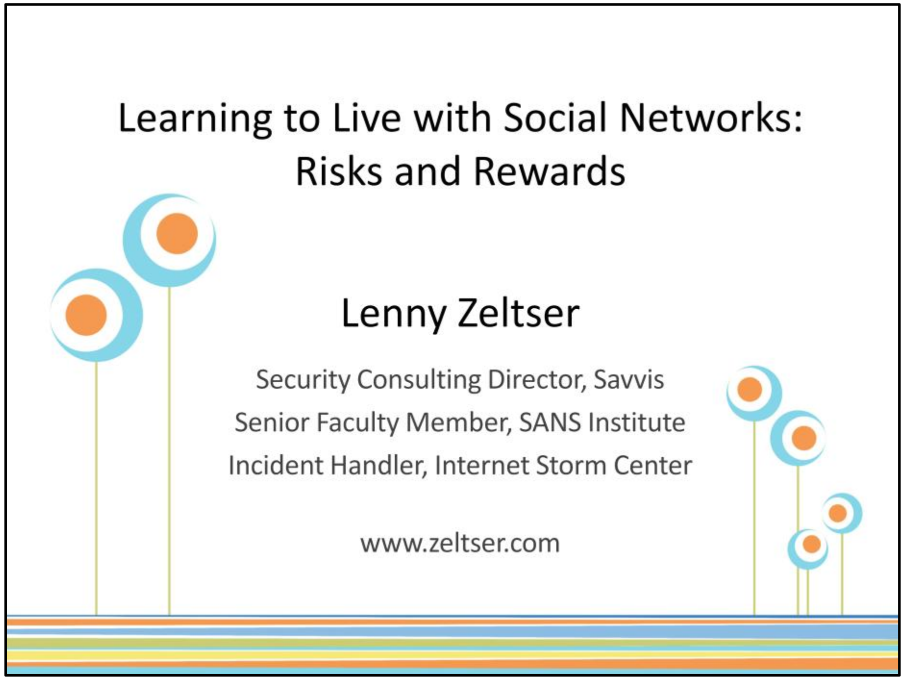


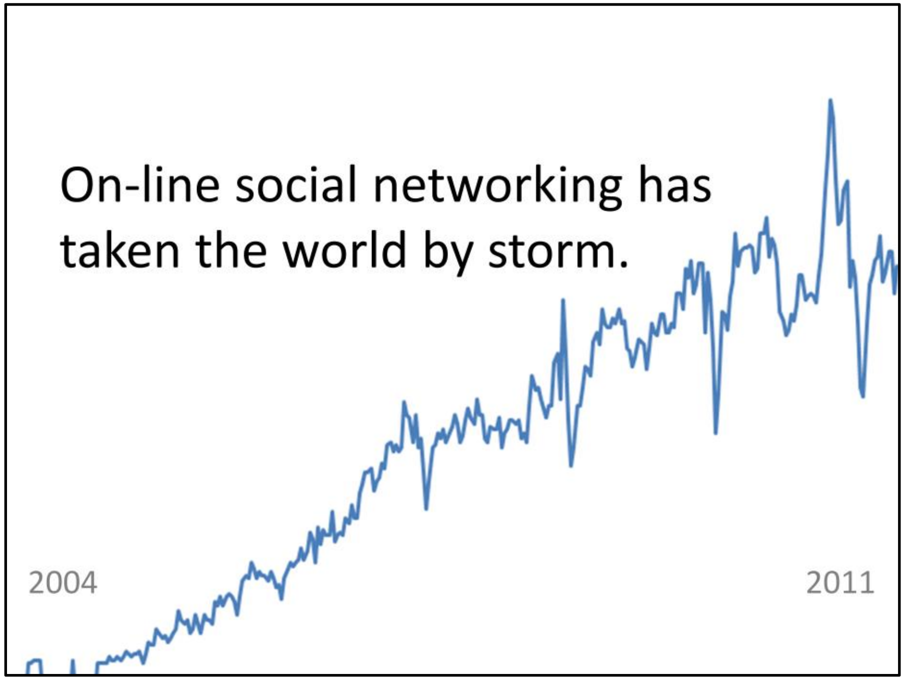
Learning to Live with Social Networks: Risks and Rewards

Lenny Zeltser

Security Consulting Director, Savvis
Senior Faculty Member, SANS Institute
Incident Handler, Internet Storm Center

www.zeltser.com

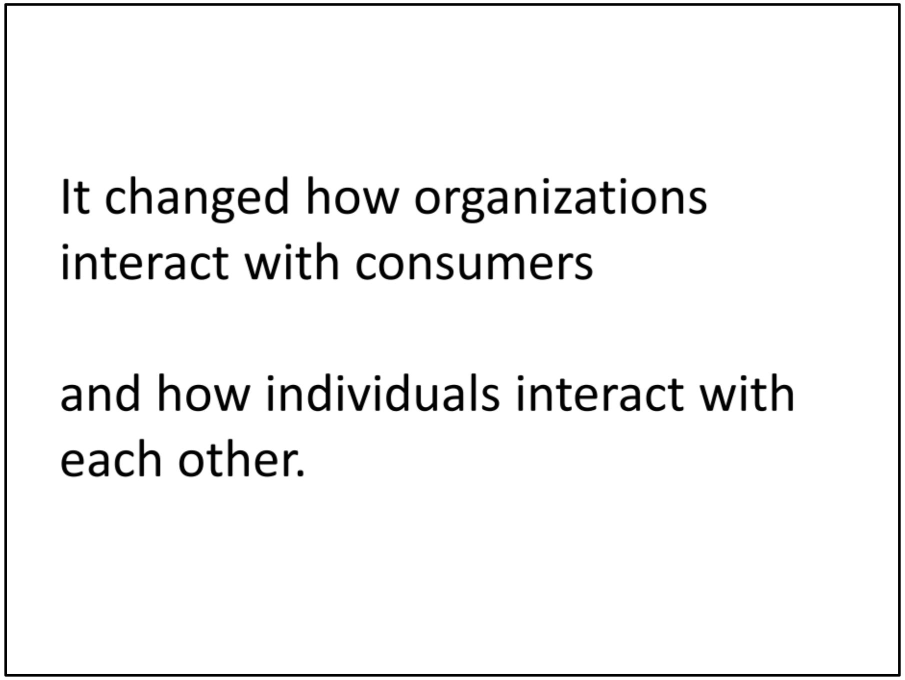
Social networking is a haven for marketers and collaboration between colleagues, but it can put at risk corporate information assets and reputation. Social networking platforms, such as Facebook, Twitter and LinkedIn, are becoming an integral part of people's personal and business worlds. This presentation explores the key risks associated with on-line social networking. It discusses how policies and technologies can aid at mitigating these risks, and how they can also fail at protecting your employees, data, and company. The presentation also addresses how to evaluate the risk of sharing too much information online with the value it brings to the business; is it worth the risk?



On-line social networking has taken the world by storm.

Social networking. It’s on a lot of people’s minds. When I searched Google Trends for the phrase “social networking,” I saw the chart displayed on this slide. The phrase was relatively uncommon in 2004 and its use on the web skyrocketed by 2011. A lot of people are talking about it!

