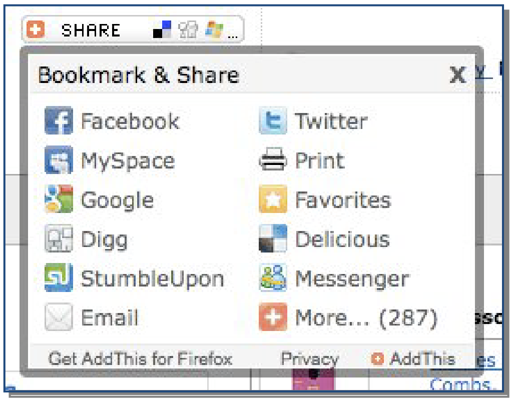
SECURITY PERSPECTIVES

Using Social Media Securely In Business and At Home

By Scott Wright
Security Perspectives Inc.

Introduction



This briefing paper is an expansion on the presentation slides and exercise handouts relating to the above topic provided during the CIN Workshops by Scott Wright.

Overview

The agenda for this paper covers the following topics:

1) **The benefits of using Social Media**. Social media tools are becoming extremely popular, especially with the younger generation of adults, as well as with teenagers. It's important to understand why these tools are so popular, and for what good (and bad) purposes they can be used. How might you plan to use Social Media?

2) **Common Social Media Features**. What does it mean when we talk about Social Media? Is everything "Social" necessarily good?

3) **Social Media risks and tips.** There are many different risks you might encounter on the Internet, but we'll discuss the most dangerous ones that people often encounter when using Social Media, as well as some tips on how to avoid them.

4) **Summary.** Finally, we'll review the major points covered in the session to reinforce the actions you should take after completing the session.

Benefits of Using Social Media

Why is "Social" such a big thing on the Internet these days?

For many years, the Internet was mainly a one-way street. Anyone could create a website. But the time and effort involved made it difficult for everyone to participate. Most sites were run by large organizations. They used it primarily to advertise their products and services, and to improve their customers' experiences.

It wasn't until sometime around the year 2000 when something called "Blogs" emerged, where people could easily enter their thoughts and opinions on sites that were actually run by larger organizations. This made it easy to post “User Generated Content” on the web. You didn’t really need your own website any more.

Then, with the advent of Facebook, LinkedIn, Twitter, people have started to use these sites to enter lots of information about themselves that others could use to locate them for personal or business purposes. Since that time, these “social networks” have grown to provide many different types of value added services to those who use them.

A big question many people don’t think to ask is, “If these sites are letting us use these services for free, how are they making money?” The answer is that they can sell the information about what people do, and even the information you enter on the site, to other companies such as large marketers who want to know what people will buy. This is how the online economy now works. The terms and conditions you agree to when registering on a site might be giving the company a great deal of control over how your personal information is used.

To most people now, the term social implies that we can all benefit from information we share with others online. So, we tend to think of “social” as good. But as people become more comfortable and trusting of this new online culture, there are opportunities for bad things to happen… and lots of them.

So, not everything “social” is necessarily good. You need to stay alert to the risks. In fact one risk, called “Social Engineering” is a very dangerous situation. It’s where people try to trick you because they know you are likely to trust them. This kind of risk has been around since long before Social Media or the Internet. Travelling salesmen and chain letters often have elements of Social Engineering in them to make you believe them, and take some action that you wouldn’t normally take if you knew the real situation, or their intent.

How Can You Use Social Media?

You may already have found a number of ways to make good use of Social Media. Here are a few ideas, in case you haven’t yet tried:

1) Enabling your audience, market or community to find you and your services;
2) Finding people who can help you;
3) Keeping abreast of industry and community news and trends;
4) Publishing your own content easily and quickly

But before you do, it’s a good time to think about the kinds of information your organization handles, as well as who might be affected, and how, if that information were abused or lost.

