OWN YOUR SPACE

Compliments of Microsoft®

Going Social

KEEP YOURSELF AND YOUR STUFF SAFE ONLINE

Edited by Linda McCarthy and Denise Weldon-Siviy

Publisher: Linda McCarthy
Editor in Chief: Denise Weldon-Siviy
Managing Editor: Linda McCarthy
Cover designer: Alan Clements
Cover artist: Nina Matsumoto
Interior artist: Heather Dixon
Web design: Eric Tindall and Ngenworks
Indexer: Joy Dean Lee
Interior design and composition: Kim Scott, Bumpy Design
Content distribution: Keith Watson

ISBN 978-0-615-37366-9
Library of Congress Cataloging-in-publication Data

McCarthy, Linda
Own your space : keep yourself and your stuff safe online / Linda McCarthy.
ISBN 978-0-615-37366-9 (electronic) 1. Computer security. 2. Computers and children. 3. Internet and teenagers. 4. Computer networks-Security measures. I. Title.

Visit us on the Web: www.100 pagepress.com

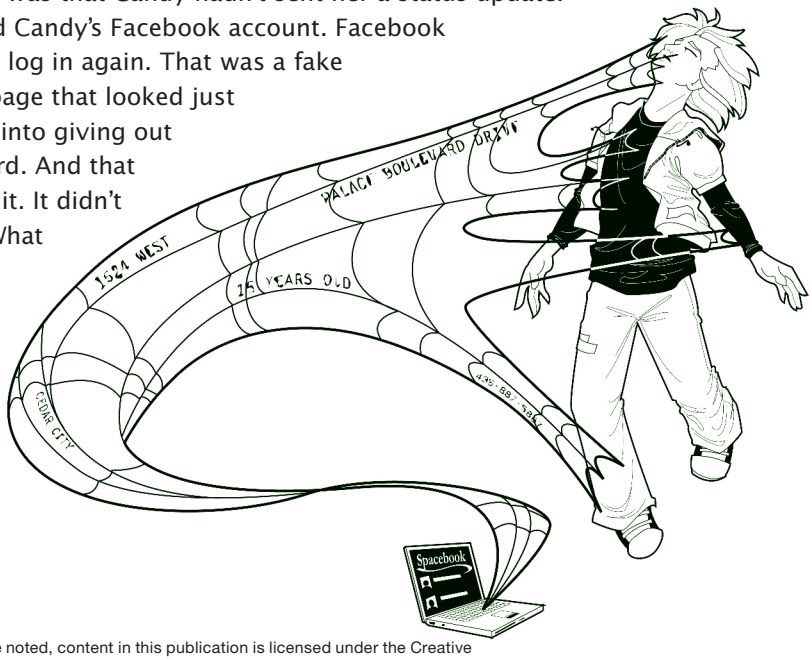
Download free electronic versions of the book from MySpace (http://www.myspace.com/ownyourspace) and Facebook (http://www.facebook.com/ownyourspace.net), and from Own Your Space (http://www.ownyourspace.net)

Chapter 11

Going Social

High school senior Miranda has always been a photo hound. Her mom kids that she's been hamming it up for family shots since before she could walk upright. So when Miranda got a status update on Facebook from her friend Candy announcing, "My friend caught you on hidden cam..." she just *had* to look. Funny, her computer wasn't behaving at the time. She had to log in to Facebook again, even though she'd just logged in a few minutes before. Then she couldn't view the photos until she downloaded a new version of Flash...

What Miranda didn't realize was that Candy hadn't sent her a status update. A nasty worm had accessed Candy's Facebook account. Facebook also didn't want Miranda to log in again. That was a fake screen, displaying a login page that looked just like Facebook's to trick her into giving out her user name and password. And that Flash update? You guessed it. It didn't link to Adobe Flash at all. What Miranda downloaded was rogue security software. Minutes later, she was seeing pop-up windows informing her that her computer was infected with spyware and it would only cost her $49.95 to upgrade her security software to get rid of it...



ISBN 978-0-615-37366-9

Like many users before and after her, Miranda was scammed by malware targeting social networking sites. In this case, the worm distributed a link to a fake login screen to phish her password, then tricked her into downloading a Trojan which kept directing her browser to fraudulent websites that pushed rogue security software. In less than 15 minutes, Miranda managed to get hit with almost every variation on malware!