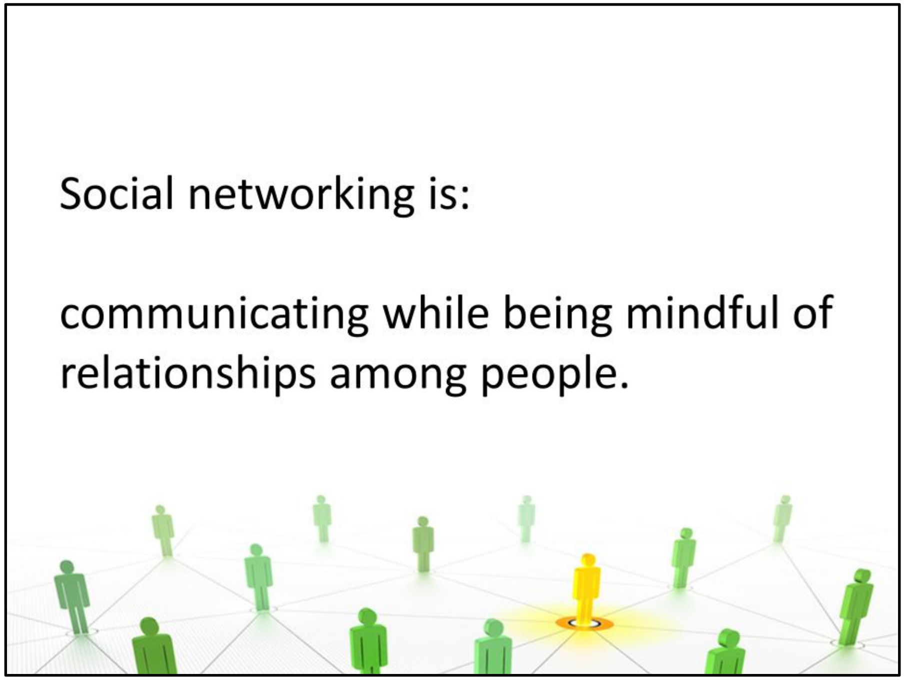
http://www.google.com/trends?q=%22social+networking%22



It changed how organizations interact with consumers

and how individuals interact with each other.

On-line social networking has changed how organizations interact with their customers. It has also drastically changed how individuals interact with each other.



Social networking is:

communicating while being mindful of relationships among people.

Before we discuss the risks of social networking, let’s first agree on what this activity entails. I’ll begin with the definition of the term *social* network, which Wikipedia defines like this:

“A social network is a social structure made up of individuals (or organizations) called ‘nodes’, which are tied (connected) by one or more specific types of interdependency, such as friendship, kinship, common interest, financial exchange, dislike, sexual relationships, or relationships of beliefs, knowledge or prestige.”

This implies that the term social networking means navigating a social network. In other words, *social networking is communicating while being mindful of relationships among people*.

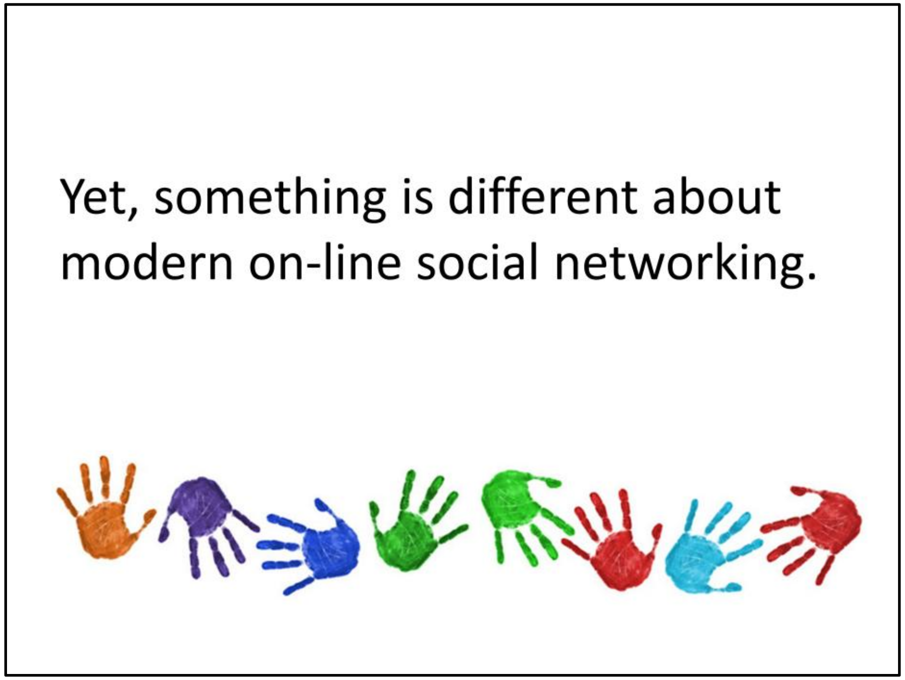
For additional details regarding the definition of social networking, see http://blog.zeltser.com/post/1366016936/definition-of-social-networking

Turns out, we've been social networking for a while.

Humans have been social networking for a long time—probably as long as we've been able to talk to each other. Eventually we learned how to write, and social networking incorporated the practice of sending letters and publishing articles. At some point we learned how to send text by telegraph and how to transmit voice by phone, and social networking took on additional forms.

Were businesses as concerned about data security of social networking when each of these communications methods appeared? I suspect that because businesses relied less on data than they do now, there were fewer information security concerns

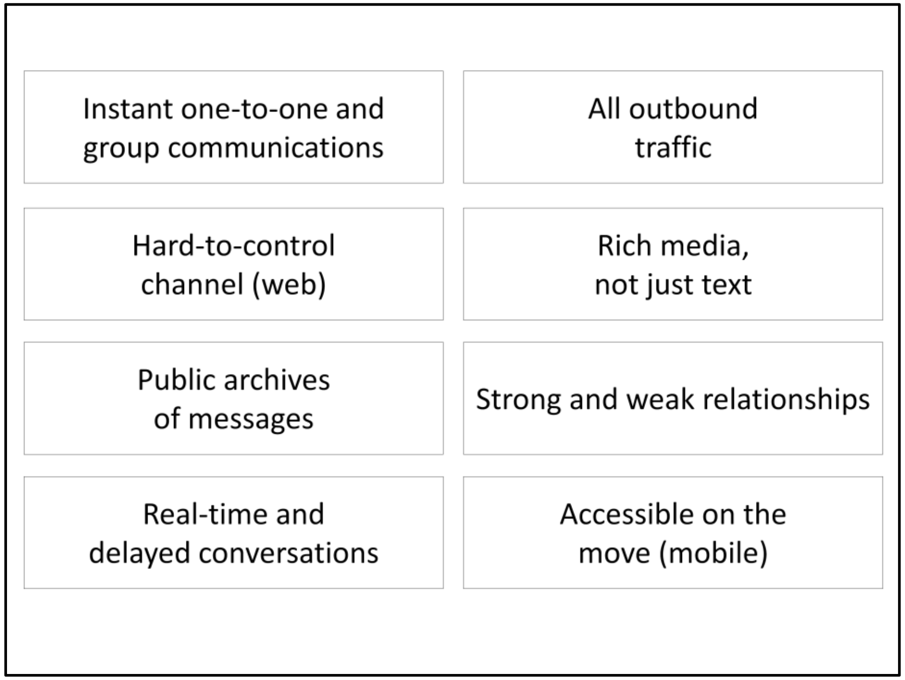
In the more recent times we've been using email to social network with the help of computers. From the information security perspective, this turned out to be a big deal. Email has been an formidable threat vector through which attackers have been sneaking malware past companies' perimeter defenses. The good news is that email has been around for a while, and the security tools and practices are relatively mature for curtailing email threats.