Questions to think about regarding Social Media risks:

1) What might attackers target in different types of organizations?
   - Personal information of clients, partners and employees
2) How might they try to trick you?
   - Posing as a new employee at a partner organization or as a prospective client
   - Posing as a donor with big prospects. What would you be prepared to do for someone who says they might give a big donation?
3) What can you say to somebody if you aren't sure they are for real, but don't want to offend them?
   - Suggestion: "Appreciate your effort in reaching out to us; but in order to protect our clients, our policy prevents us from sharing/committing to anything without an "in person" meeting at our location – and maybe a signed agreement with full name and address that you can verify
4) What if somebody thinks YOU are trying to trick them when you call on them?
   - Be prepared to offer your public website address and published contact info where they can go independently to verify your legitimacy
5) Are any of these issues preventing you from using Social Media tools effectively?
   - You should try to assess the potential benefits, while staying alert to the potential risks
   - Don't worry if you feel the risks are too great. As long as you've considered them and are comfortable with your rationale.

You should try to think about these questions as you read the following sections of this paper.

Common Social Media Features

Friend Finders

Friend Finders are commonly found features that many websites promote as a way of accelerating your participation and engagement. The idea is to help you find people you already know within the website or network, so you can share content with them easily, and gain value quickly from the community.

But beware of sites that ask you to enter your Webmail password (e.g. Yahoo Mail, Gmail, Hotmail, AOL, etc.). This provides them access to your entire address book. Not only could it result in the site abusing your contacts' Email addresses, but your Email password could be divulged to other parties – either intentionally, or by accident. You should never give your Email password to any site unless they are the Email provider.

Discussion Forums

Discussion forums are very popular and valuable tools for asking questions and getting answers. You may find information that makes your job easier, or you may be helping others by answering their questions.

1 Posts
1 Topics

Last post by Dave
in Re: battery charging
on December 20, 2010,
12:36:02 pm

Last post by Dave
in Re: UPS with Renewable O...
on January 07, 2010, 06:52:1

0 Posts

The risks here arise because attackers know that forums can be a good place to either snoop around for information that lets them launch a credible attack on your organization. They may also use forums as a place to plant malicious links or messages that might cause you to take actions that help them gain access to your computer or have you divulge information - in good faith - but that they can abuse or sell.

Examples of Social Media Benefits

Facebook (www.facebook.com)

Facebook is a great tool for connecting with personal friends and sharing casual information. Facebook lets you invite others to be your friends so you can interact and see what's going on in each others' lives. It's a "symmetrical" relationship, meaning that if I'm your friend, then you're my friend.

There are also "Facebook Pages" that can be set up by organizations as a way of promoting themselves and engaging with their customer base. Radio and TV stations have recently discovered that this is a good way to keep their audiences engaged. So, Facebook can be a very good tool for marketing.

However, if you intend to use Facebook for marketing purposes, try to use a completely separate account from your personal account. Otherwise, you may find that business associates are learning too much about your personal activities, and those of your friends.

You can adjust how much of your personal information is shared with your friends, and with the general public, and it's a good idea to check these settings regularly by clicking on the Facebook menu item at the top right of your Facebook Profile page that says "Settings" and look for "Privacy Settings".

LinkedIn (www.linkedin.com)

LinkedIn is much like Facebook, but it is geared towards business users who want to network with others for business purposes. People looking for jobs, suppliers or customers can use LinkedIn to easily make new connections. If your connections post their activities, you can see them. There are many other features in LinkedIn that make it a useful tool for business purposes.

Because LinkedIn is more "closed" than Facebook when it comes to the amount of information visible between users, by default, it is considered a little less risky. But there are still some risks we'll discuss later.

