The 7 Security Secrets of Social Networking

An Exclusive White Paper by John Sileo

GT62JSWP

On the surface, social networking is like a worldwide cocktail party — full of new friends, fascinating places and tasty apps. Resisting the urge to drink from the endless fountain of information is nearly impossible because everyone else is doing it — connecting is often advantageous for professional reasons, it's trendy and, unchecked, it can be dangerous.

Beneath the surface of the social networking cocktail party lives a painful data-exposure hangover for the average business. Sites like Facebook and Twitter are now the preferred tool for malware delivery, phishing, and "friends-in-distress" scams while more business-oriented sites, like LinkedIn, allow for easy corporate espionage and the manipulation of your employees.

> *"Beneath the surface of the social networking cocktail party lives a painful data exposure hangover..."*

To avoid the cocktail party altogether is both impractical and naïve — the benefits of social networking outweigh the dangers — but applying discretion and wisdom to your social strategy makes for smart business. Follow *The 7 Security Secrets of Social Networking* to begin locking down your sensitive data.

1. On social networks, possession is ten-tenths of the law.

When you put your business's information on a social network, you have forfeited your exclusive right to that information. Unlike a physical asset, information can be simultaneously recreated, stored and accessed by unlimited users at any one time, allowing it to flow like water through your fingers. Additionally, there are very few laws governing the ownership of information once it leaves your office (e.g., goes into the cloud), leaving you no legal precedence for winning back your privacy. On a personal level, for example, when you populate your Facebook profile with a date of birth, it is sold to advertisers along with your demographics, "Likes" and a map of your

friend network. Similarly, in the business world, the minute you establish a Facebook page and begin to attract "fans" or a Twitter page for followers, you've just centralized and publicized your customer list for competitors.

Solution: Create a strategic plan *before* you expose your intellectual property.

Prior to going live with a corporate social networking profile or sharing your next post, think through how much sensitive information you are sharing, and with whom. Unlike a traditional website, social networks connect human beings, some of whom want to map your organizational structure, track your marketing initiatives, hire your star employees, breach your systems, poach your fan list or steal sensitive intellectual capital. It is imperative that you: **1.** Create a strategic social networking plan that defines what information can and should be shared by executives and employees on Facebook, Twitter, LinkedIn, etc.; **2.** Consider using social media to attract new prospects rather than creating a following of existing (and poachable) clients; **3.** Populate your profile with only publicly available, marketing-based data; **4.** Keep personal comments for personal pages, as they have no place at work; **5.** Don't rely on a *policy* to communicate your intentions and requirements surrounding social media. The most successful companies build a culture of privacy through an interactive process that allows the entire team to co-create a solution.

2. Lack of education, not technology, is the greatest source of risk.

It's easy to blame our data privacy woes on technology. At the heart of every security failure (technological or otherwise) is a poor human decision, generally due to a lack of awareness. For instance, an employee, not a machine, decides to spend their lunch break using their work computer to post on personal social networking sites. In many cases, they do so because the business has not established guidelines for these scenarios, nor have they educated them on the risks. For example, most employees don't understand

that more than 30% of all malware is delivered to corporate computers via social spam through *personal* social networking use conducted on work computers.

Solution: Educate your team as individuals *first*, employees second.
The most effective way to change a human being is to appeal to them emotionally, not intellectually. Most of us are more emotionally connected to our personal lives than to our jobs. Consequently, by motivating your employees to protect their own social networking profiles first (and their kids'), you are not only lowering the malware and fraud that they introduce into your computers through lunch-time surfing, you are also giving them the framework and language to protect the company's social networking efforts. Be sure to:
1. Break the training down into bite-sized, single-topic morsels that won't overwhelm or discourage employees; **2.** Allow employees to spend a few moments applying the fixes you've just given them and once they've made the changes personally; **3.** Reconvene and discuss what it all has to do with your organization's social networking strategy. They will return to the learning table with emotional buy-in and awareness. Strategies **3** and **5** (below) are examples of this bite-sized, personal-to-professional adaptation process.