Right now, scammers are targeting social networking sites big time because that's where people are spending more and more of their time online. Why so popular? Social networking is what the pundits call being part of an online community that facilitates connections between users. Obviously, there have been places to meet and discuss issues with online "friends" since the Internet began. However, the early bulletin boards and discussion groups were limited. Users posted their opinions and often responded to the postings of others, but they didn't grow their communities in the same way as today's social networks.

11.1 Where the Friends Are

In 2003, MySpace became the first major **social networking site**. Based on an earlier, less developed site called Friendster, MySpace hit the big time in a big way. By 2010, the U.S. site sported over 70 million users. Factoring in MySpace sites for 30 countries worldwide, plus specialty sites like MySpace Latino, that's about 125 million MySpace users.

Social networking site A website that allows users to define relationships between themselves and network among not just their own friends, but friends of friends, and friends of friends' friends—ever expanding their online network.

Hardly the first social networking site, MySpace was the first to "go viral" in terms of coming to the attention of the general public. While users are technically "required" to be at least 13, the requirement is based on self-reporting of age.

MySpace users, while dedicated, often also have accounts at other social networking sites, like Facebook. Facebook was started in 2003 by Harvard sophomore Mark Zuckerberg as an online version of the college facebooks. These were photo books issued for each freshman class (at smaller schools) or each dorm (at larger

universities) to help new students get to know each other. At the time, Harvard didn't have a student directory with photos and web mythology credits the site with 22,000 photo views in its first four hours online. The response was so high that Zuckerberg launched an official site, limited to Harvard students, in 2004. Within a month, half the undergraduate student body had registered.

It wasn't until September 2006 that Facebook opened membership to anyone 13 or older with a valid email address. By mid-2008, Facebook was running neck to neck with MySpace, pulling ahead worldwide in November 2008 when Facebook drew 200 million unique worldwide visitors. That month, over 20% of Internet users visited Facebook. By August 2010, Facebook alone reported 500 million active users.

While MySpace and Facebook most certainly dominate the market, they are far from the only social networking sites frequented by teens. Other popular sites include Friendster, Yoursphere, and Bebo. Altogether, those sites boast enough users to populate a Latin American country. By 2009, 72% of teens and young adults used at least one social networking site.

11.2 Friends: Real and Virtual

"Friending" and being "Friended" are incredibly important concepts to understanding the social network scene. When you register for an account at MySpace or Facebook, the service offers to look up all the email addresses in your web-based email and compare those addresses against actual Facebook users. In 2010, the average Facebook user had 130 Friends.

Poke Hitting Poke in Facebook lets another user know you'd like to get her attention. She can poke you back, write on your wall, or even ask to Friend you.

Collecting "Friends" is both the greatest advantage and the weakest link of online social networks. Because of privacy controls, most of the Profile information you post on social networks is viewable only by other users that you've designated as Friends. The danger comes when teens eager to appear popular accept Friends that they don't really know and post too much information thinking that only their

friends will see their page. Sixteen-year-old Eric from Novato, California thought it was really cool to have 1,700 friends. In reality, some of those friends could just be creeps peeking around at your life. Further, malware has been created to exploit that trust on social networks. Naïve users who believe that only their friends have access to their postings are often appalled when those postings are captured, re-posted, and circulated to people they never would have wanted to share them with.

11.3 Groups

Both MySpace and Facebook have official policies against "Harmful content" as well as content deemed offensive or abusive. While these are great policies in theory, the practice leaves much to be desired, especially in the area of Group content.

Facebook alone sports thousands of groups which allow members with similar interests to meet and network—purportedly the actual point of having a social networking site. These groups include scores of innocuous Fan Clubs like "Addicted To Project Runway" and rather imaginative whimsical groups like "Physics doesn't exist, it's all gnomes." Some even sound a bit desperate, like "We need to find a kidney donor for our father. Help us spread the word." Or promote a political or heartfelt religious sentiment.

Unfortunately, other groups seem to live on the dark side. In the first 10 minutes of scanning groups to prepare this chapter, we had occasion to report no less than 12 groups to Facebook for violations including nudity in photos, obscenity, and vulgar language.

In addition to general smut, a bigger problem rests in the intended content of many of the groups. Even if you discount the heavily questionable content of some of the groups categorized under Sexuality, you're left with a large number of groups that glorify underage drinking.

Friend to All

Feeling friendless? Whatever you do, don't compare yourself to Tom Anderson.

