looks like we'll have Saturday nights out now."

Although these might seem relatively harmless, the third and fourth points should raise some concern. You have just told all your friends, and potentially all their friends and strangers depending on your privacy settings, that you will be away from home for a full week and that you have young children alone at home. This is comparable to putting a sign on the main road that shouts "Empty House" for passers-by to see. Even if you have an 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, or for pedophiles to make phone calls or pay a visit to your children.

To protect your privacy and restrict who can see your updates and different levels of personal information, select the Settings option from the drop-down list at the top-right of your Facebook page (to the right of the Home link). Then,

Select the Privacy Settings options:

1. Under "Who Can See My Stuff," set the default visibility for your posts. [Keep in mind that Facebook remembers your previous visibility setting. So if your most recent post was set to Public, your next post will also be public. You'll need to keep a vigilant eye on this setting as it's very easy to forget to change it on future posts.]

2. Under "Who Can Contact Me," you can control who can contact you or send you Friend requests. For the most part, it's okay to let anyone contact you. Setting this to anything else somewhat defeats the purpose of Facebook. Just be aware that you may not want to respond to requests from complete strangers!

3. Under "Who Can Look Me Up," determine if people can search for you based on phone number or email address. My personal suggestion is NOT to include this information in my personal profile anyway, so I just leave the setting at the default of Everyone. But if you decide to include it in your own profile, then consider restricting this setting to Friends only, or at least Friends of Friends.

Select the Timeline and Tagging option:

1. Under "Who Can Add Things To My Timeline," you can restrict the content that others can post to your timeline by limiting posts to just friends or friends of friends, and by enabling an approve/reject option. Since you don't want people posting sensitive or potentially harmful information about you or your business, this will enable to block the content before it becomes visible.

2. Under "Who Can See Things On My Timeline" is a very underutilized and useful feature. Click the View As link next to "Review What Other People See On Your Timeline" to see how your timeline appears to the general public or even to specific individuals. This will reveal potential mistakes in your settings. For example, you may have forgotten to mark a personal photograph for friends only yet the general public can see it. Once you have this information, you can then correct the settings.

3. Under "How Can I Manage Tags People Add And Tagging Suggestion," you can set options to enable a review of tags that people may add with your name. This is important since you may not want someone to tag you in a public photograph showing you in a private situation (party, bathing suit, etc).

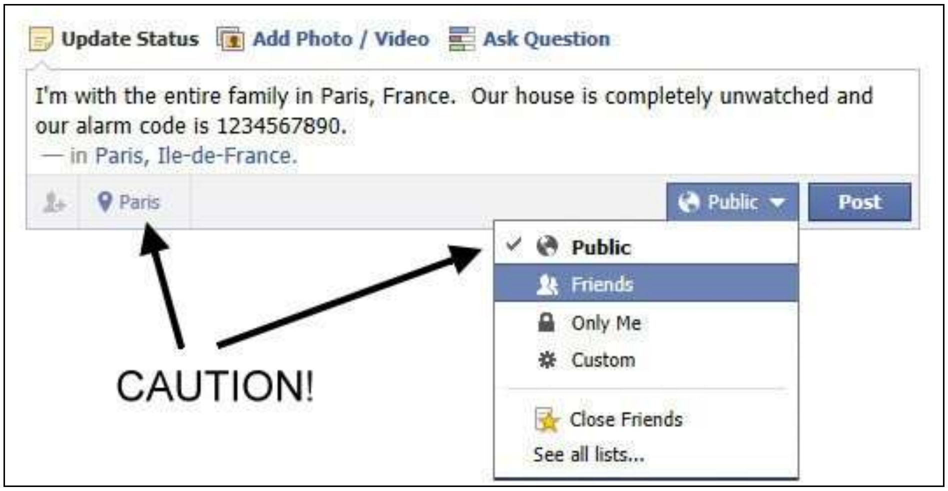
Select the Blocking option.