Yet, something is different about modern on-line social networking.

Social media, in the form of blogs and social networking sites such as Facebook and Twitter is the more recent phenomenon. As the result, we’re still trying to understand the risks associated with social networking practices. The technologies and approaches for dealing with the risks are relatively immature as well. This is partially why social network security is a big deal today.

Today’s social networking possesses traits that make it stand out from the earlier forms of social networking…



Instant one-to-one and group communications

All outbound traffic

Hard-to-control channel (web)

Rich media, not just text

Public archives of messages

Strong and weak relationships

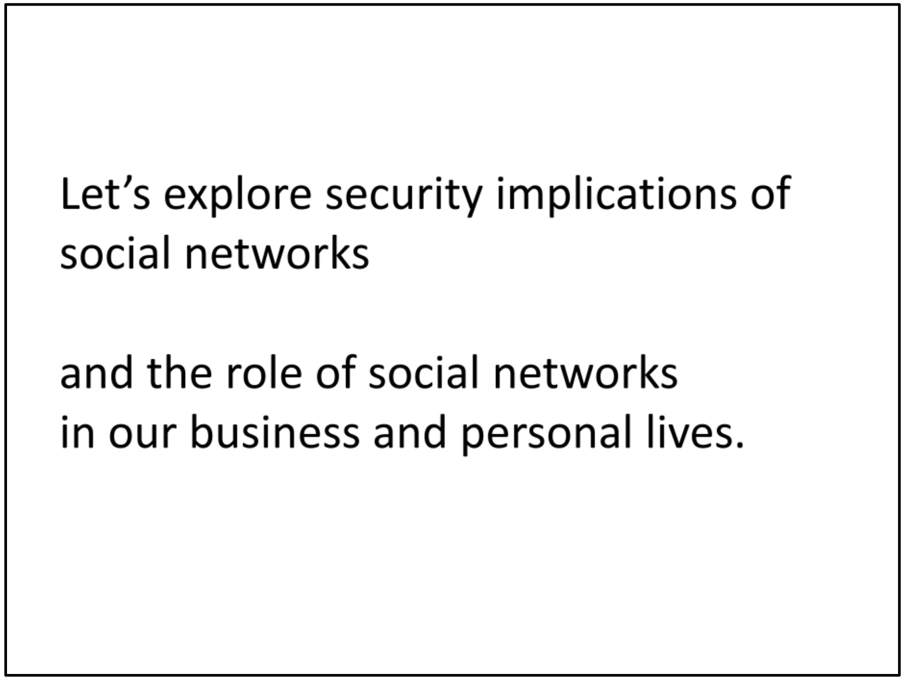
Real-time and delayed conversations

Accessible on the move (mobile)

This slide outlines some of the ways in which on-line social networking differs from the way people have been interacting in the past. Any one of these characteristics might not be special, but together, they describe a platform that allows people to communicate in powerful, exciting, and sometimes risky ways.

Security professionals get nervous about new communication methods.

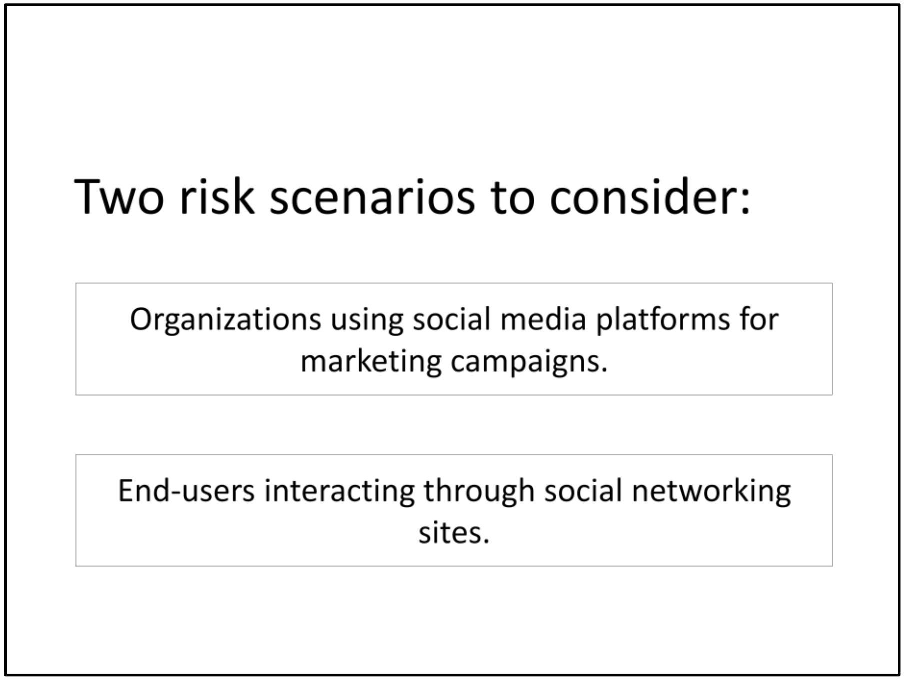
As security professionals, we operate as part of an IT risk management ecosystem and are paid to be cautious. It is natural for us to worry about data controls. This is especially true when the technological and cultural forces that encourage data sharing are ahead of information protection tools and processes.



Let’s explore security implications of social networks

and the role of social networks
in our business and personal lives.

There are good reasons to be concerned about the risk associated with social media and social networking. To understand what can be done about them, it’s important to understand the role that social networking plays in business and personal lives—how people and organizations use it. Only then can we hope to create security controls enable safer on-line social network activities, rather than those that hopelessly attempt to stop the tidal wave of this powerful communication medium.