Co-founder of MySpace, 34-year old Tom is the "default" friend given to all new MySpace users. By April 2010, Tom had over 12 million friends.

In their defense, keeping social networks clear of bad content given their millions of users must be a daunting task indeed. Even if such entries are removed within hours, the constant postings of new users would still provide a nearly endless stream of objectionable material.

11.4 Third-Party Apps

A social networking application is a separate program that works within the social networking site to provide additional functionality. Because these functions are written by independent companies, they're referred to as third-party apps. If you've used Farmville, played Scrabble, or sent a birthday card on Facebook, you've used a third-party application. If you haven't used one, you're in the minority. Facebook reports that 70% of active users access third-party applications each month. Hardly surprising given that there are over 500,000 applications!

Because third-party applications are run by companies other than your social networking site, using them has implications for your privacy. When you agree to use a third-party application, you're giving that party permission to access at least some of your Facebook or MySpace information. According to the Facebook Terms of Service, "When you add an application and use Platform, your content and information is shared with the application. We require applications to respect your privacy settings, but your agreement with that application will control how the application can use the content and information you share." This means that you need to carefully read the user agreement when you add a new application. Not concerned? You may not realize just how much information you're giving away. In addition to a list of your Friends, your user information could include your name, profile photo, birthday, political views, hobbies, interests, relationship status, education history, and work history as well as copies of all the photos in your Facebook site photo albums. In the hands of an unscrupulous advertiser, that's a gold mine.

Sometimes, an application provides MORE than you asked for. In early 2008, it was learned that a popular Facebook application known as *Secret Crush* was delivering adware from Zango. While Facebook put a stop to that, in many respects they're playing the same game that you are with malware—they're just playing on

a much larger scale. Facebook changes their policies and attempts to block obvious malware, phishing attempts, and adware. The bad guys look for loopholes in the legal writings or software to get around the new rules. As the victim in the middle, it's your job to beware of scams and keep track of what you're agreeing to and with whom.

11.5 Phishers of Friends

By 2009, phishing expeditions on social networking sites became a nearly daily event. Some of the more memorable were FBAction.net, Koobface, and Areps.at. Most of these phishing scams took the form of status postings containing embedded links. If you clicked the link, you were routed to an outside website where you saw a Facebook login screen that looked almost exactly like the real screen. If you bit and logged in a second time without thinking about it, your Friends would soon receive a status posting with an embedded link. To add insult to injury, the outside website often infected your computer with adware.

These types of phishing attacks are especially on the rise. Knowing what we all know at this point about phishing attacks, why do so many people still fall victim? The attackers rely heavily on social engineering. While users have learned to be very cautious about links embedded in emails, we tend to be very trusting of links embedded in postings from Friends. Basically, the phishers exploit our natural tendency to trust our own friends. For even higher click through, attackers use postings guaranteed to pique your interest. The Koobface attack on MySpace and Facebook in 2009 generated status updates like *Paris Hilton tosses dwarf on the street* and *My friend caught you on hidden cam. Have a look!*

11.6 Posting Too Much Information

Most teenagers post a lot of very personal information online. This can have long-lasting consequences that you may not have thought about. According to Career-Builder, about 30% of employers search social networking sites to check out new hires. And a third of hiring managers report turning down an application because of information they found online.

Experts disagree on whether employer screening of social networking sites is good or bad. On the plus side, ambitious teens can use social networking sites to present their better sides by including photos and postings about extra-curricular activities and volunteer work. On the down side, students often post a lot of personal information that employers aren't allowed to ask about because they can't legally use that information to make a hiring decision. Those details can include a job candidates' gender, age, race, religion, political views, physical or mental disabilities, and sexual orientation. It isn't just racy photos you need to worry about. That photo of you at a Gay Rights March or a Pro-Life Rally could seriously offend a potential employer. Should they make hiring decisions based on that type of personal information? Not really. The problem is that once your information is public, it's public.

To protect your personal information, take Facebook's own advice and "Control every time you share." On all of the social networking sites, you have the option to lock-down your profile and limit access to your personal information and photos to just your Friends. In many cases, you can even select a subset of Friends.

11.6.1 Questionable Photos

People who love social networking sites LOVE photos. Facebook reports that three *billion* photos are uploaded to its site every month. That's a lot of birthday parties, anniversaries, and graduations. That's also billions of opportunities for users to post photos that they probably should have kept to themselves (or never taken in the first place!).