3. Most social networking risks are old scams with new twists.

During a lunch break at work, you receive a Facebook post that seems like it's from a friend. It's impossible not to click, enticing you with captions like, "Check out what our old high school friend does for a living now!" Seemingly harmless, you click on a video, a coupon, or a link to win a FREE iPad and presto, you've just infected your computer with malware that allows cyber thieves full access into your company network. You've been tricked by a repackaged version of the virus-delivering-spam emails of five years ago. Spam has officially moved into the world of social media (thus, social spam), and is now responsible for 30% of all viruses, spyware and botnets that infect our computers.

Solution: Discuss social spam self defense at your next team meeting. It's amazing how quickly people detect social spam *once* they've been warned! After all, they've seen it before just disguised in other forms. In addition to giving employees visual examples of social spam, click-jacking and like-jacking, make sure that they are equipped with the following knowledge. **1.** If an offer in a social networking post is too enticing, too good to be true, too bad to be real or just doesn't feel right, *don't click!* **2.** If you do click and *aren't* taken directly to the site you expected, make sure you *never click a second time*, as this gives cyber thieves the ability to download malware onto your system. **3.** Deny social media account takeover by using strong alphanumeric passwords that are different for every site and that you change frequently. **4.** Account takeover is easy for criminals, which means that not all "friends" are who they say they are. If you suspect foul play, call your contact and verify their post. **5.** Make sure that you protect your business with the latest cyber security and anti-theft prevention tools available. I will discuss these in the next strategy.

"Criminals, either highly efficient or lazy, want the highest return on their investment (time) for the least amount of work, which is why they follow the path of least resistance."

4. Cyber thieves follow the path of least resistance by looking for open doors.

Data thieves aren't interested in delivering malware to just *any* business (using social networking as their primary delivery device); they specifically target organizations that have done the least to protect their computers, networks, mobile devices, Wi-Fi and Internet connections. Why burgle a house with deadbolts and an alarm when you can attack the home down the street that left the front door wide open? In business, the "open door" usually comes in the form of poor computer security.

Solution: Create a Path of Strategically Elevated Resistance. Thieves get discouraged (and move on to other victims) when you put roadblocks

in their way. Keeping your network security up to date is the smartest way to quickly and effectively elevate your defenses against cybercrime. Follow these simple steps: **1.** Hire a professional to conduct a security assessment on your network; the investment will pay for itself hundreds of times over. **2.** During the assessment and follow-up process, make sure that the IT professional:

a. Installs a security suite like **McAfee®** on every computer, including mobile devices that travel. **b.** Sets up your operating system and critical software for automatic security updates. **c.** Enables and configures a firewall to block incoming cyber criminals, and **d.** Configures your Wi-Fi network with WPA2+ encryption.

To cover all of your bases, make sure that you are prepared for a breach. **Safeguard®**, in partnership with **EZShield®**, provides state-of-the-art identity protection and recovery services for businesses. It's like health insurance for your information assets.

5. Data criminals systematically exploit our defaults.

Another way to create a path of strategically elevated resistance is to take away the "broadcast" nature of social networking exploited by thieves and competitors. Instead of inviting everyone to your cocktail party, only allow people you know and trust. When users set up a new social networking profile, the tendency is to accept the "default" account settings. For example, when you establish a Facebook account, by default, your name, date of birth, photo, hometown, friend list and *every* post you make are available to more than one billion people.

"Install a security suite like McAfee to guard your systems and cover your data breach bases with a recovery product like EZShield."