Two risk scenarios to consider:

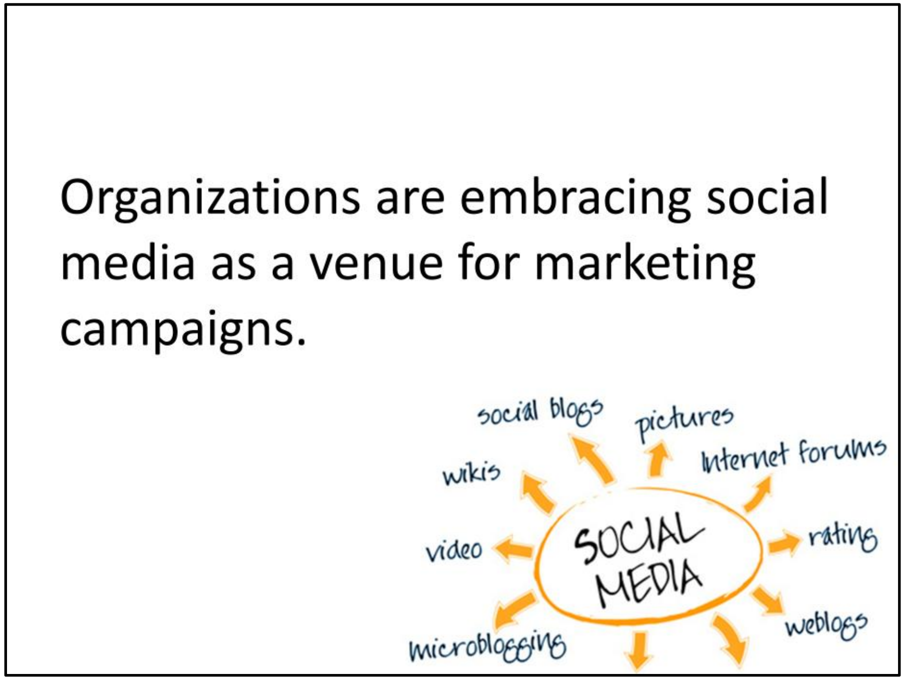
Organizations using social media platforms for marketing campaigns.

End-users interacting through social networking sites.

I’ve been thinking about the various risks associated with social media and social networking. In my mind, the risks fall into two categories in a business setting:

- *Risks as the result of organizations using social media platforms for marketing campaigns.* In this scenario, the organization interacts with consumers on social networking sites, such as Facebook and Twitter, rather that focusing on bringing consumers to the websites under the organization’s direct control. The battle is fought on untrusted turf, if you will. This exposes the organization to several risks, including brand tarnishing, impersonation attacks, and the use of vulnerable IT infrastructure.

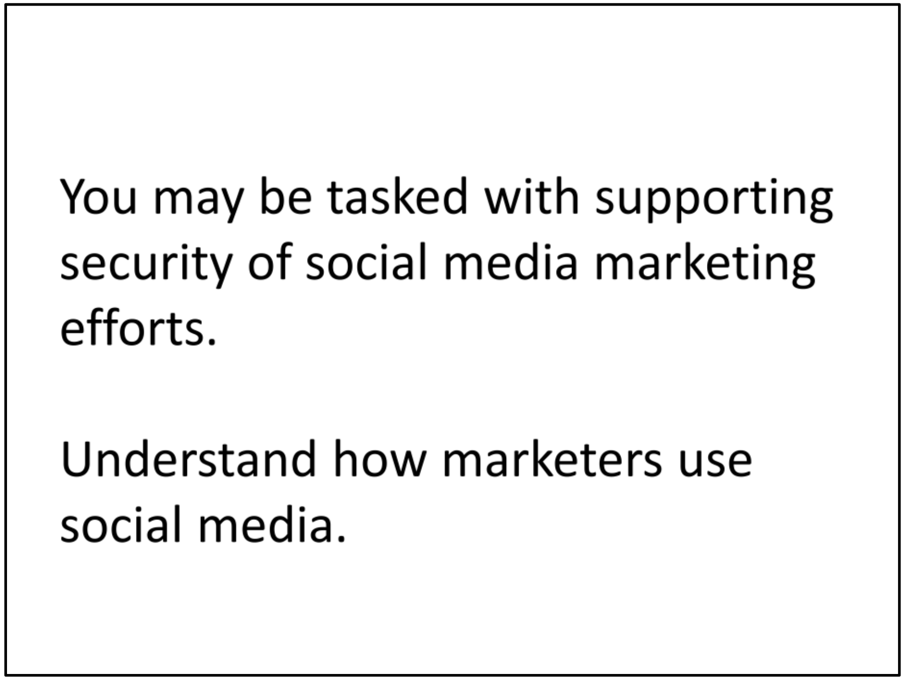
- *Risks as the result of end-users interacting through social networking sites.* In this scenario, the users of social networks are at risks due to the link-sharing culture of such sites, whereby they may be targeted by malicious websites and may be social engineered into installing malware or into giving up sensitive data. The organizations are also at risk when the employees inadvertently leak proprietary, regulated or otherwise sensitive information. Related risks are situations where employees reveal personal data that can be used to attack the individuals or their employers.



Organizations are embracing social media as a venue for marketing campaigns.

SOCIAL MEDIA
social blogs
pictures
Internet forums
wikis
rating
video
weblogs
microblogging

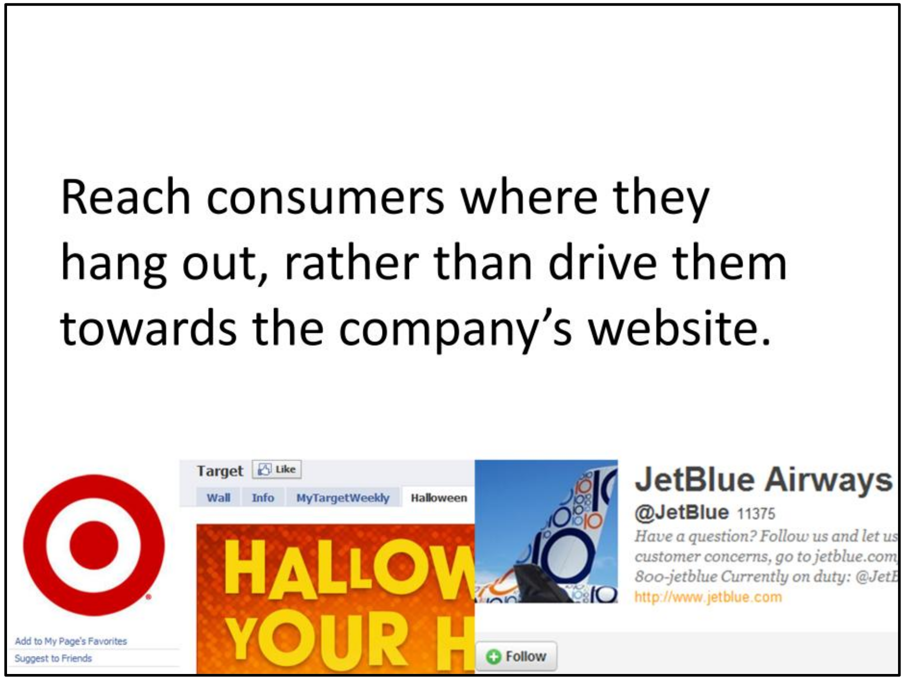
If you have information security responsibilities, you need to think not only of how your employees interact with social networks as end-users, but also how your marketers use social media to interact with your customers. Your organization probably has a marketing team that is either planning to or is already using social media.



You may be tasked with supporting security of social media marketing efforts.

Understand how marketers use social media.

As an information security professional, you may be tasked with supporting the social media marketing efforts of your organization or of your clients. You need to understand how the organization—usually its marketing department—is using social media before you attempt to identify and help mitigate the associated risks.