1. Under "Block App Invites," and "Block Event Invites" you can block individuals from sending you invitations to participate in certain apps, typically games, or from sending you invitations to the events that they may be hosting.

Two other methods to enhance security, both referenced in Screen Shot 2, include:

1. Restrict the audience of your status updates and photos that you publish to only those that need to know. You can do this directly in the update field. Allowing an update to be visible as "Public" means that anyone with a Facebook account can see your post.

2. Do not include your location if it creates a security risk. For example, if your entire family is in Paris, then you might not want that to be known because it sets up your house as a target for burglars.



I'm with the entire family in Paris, France. Our house is completely unwatched and our alarm code is 1234567890.
— in Paris, Ile-de-France.

Screen Shot 2 – Control location awareness and public visibility.

Twenty Things You Don'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 Don't Know About Me." I was 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 items that the list instructions suggested to identify about myself:

1. What was my most embarrassing moment?

2. Have I ever played hooky?

3. What was the name of my elementary school?

4. What was my favorite pet's name?

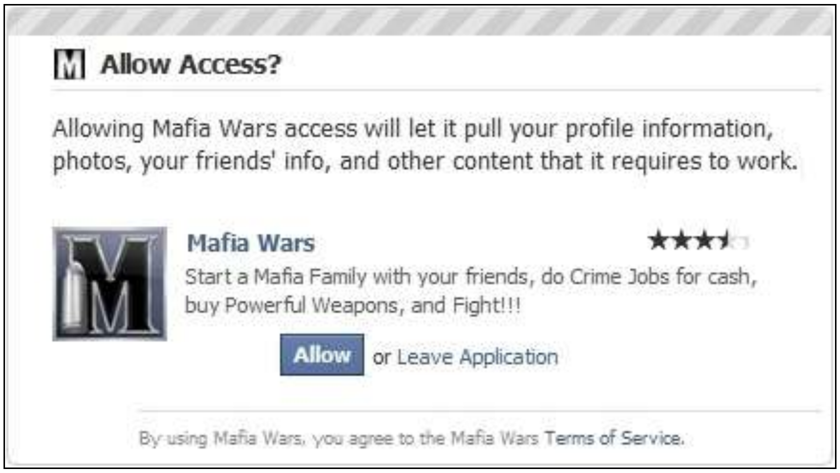
In ordinary conversation with family, friends and colleagues, these are questions that we aren't typically afraid to answer. But look more closely at the last two questions, and now think about the way that you may have set up your online bank account, Amazon.com profile or the access to your work's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

When setting up online accounts, in addition to creating a username 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 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 can be used if it falls 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 Screen Shot 3.)



Allow Access?

Allowing Mafia Wars access will let it pull your profile information, photos, your friends' info, and other content that it requires to work.

Mafia Wars

Start a Mafia Family with your friends, do Crime Jobs for cash, buy Powerful Weapons, and Fight!!!

Allow or Leave Application

By using Mafia Wars, you agree to the Mafia Wars Terms of Service.

Screen Shot 3 – A typical Facebook application.
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/antimalware software, and only install or run these applications if they are from a trusted source or approved by your corporate IT department.

Protect your privacy and computer systems and limit which applications can run. To do so, select the Account Settings option from the drop-down list at the top-right of your Facebook page (next to the Home link), and then select the Privacy Settings option. Once there, select "Apps, Games and Websites" to control which aspects of your personal information can be made available to others through apps and games that you use.

So What Else Can You Do To Protect Yourself?

In addition to the steps described in the previous sections, here are four additional ones that you can take to enhance your security:

1. Be attentive to personal information or posts that are visible to "Friends of Friends." Although you may trust your real friends and family, you cannot know all of the individuals who they in turn have friended. These can number in the thousands. Referring to the example of posting that you are on vacation and your house is empty (Screen Shot 2), consider the hundreds/thousands of strangers that now know this fact because you set the update visibility to "Friends of Friends."

2. Check both your system settings and your Facebook App settings on handheld devices such as Apple iPhones/iPads. These devices are location-aware and may automatically advertise your location through these Apps if you have not specifically disabled the feature.