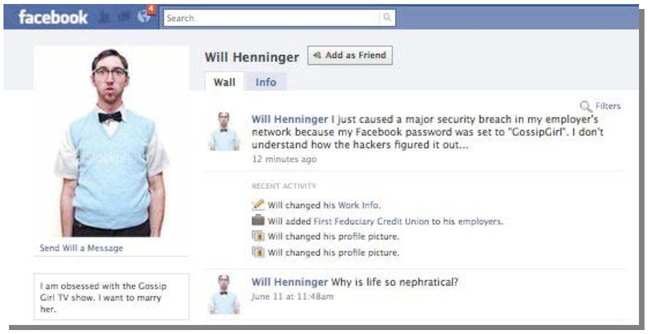
Twitter (www.twitter.com)

Twitter is sometimes called a "microblogging" platform, which means you can write short updates about what you are doing, or your thoughts. There's a limit of 140 characters on a single post. It's a very quick and easy way to spread news and promote events.

People often forget that everything they post on Twitter is essentially available to the general public. This has caused problems for many people – from losing a job that was offered verbally, to receiving a cold reception at a speaking engagement – when they "tweet" something that really should have been kept private.

Top 5 Social Media Security and Privacy Risks

1) Impersonation and Fake Profiles



Will Henninger I just caused a major security breach in my employer's network because my Facebook password was set to "GossipGirl". I don't understand how the hackers figured it out...
12 minutes ago

RECENT ACTIVITY
Will changed his Work Info.
Will added First Feduciary Credit Union to his employers.
Will changed his profile picture.
Will changed his profile picture.

Will Henninger Why is life so nephratical?
June 11 at 11:48am

I am obsessed with the Gossip Girl TV show. I want to marry her.

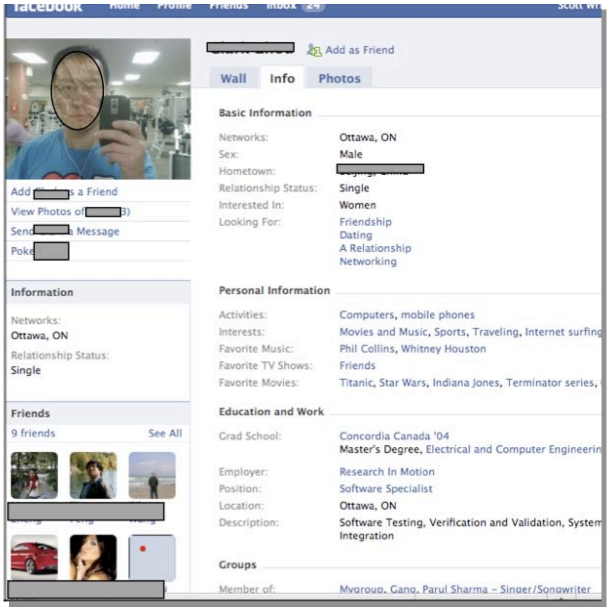
Security professionals agree that as many as 40% of new Facebook profiles are fakes – created by attackers who are trying to gain the trust of innocent users. This approach is often successful because attackers know that social media site users tend to trust people they have accepted as friends. Besides, most people tend to believe that, "It's not very sociable to reject an invitation from somebody who wants to be your friend."

Unfortunately, attackers don't feel any compulsion to uphold the trust that's been put in them. They will exploit this trust to learn more about their new "friends", finding out more personal information that can be used to guess passwords or password recovery questions, which will let them take over the account. Or, they might try to use other methods described below, once they are able to gain your trust.

TIP: Never accept “Friend” requests on any social network from people you don’t know already, without checking into their background. They may not be real, and they could be dangerous.

2) Too much information

Many people don’t realize how much information about them is visible to others on a social network. When you first create an account on Facebook, for example, you are asked to fill in many fields with personal information. It’s usually not necessary, but when asked, people enter this information anyway. The problem is that, unless you check to see which information is made public, and which is only shared with friends, you could be exposing more of your personal information than you intended.