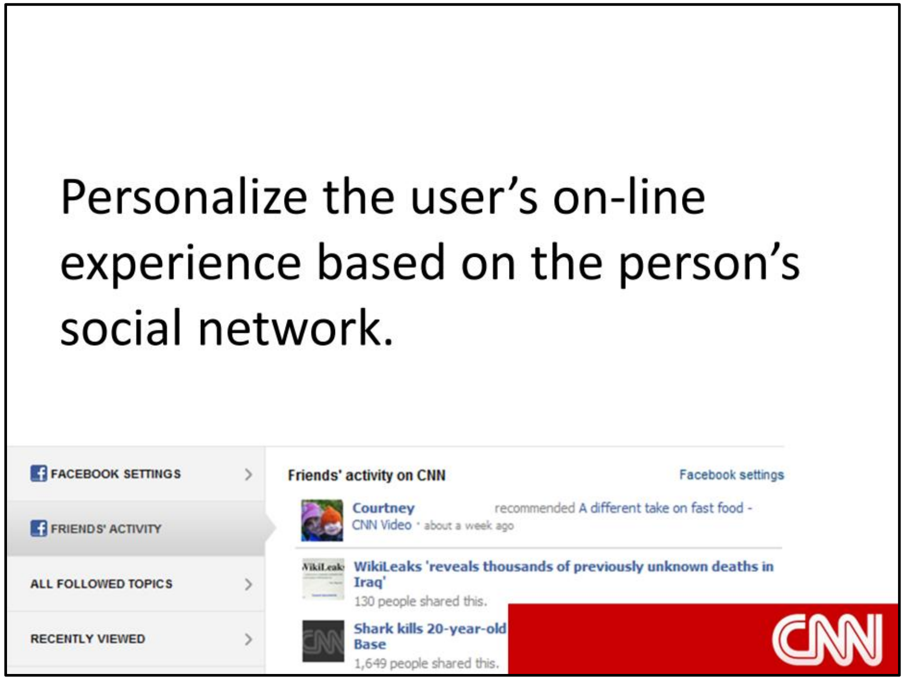


Reach consumers where they hang out, rather than drive them towards the company's website.

Target
Like
Wall
Info
MyTargetWeekly
Halloween
HALLOW
YOUR H
Add to My Page's Favorites
Suggest to Friends
JetBlue Airways
@JetBlue 11375
Have a question? Follow us and let us
customer concerns, go to jetblue.com
800-jetblue Currently on duty: @JetB
http://www.jetblue.com
Follow

Social media campaigns allow the organization to interact with its customers on social networks—to go where the customers are—rather than bring the customers to the organization's own website. This is drastically different from the way marketing used to work a few years ago. As the result, the business processes associated with social media marketing are as new as the understanding of the risks tied to such on-line interactions.

Incorporating social media into marketing campaigns provides organizations with opportunities for exposing the brand to customers, directly on social networks and by improving search engine rankings.



Personalize the user's on-line experience based on the person's social network.

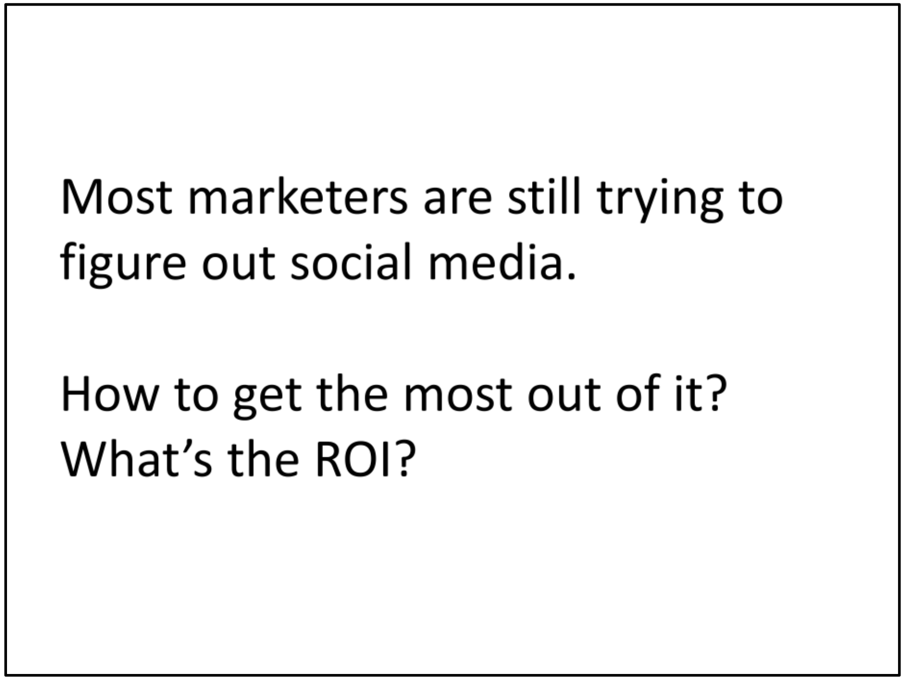
Friends' activity on CNN

Courtney recommended A different take on fast food - CNN Video · about a week ago

WikiLeaks 'reveals thousands of previously unknown deaths in Iraq'
130 people shared this.

Shark kills 20-year-old
Base
1,649 people shared this.

Another way in which organizations use social media is by tapping into the customer's social network to customize content or other aspects of the person's browsing experience. For instance, when you visit CNN.com, website might present you with CNN-related activities from your Facebook social network. Now you're not merely reading the news that CNN's editors thought you might like—instead, you are interacting with content that is directly relevant to you.

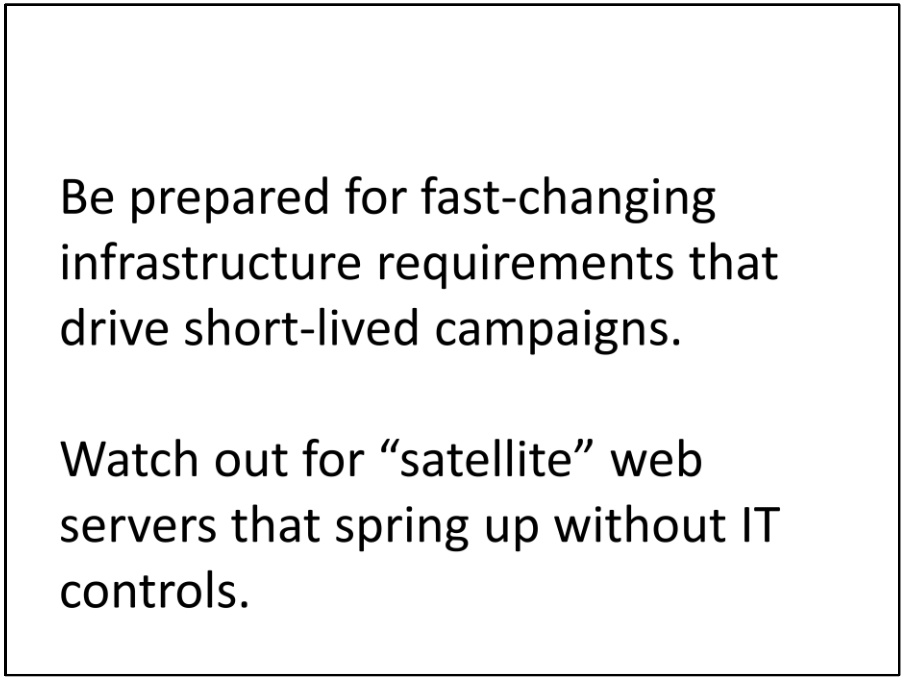


Most marketers are still trying to figure out social media.