Online photos are a great source of entertainment—especially for personnel directors and job recruiters. As Allan Hoffman, a Tech Jobs Expert at mega-employment firm MONSTER points out, "It's not just what you say that can be held against you when you're looking for a job. It's also what you post on MySpace, write in your blog and broadcast on YouTube." Photos from last year's homecoming dance that entertain your friends today could keep you from being hired in the future.

Photos can also allow stalkers and pedophiles to identify you. To protect yourself from all of these dangers, be very careful about what you post online. Also try to

keep tabs on the photos others post of you in which you're identified ("tagged"). By tagging photos, your friends can easily identify you to the world within photos you'd rather not share. ***Real*** friends aren't determined to make you look foolish online.

11.6.2 Dangerous Webcams

Webcams present all the dangers of digital cameras and then some. A frightening recent phenomenon has been the advent of pedophiles on social networking sites offering teens money to take off their clothes and perform inappropriately in front of their webcams. Justin Berry was just 13 when he was propositioned by a pedophile. For the next five years, he used his webcam to basically work as a child prostitute.

While it is unlikely that your webcam will turn you into a prostitute, it is likely at some point to make you look like an idiot. Silly pranks make home movies endlessly entertaining when shared with family and close friends—people who know you and love you and find it funny because the behavior on film is so *unlike* you. Strangers don't see videos that same way. They're laughing AT you, not with you. Again, use discretion with anything you put online. Consider how you'll feel about that video when you're 30.

In the meantime, having a webcam in your home may seriously compromise your privacy. Imagine how surprised Blake Robbins was to discover that his high school had activated a webcam in the school-provided laptop and was spying on what he did in his own bedroom. Blake became aware of the spying when the school disciplined him for suspected inappropriate behavior and provided as proof a photo the laptop webcam had taken of him without his knowledge. Fellow students were stunned. Savannah Williams, a sophomore at the same school outside of Philadelphia was very distraught, pointing out that she often took her laptop into the bathroom with her to listen to music while showering.

11.6.3 YouTube

Webcams allow you to embarrass yourself in front of all your social networking Friends. YouTube lets you share that humiliation with perfect strangers.

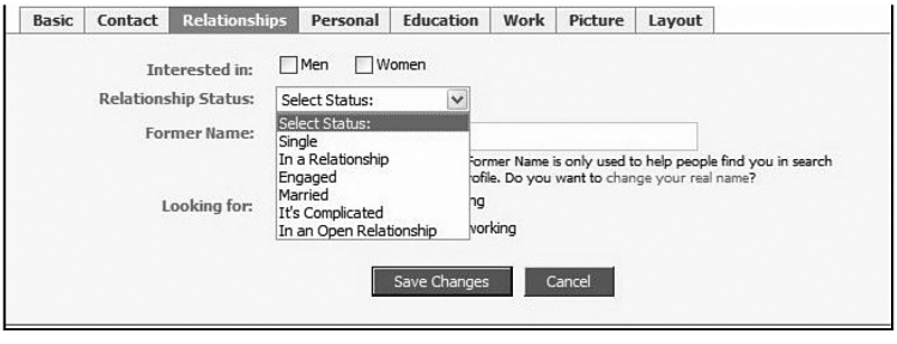
We've all seen YouTube videos that were hysterically funny. To us. But when they're viewed millions of times, those funny videos can really damage their

subjects' self-esteem and mental health. Imagine how you'd feel knowing that millions of perfect strangers were laughing at you. That's only funny when it happens to someone *else*.

Mental health isn't the only issue either. The would-be producers can easily get carried away. One mom reported in 2009 that her 15-year-old son and his friends had produced some seriously disturbing videos for YouTube. "They had everything from silly stunts to self-injury like stapling themselves and pouring rubbing alcohol on their hands and lighting it with a lighter." Was her son a problem kid? Not really. He was trying to be creative and felt that he needed to be extreme in his video to get attention online. He's lucky he wasn't permanently injured.

11.7 Breaking Up Online

Another thing to keep in mind about social networking sites is that more and more they take the place of people actually meeting, talking, and connecting on emotional issues. In researching this book, we've heard from a remarkable number of teens who tell us they've been dumped at least once on Facebook. How does this work? Facebook provides a relationship indicator. When you enter your profile information, it allows you to define your **Relationship Status**.