3. Logon as a different user and view your profile. Despite your best efforts to keep your postings limited to your desired audience, you may still have missed some settings since there are so many and not all options are intuitive. Fortunately, Facebook provides a means to see how your profile and timeline will appear to other individuals. Under Timeline and Tagging Options in the Privacy settings (see earlier section), go into "Who Can See Things On My Timeline." Click the *View As* link next to "Review What Other People See On Your Timeline" to see how your timeline appears to the general public or even to specific individuals. This will reveal potential mistakes in your settings. For example, you may have forgotten to mark a personal photograph for friends only yet the general public can see it. Once you have this information, you can then go back to the specific item and correct the setting.

4. Review Facebook's Privacy Settings and Account Settings from time to time, since they are liable to change without notice.

Twitter, Instagram and LinkedIn

Twitter, Instagram and LinkedIn are four social networking applications that allow the posting of status updates along with photographs, videos or other forms of media. They are not as full-featured as Facebook, but they are very popular amongst different groups of people.

Twitter

Twitter allows you to post brief comments ("tweets") on any topic along with photographs, indicate your current location, mark your tweet with a hashtag that allows others to find what you've written or to identify it with other tweets with the same hashtag, or direct the tweet at a specific individual with that person's Twitter handle (username).

Other Twitter users can "follow" you and be alerted whenever you post a new Tweet. Your followers can then reply to or forward (retweet) your original tweet, exposing you to an additional audience.

Twitter can be a very useful application for businesses and other organizations, such as news stations or law enforcement agencies that need to send out reports and alerts. Companies can notify customers about software updates and restaurant chefs even shout out the specials of the day. Twitter is also very popular amongst teenagers who just want to let each other know what kind of ice cream they are currently enjoying.

Instagram

Instagram is a photo and video sharing application. Although smart devices such as iPhones/iPads and Droids are its primary platforms, it also operates on everyday workstations and laptops. Similar to Twitter and Facebook, Instagram allows you to "like" someone's photo/video, tag the item with hashtags so that others can find it and add comments to your or others' posts. Instagram is primarily targeted at individuals rather than businesses or other organizations.

Other Instagram users can "follow" you so that they are notified whenever you upload a new photo/video.

LinkedIn

LinkedIn is primarily targeted at professionals and business/organizations. Similar to Facebook, users can create a complete profile of themselves, which include educational and professional history, links, photographs and recommendations. Users associate with networks (frequently geographical in nature) and join groups that relate to their specific interests or background.

Other LinkedIn users can request that they "connect" with you. This is analogous to a Facebook friend or Twitter follower in that it gives them more visibility into your profile/personal information.

Facebook, Twitter, Instagram and LinkedIn: The Risks of Disclosing Confidential and Personal Information

Facebook, Twitter, Instagram and LinkedIn 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 organization. For example:

1. "The boss just laid off 32 employees. I hear there may be more coming on Wednesday."

2. "Rumor has it that the Acme Widgets acquisition fell through."

3. "Working to troubleshoot a major software bug we just found."

4. "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 or is a government/state/municipal agency. 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.

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.