How to get the most out of it? What’s the ROI?

A good starting point for learning about the role that social media and social networking plays in marketing is the 2010 Social Media Marketing Industry Report. (http://www.socialmediaexaminer.com/social-media-marketing-industry-report-2010)

The research data, presented in the report, supports the following point: Most marketers are new to the world of social media and are still trying to figure out how to best use it. Many are also looking for ways to measure the Return on Investment (ROI) of social media campaigns.

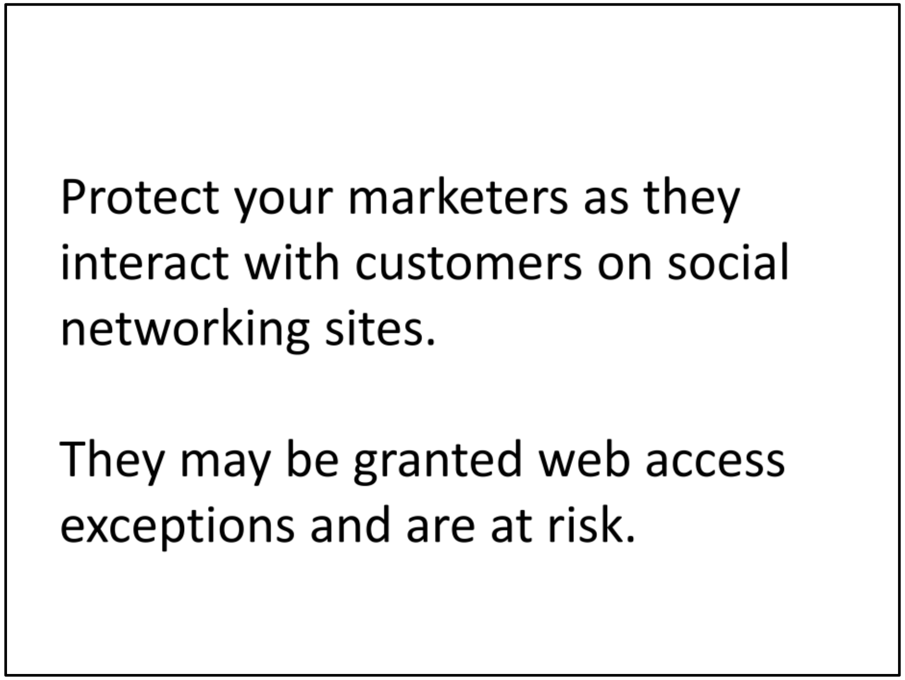


Be prepared for fast-changing infrastructure requirements that drive short-lived campaigns.

Watch out for “satellite” web servers that spring up without IT controls.

Your organization’s marketers may change tactics quickly, trying campaigns and abandoning approaches that don’t seem to work. Information security personnel needs to be prepared to handle fast-changing infrastructure requirements that might drive these short-lived campaigns.

Also, watch out for satellite web servers: Social media marketing campaigns are likely to be fast-conceived. In addition to making use of social networking sites, they may need to set up landing pages on satellite web servers. If your organization’s IT department cannot set up these servers quickly, marketers might take it upon themselves to provision the websites elsewhere. The satellite servers outside of your control, if compromised, will adversely affect your organization’s security posture by leaking data, undermining good will, weakening compliance efforts, and so on.

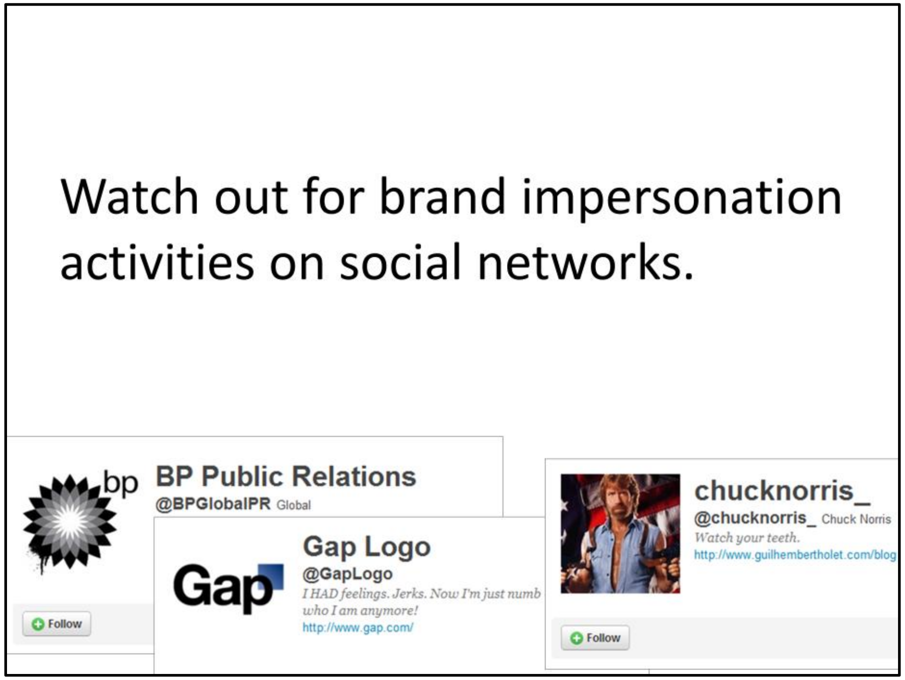


Protect your marketers as they interact with customers on social networking sites.

They may be granted web access exceptions and are at risk.

Marketers who conduct social media marketing campaigns need to have access to social networking sites, such as Facebook, Twitter and LinkedIn. According to the 2010 Social Media Marketing Industry Report, it’s not uncommon for marketers with social media experience to spend 10 hours per week on social media efforts.

Organizations who restrict access to social networking sites will probably need to create exceptions for designated marketing personnel. As the result, marketers may be at a greater risk of being attacked through social networks (e.g., phishing, data leakage, malicious links, etc.).



Watch out for brand impersonation activities on social networks.