Solution: Change your defaults! It only takes minutes to modify every Privacy and Security setting offered by a social network. On a personal level: **1.** Consider limiting who can view your hometown, friend list, family, religious affiliation and interests to *Friends Only*

or even *Only Me*; **2.** Disallow Google to index and share your profile on its search engine; **3.** Businesses will want to leave the indexing feature 'On' to maximize search engine traffic; **4.** Post updates to categories of friends (friend groups), not to the entire world. This isn't only safer personally, it also makes for more targeted and appreciated customer service; **5.** Make sure to update your defaults regularly as social networking sites tend to make frequent changes. Many businesses with Facebook Fan Pages, for example, have not updated their profile in accordance with Timeline, meaning that their page is outdated and unprofessional.

6. Social engineers mine social networks to build trust and exert influence.

The greatest social networking threat inside of your organization isn't malware or information scraping. Your *greatest risk comes from a data spy's ability to get to know you* and your co-workers through your online footprint. Social engineering is the art of manipulating data out of you using emotional triggers such as similarity, likeability, fear of offending, authority, etc. A social engineer's greatest tool of deception is to gain your trust, which is easy once they know your likes, friends and updates that you publish daily. After a month or so of cultivating what appears to be a legitimate relationship, social engineers begin to manipulate you for information.

Solution: Verify, *then* trust. In the information economy, where data is quite literally currency, you must verify someone's intentions and credibility *before* you begin to trust them. Here's how: **1.** Don't befriend strangers; your ego wins, but you lose; **2.** Before you accept a secondhand friend, verify that your existing network *actually* knows and trusts that person. Too many users accept friends indiscriminately, so you need to *investigate* their credibility before you hit the *Accept* button; **3.** Don't believe everything you read on social networking sites. In fact, don't believe anything of substance until you verify it with reputable, primary sources like a national newspaper, ethical blogger or noted expert. **4.** Never send money to a friend in need, download an entertaining app or give away sensitive information via

"Businesses that are unprepared will spend an average of $7.2 million recovering from data breach."

social networking unless you know beyond a shadow of a doubt that the request is legitimate and that your communication is private and secure.

7. In social networking, there are no secrets.

The title of this paper was intentional — people want exclusive access to knowledge that others don't have. We all want to know the secret, and I used that human desire in a gentle form of social engineering to get you to read this article. But in social networking, *there are no secrets*. The instant you hit the post button, *your information becomes public, permanent and exploitable*. It's public because you have little control over how it is forwarded, accessed by others or subpoenaed by law enforcement. In the blink of an eye, your information is backed up, re-tweeted and shared with strangers. Digital DNA has no half-life; it never disappears. And, as you've seen above, it can be used against you.

Solution: Don't just read, act!

Reading is not enough; you must *act on what you have read*. **1.** Revisit the information you over-share on your social networking profiles and remove it. **2.** Modify your account privacy and security defaults so that you share only with the people you trust. **3.** Educate your team from a personal perspective first and then apply it to your organization's needs. **4.** Strategically elevate your defenses by securing your computer network with software like McAfee, and recovery services like EZShield. **5.** Research advanced fraud and social engineering tactics to protect yourself and your company.

Every company I've consulted with that has experienced a data breach wishes that they could "go back in time." Why? Because recovery is often 10-100 times more expensive than prevention, and because data breach causes customer flight, bad press and depreciated value. Companies that prepare for the coming onslaught of social networking fraud will escape relatively unaffected. Businesses that are unprepared will suffer extensively. According to the Ponemon Institute, the *average cost to a business of any size* that experiences a data breach is $7.2 million, which explains why so many small businesses go bankrupt after a data loss event, as they are unable to pay the recovery costs. That gives you 7.2 million reasons to pay attention.

John Sileo is an award-winning author and Risk Management Speaker on the *dark art of deception* and its polar opposite, *the powerful use of trust*. He is CEO of The Sileo Group, which advises clients on maximizing their return on risk, including data theft prevention, social media privacy and fraud training. His clients included the Pentagon, Pfizer & Homeland Security. Sample his Keynote Presentations or appearances on 60 Minutes, Anderson Cooper & Fox.