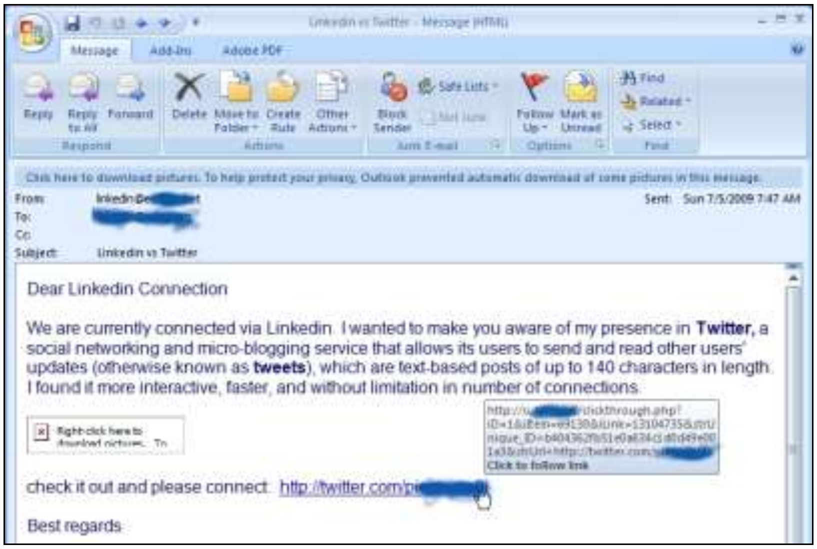
Alternatively, the company could (and should) have an Acceptable Use Policy, a document that details how these applications and the Internet in general can be used. The policy also defines consequences for failure to comply, which might be as simple as a written reprimand or as heavy as termination of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

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 Web sites 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.

From a personal/privacy perspective, there is always a risk that what you post could damage your reputation, whether in near-term or even many years from now. It's extremely easy to post a photo of yourself having a bit too much of a good time at your holiday party, or overexposing yourself in a bathing suit while on vacation at the beach. If you restrict your account's privacy settings so that only close friends or relatives see these, then perhaps this will not be a problem. But very often, prospective employers will see this information and almost demand to see it as a condition of employment.

Facebook, Twitter and LinkedIn: Spam and 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 Screen Shot 5.) 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.



From: linkedin@e[redacted]t
To: [redacted]
Cc:
Subject: Linkedin vs Twitter
Sent: Sun 7/5/2009 7:47 AM

Dear Linkedin Connection

We are currently connected via Linkedin. I wanted to make you aware of my presence in **Twitter,** a social networking and micro-blogging service that allows its users to send and read other users' updates (otherwise known as **tweets**), which are text-based posts of up to 140 characters in length. I found it more interactive, faster, and without limitation in number of connections.

http://u[redacted]/clickthrough.php?ID=1&iBen=e9130&iLink=13104735&strUnique_ID=b404362fb51e0a634cd0d49e001a3&strUrl=http://twitter.com/[redacted]

check it out and please connect: http://twitter.com/p[redacted]

Best regards

Screen Shot 5 – An example of an email hoax.
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 obtained 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?

1. Use an up-to-date email client such as Microsoft Outlook 2007 or 2010 which has 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.) Gmail and other Web-based email systems may have protection, but you should also have a recent and updated Web browser.

2. 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.

3. Use up-to-date anti-virus/anti-malware software on your computer to block any harmful files that you may have accidentally opened.

4. Always use common sense on the Web and in email; take an extra moment or two to think about what you've 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 Web sites 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 TinyURL (http://tinyurl.com) or Bitly (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 contains 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 a URL’s full path so that you know where your browser is actually directing you. Examples of Web sites 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 an individual or a company in a compromising position or at serious risk. Aside from not using these sites at all, end-user education combined with 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.

And last but not least, please feel free and secure to become a fan of Fieldbrook Solutions and/or the National Information Security Group on Facebook and LinkedIn!

• Fieldbrook Solutions on Facebook:	http://www.fieldbrook.net/facebook/
• National Information Security Group on Facebook:	http://www.naisg.org/facebook/
• National Information Security Group on LinkedIn:	http://www.naisg.org/linkedin/

***

About the Author

Brad Dinerman is the president of Fieldbrook Solutions LLC (http://www.fieldbrook.net/), 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 Information Systems Security Professional (CISSP), a Certified SonicWall Security Administrator and an Acronis Certified Engineer. 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 (http://www.fieldbrook.net/techtips/) which has been used by IT support personnel from organizations including NATO, the US Department of Homeland Security (DHS), the Department of Energy (DoE), the Department of Justice (DoJ), the National Institute of Standards and Technology (NIST), the Office of Naval Intelligence and the US Nuclear Regulatory Commission (NRC).

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.