BP Public Relations
@BPGlobalPR Global

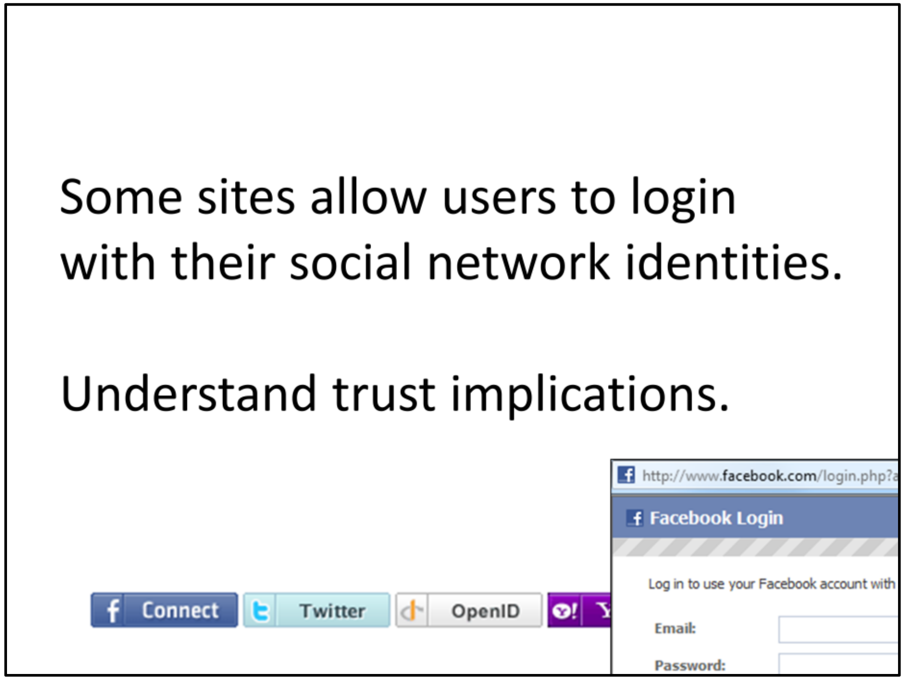
Gap Logo
@GapLogo
I HAD feelings. Jerks. Now I'm just numb who I am anymore!
http://www.gap.com/

chucknorris_
@chucknorris_ Chuck Norris
Watch your teeth.
http://www.guilhembertholet.com/blog

Organizations might be impersonated by attackers on social networking sites to target the organizations' customers. A fraudulent marketing campaign on a social networking site might look like it is conducted by the organization, but it might actually be led by someone else. In the style of phishing, impersonation incidents put the organization's customers' data at risk, and may tarnish the firm's reputation. As far as I can tell, these Twitter accounts are fake:

- BPGlobalPR: Set up during the gulf oil spill in 2010 to satirize and criticize the situation. Around 175,000 followers. While the official BP account BP_America has around 26,000 followers.
- ChuckNorris_: Around 24,000 followers. Spreads the humorous meme about Chuck Norris' super powers.
- GapLogo: Around 4,500 followers. Set up in 2010 when Gap attempted to change its logo design to satirize and critique the new logo.

For more thoughts about on-line brand impersonation activities and risks see http://isc.sans.edu/diary.html?storyid=9952



Some sites allow users to login with their social network identities.

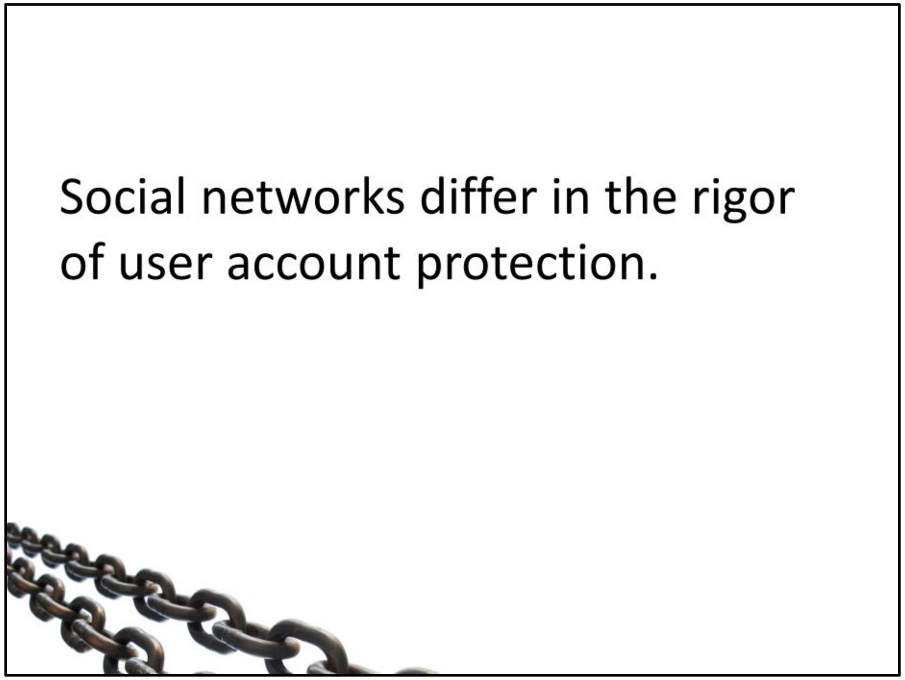
Understand trust implications.

Connect
Twitter
OpenID
http://www.facebook.com/login.php?a
Facebook Login
Log in to use your Facebook account with
Email:
Password:

Some organizations allow the their customers to authenticate to their favorite social networking site, and use that identity to access personalized content on the organization's own website. Facebook for Websites is one platform that delivers such capabilities; it was designed to "make your website more personalized and social." (http://developers.facebook.com/docs/guides/web)

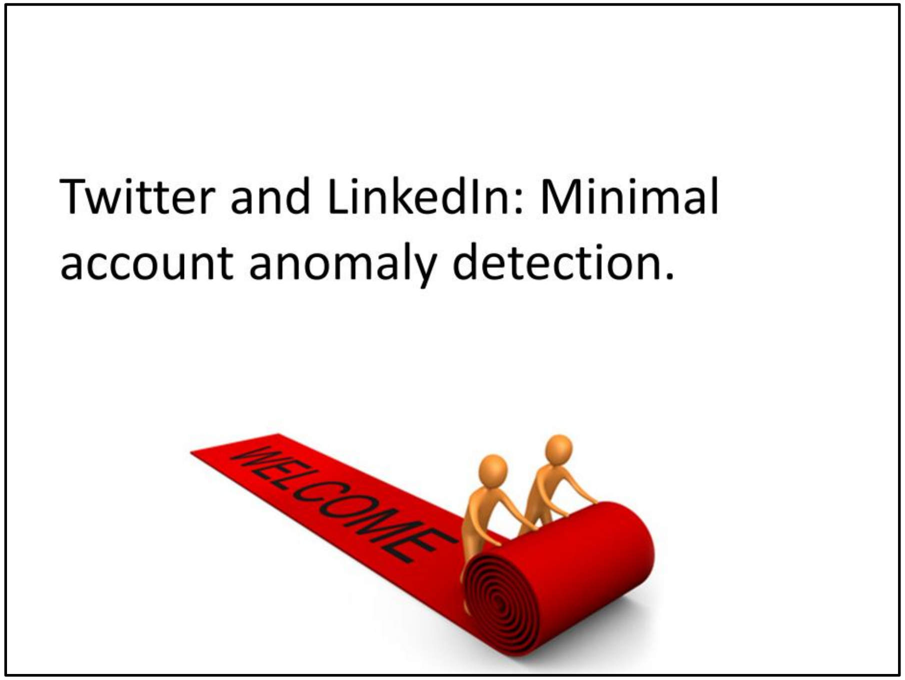
On the one hand, it's attractive not to have to worry about properly implementing authentication and about storing logon credentials. On the other hand, organizations lose control over authentication when relying on identity attestation provided by a third party, such as Facebook.