[redacted]

Add [redacted] s a Friend
View Photos of [redacted] 3)
Send [redacted] a Message
Poke [redacted]

Information
Networks:
Ottawa, ON
Relationship Status:
Single

Friends
9 friends See All
[redacted]
[redacted]

Basic Information
Networks: Ottawa, ON
Sex: Male
Hometown: [redacted]
Relationship Status: Single
Interested In: Women
Looking For: Friendship
Dating
A Relationship
Networking

Personal Information
Activities: Computers, mobile phones
Interests: Movies and Music, Sports, Traveling, Internet surfing
Favorite Music: Phil Collins, Whitney Houston
Favorite TV Shows: Friends
Favorite Movies: Titanic, Star Wars, Indiana Jones, Terminator series,

Education and Work
Grad School: Concordia Canada '04
Master's Degree, Electrical and Computer Engineerin
Employer: Research In Motion
Position: Software Specialist
Location: Ottawa, ON
Description: Software Testing, Verification and Validation, System Integration

Groups
Member of: Mygroup, Gang, Parul Sharma – Singer/Songwriter

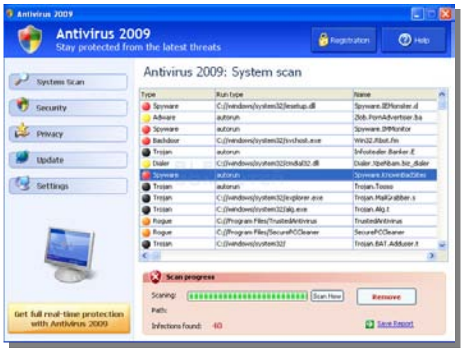
With the right information, an attacker could be able to guess your password, or even answer the questions you set up to reset your password, in case you forgot it. This allows them to assume your identity, post information and send messages to your friends with malicious intent.

Attackers might also use the information they know about you to set up another fake account in your name. They could then start sending invitations to your real friends who are not yet already connected to you. Then, your friends might become targets of Identity Theft or other attacks.

TIP: Always check the privacy settings that control which information is visible, and to whom. You should also remember that anything you enter into a site might one day become available, either accidentally or maliciously, to people you did not intend to see it. So, try not to post information you wouldn’t want your mother or your boss to see – even if you have set your privacy settings appropriately. Once it is available on the Internet, “Data Never Dies”. It can persist forever.

3) *Deception and Tricky Tactics*

Social Engineering is the fancy word used to describe scams, hoaxes and tricks that attackers use to convince you to do something you wouldn't normally do. Whether it's posing as a friend of yours who's supposedly been robbed in a foreign country, and needs you to wire money to get home; or a pop-up window saying your computer has a virus infection when it really doesn't, these can be very costly situations if you become a victim of them.



Antivirus 2009: System scan

Type	Run type	Name
Spyware	C:/windows/system32/lesetup.dll	Spyware.IEMonster.d
Adware	autorun	Zlob.PornAdvertiser.ba
Spyware	autorun	Spyware.DMMonitor
Backdoor	C:/windows/system32/svchost.exe	Win32.Rbot.fm
Trojan	autorun	Infostealer.Banker.E
Dialer	C:/windows/system32/cmdial32.dll	Dialer.XpehBam.biz_dialer
Spyware	autorun	Spyware.KnownBadSites
Trojan	autorun	Trojan.Tooso
Trojan	C:/windows/system32/explorer.exe	Trojan.MailGrabber.s
Trojan	C:/windows/system32/alg.exe	Trojan.Alg.t
Rogue	C:/Program Files/TrustedAntivirus	TrustedAntivirus
Rogue	C:/Program Files/SecurePCCleaner	SecurePCCleaner
Trojan	C:/windows/system32/	Trojan.BAT.Adduser.t

Scaning:
Path:
Infections found: 40

These types of attacks can happen on the Internet, in phone calls or in person. But they work particularly well on users of social networks. This is another reason why attackers try to get you to accept friend requests from fake users. If you are a very trusting person, you might not realize that there are some really bad people who will try to convince you that you should help them, or take unusual actions.