Today, those emotionally underdeveloped partners who would have slunk off without calling in years past simply change their **Relationship Status** online. Far too many a committed partner now learns from a friend that their significant other is now listed as **Single**. This brings up probably the best indicator of whether you're

really ready for online social networks—self-confidence and maturity. Are you self-confident enough to handle being dumped online? Even better, are you mature enough NOT to do that to someone else? We saw one teen devastated when his best friend told him that Suzie (his girlfriend for four years) had changed her relationship status to **Single**. That's not cool. It's cruel.

11.8 Tweet, Sweet

Created in 2006, Twitter is a social networking site that specializes in microblogging. That's heavy on the "micro." Twitter updates, called tweets, are required to be short and sweet.

```
Tweeting is the social networking equivalent of text messaging. Each "tweet" can
contain no more than 140 characters... This "tweet" is exactly 140 characters long...
```

Often jokingly referred to as blogging for the sound-bite generation, Twitter was designed for users on the go who were posting from cell phones and other mobile devices. That's actually the reason for the short status limit. Cell phone text messages are limited to 160 characters, so Twitter limits tweets to 140 characters, leaving 20 characters for author attribution.

Like other social networking sites, Twitter works with third-party applications. 50,000 of them by 2010. It's also susceptible to many of the malware and phishing attacks directed at the other social networking sites.

Twitter has also been a target itself. In 2009, 184+ million users were locked out on several occasions due to denial of service attacks aimed at the site. Some pundits speculated that Twitter was targeted because the site has been aggressively filtering URLs to block those used in malicious tweets, reducing the malware writers' income. Sometimes, even when you win, you lose.

11.9 Tips for Staying Safe and Social

Scammers are targeting social networking sites because that's where people are spending their time online. Here are some tips for staying safe:

- Watch out what you post. Don't reveal your full name, address, phone number, or school.

- Stay in your age group. If you're 13, don't pretend to be 19. That could put you in conversations and discussions that are uncomfortable because you're not quite emotionally ready for them.
- Don't post content you wouldn't want your parents to see. Remember that information you post today could come back to haunt you when you are trying to get a scholarship or a job.
- Understand the privacy settings for the social networking site you use. Then use those privacy settings!
- Even if you lock down your profile and define your postings as private, don't assume that no one can see them. Some malware specifically targets "private" pages.
- Remember that you're not the only person you know with a camera or webcam. Keep tabs on any photos or videos your friends are posting that might feature you.
- Don't take Friends at face value unless you've actually looked at their faces. That 16-year-old girl you met online might be a 65-year-old man.
- Don't let anyone talk you into doing anything you find creepy or feel uncomfortable about. That especially means anything that involves your webcam. Inappropriate videos NEVER go away. Just ask Paris Hilton….
- Never ever meet anyone F2F for the first time by yourself. This is pretty self-explanatory but the most critical deterrent to online creeps. Don't put yourself in a dangerous situation when you don't need to.

OWN YOUR SPACE

KEEP YOURSELF AND YOUR STUFF SAFE ONLINE

THE BOOK FOR TEENS THAT EVERY PARENT SHOULD READ!

A collaborative project to provide free security learning to teens and families online, made available under the Creative Commons Licensing, and made possible by the support of individual and corporate sponsors.

Every day, millions of American school children log on or log in and make decisions that can compromise their safety, security, and privacy. We've all heard the horror stories of stolen identities, cyber stalking, and perverts on the Internet. Kids need to know how to stay safe online and how to use the Internet in ways that won't jeopardize their privacy or damage their reputations for years to come.

Learn how to

- Kill viruses, worms, Trojans, and spyware
- Deal with cyberbullies
- Give SPAM the curb and smash web bugs
- Understand just how public your "private" blogs are
- Keep wireless freeloaders off your network
- Prevent sexting from ruining your life

About the team

Linda McCarthy, the former Senior Director of Internet Safety at Symantec, wrote the first edition of *Own Your Space*. With 20+ years experience in the industry, Linda has been hired to test security on corporate networks around the world. For the 2010 edition, Linda's expertise is backed up by a full team to provide the best security experience possible for teens and families online. That team includes security experts, design experts, anime artists, and parent reviewers, as well as a dedicated group of teen reviewers, web designers, and test readers.

General Computing

ISBN 978-0-615-37366-9

51999>

9 780615 373669

$19.99 US / $24.99 CAN

Cover design: Alan Clements
Cover artist: Nina Matsumoto

www.100pagepress.com

page press
Smart Books for Smart People®