TIP: Always be suspicious of people – online or in person – who ask you to do something unusual, or who seem to be in a desperate situation. They may even try to pull rank on you by saying they are from a bank or some authority such as the government. Always check their identity carefully, and if possible, tell them you will call them on a publicly listed phone number for their "organization". For example, look up the customer service number for them, which is usually easy to find if it is a popular institution such as a bank, government or delivery company. Never take action on a single piece of information that is asking you to do something. Always double check through some other source to make sure it's not a scam that could cost you money or your identity.

4) *Password and Identity Theft*

You might not think that stealing your identity is a big deal. After all, if your credit card is stolen, you may only be liable for $50 or less. But aside from the inconvenience of having to change accounts, you might end up having loans taken out in your name, that you would be liable for paying back. Or, you might find out that a crime was committed in your name using your identity information. This can be very hard to have corrected, and might cause you a great deal of embarrassment.

One of the easiest ways for attackers to steal your identity is to obtain your password to an online account. Whether it's your Email account and password or your Facebook account can be the beginning of an escalating attack that provides the attacker with enough information to impersonate you in committing a crime.

TIP: Protect your personal information well by using good passwords, and keeping them a secret. Ideally, every account you create should use a different password, since it is a common practice for bad guys to try a stolen password on many different accounts such as banks, payment services or even employer networks. You should never share your passwords with anyone – not even your employer's IT department. Attackers will often pose as system administrators asking for help in solving a problem by having you given them your password. A legitimate system administrator with appropriate privileges on your office network should never need to ask for your password. They may change it for you and then ask you to change it. But you should never have to divulge it to them.

5) Insider Threats and Human Resources Risks

There are many ways that social networks can be used (and abused) within an organization. So, employers have to be vigilant and exercise due diligence in allowing and monitoring employee access to social networks. Whether it is screening new employment candidates or checking for discrepancies in a claim by an employee, supplier or customer, there can be legal issues that should be considered.

TIP: It's a very good idea for employers to have a clear "Posting Policy", which tells employees what they are allowed to do when it comes to posting information about the employer or their job online. It may be allowed, or even required, in certain positions, such as Marketing. However, there should be controls on which individuals or roles have this privilege, as well as which accounts should be used, and what information can and can't be posted online. No employees should be allowed to post information about the employer without authorization, and it's a good idea to require that it always be done from authorized accounts.

Summary

While it is becoming more and more important to have a presence on social networks, and to use online social media websites, you should make an effort to understand the risks associated with each website you use. Virtually every website has a social media element to it nowadays, and they can have varying degrees of risk.

Following these tips, and keeping up to date on new types of risks and attackers – especially related to your business – can make the difference between being productive with social media and becoming a victim of an online attack:

1) Don't accept invitations from "Friends" you don't know, and be careful to check that the person you are connecting with is the actual person, and not an imposter.
2) Check the privacy settings for social media accounts you set up on any website to make sure you know what information is being shared, or adjust the settings to protect your personal information from people you don't know. Also, don't post anything your mother or boss shouldn't see, just in case the data becomes exposed.
3) Be suspicious of unusual requests or statements from people online. If it doesn't seem right, it could be a social engineering attack, intended to steal your identity or to get you to do something you wouldn't normally do.
4) Use different, strong passwords on different sites, and keep them secret. Passwords are the keys to your kingdom. Protecting them will reduce the risk of Identity Theft.
5) Have clear social media or Internet posting policies for employees who use social media accounts. Only authorized information should be posted from authorized accounts to reduce the risk of accidental disclosure of sensitive information on the Internet.

About Scott Wright

Scott Wright is a professional speaker, blogger and security coach who helps teams in facing the risks of using the Internet. He has over 20 years of experience with public and private sector organizations, and uses innovative techniques and products to engage and educate staff on how to work securely and efficiently with sensitive information in the office, at home and the Internet.

You can contact Scott at:

Security Perspectives Inc.
104-2720 Queensview Dr.
Ottawa, ON
K2B 1A5

swright@securityperspectives.com

613-693-0997