For details about "Sign-in with Twitter," which also offer an opportunity for sites to delegate authentication, see http://hueniverse.com/2009/04/introducing-sign-in-with-twitter-oauth-style-connect.



Social networks differ in the rigor of user account protection.

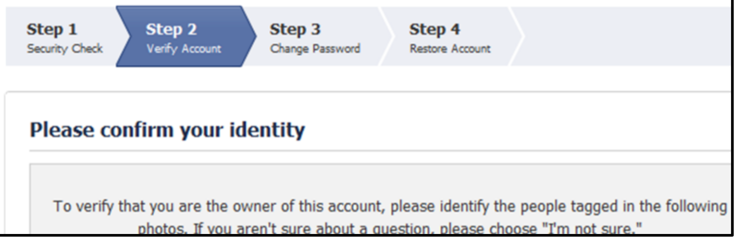
If your organization has a website that delegates authentication to a social networking platform, keep in mind that not all social networks apply the same rigor to protecting and authenticating user accounts. As the result, you might consider some social networking sites' authentication attestation more reliable than others'...



Twitter and LinkedIn: Minimal account anomaly detection.

LinkedIn seems to offer little in the way of automatically detecting when a user account has been compromised. Twitter seems to have some controls built in, as part of its effort to curtail Twitter spam. However, both of these popular networks are falling behind Facebook in their measures to protect user accounts.

Facebook implemented “social CAPTCHA” challenges for anomalous access.



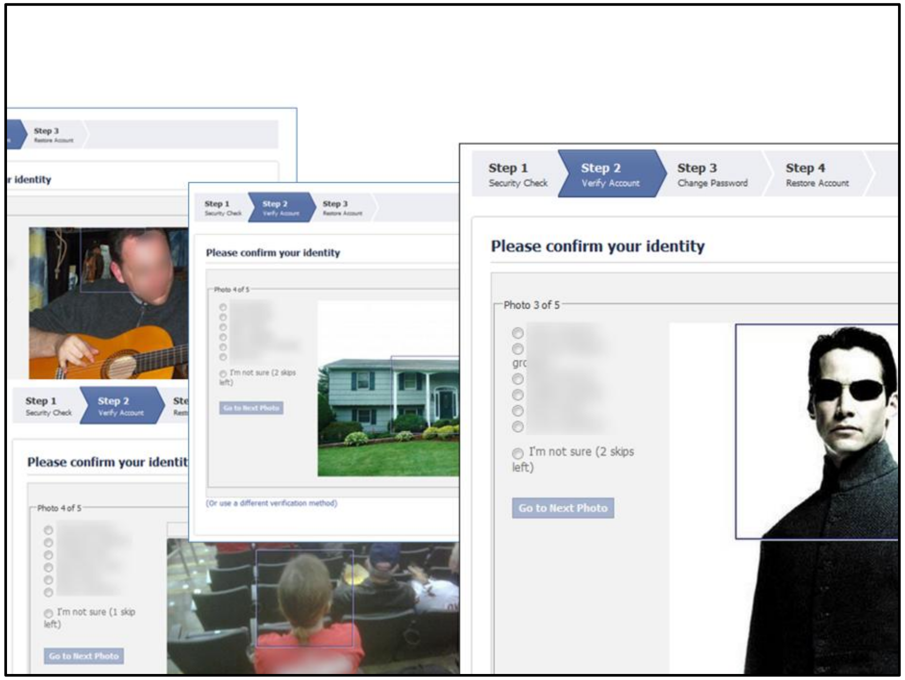
Please confirm your identity

To verify that you are the owner of this account, please identify the people tagged in the following photos. If you aren't sure about a question, please choose "I'm not sure."

Facebook implements a mechanism known as “social CAPTCHA” to authenticate user accounts that are considered at risk. While CAPTCHA is traditionally used to distinguish between humans and bots, Facebook’s method is designed to distinguish legitimate users from impostors. It does this by asking questions about the user’s social network.

Facebook prompts the user to authenticate using the “social CAPTCHA” approach if the site notices an anomaly in the way the person is logging in. In one such case, Facebook states: “You are signing in from a location we’re not familiar with. For your protection, please take a moment to answer a few security questions.” The user is then presented with an option to answer their predefined secret question or to identify photos of their friends.

If the user selects the photo option, they are asked to successfully tag photos of 5 friends. Facebook presents one or two photos of a friend per page, and lists 5 multiple-choice options of that person’s name; each choice is a name of the user’s Facebook friend. The user needs to select the name of the pictured friend to proceed.

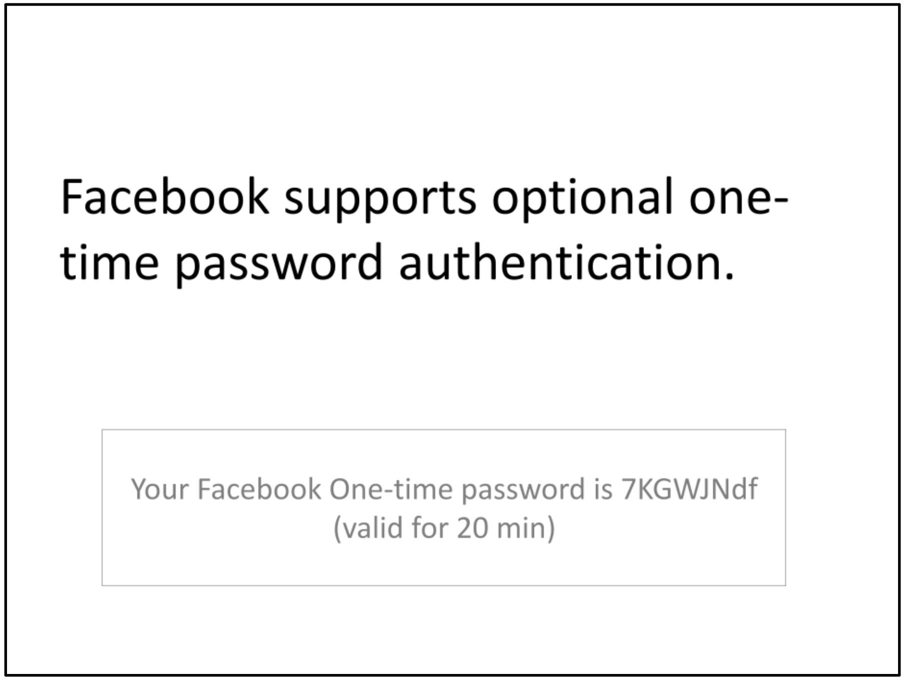


This slide presents a few photos that a Facebook user might be presented with when dealing with "social CAPTCHA." (I obscured people's faces and names—the faces and names actually displayed on Facebook aren't obscured.)

As you can see, sometimes identifying your friend can be tricky. For instance, the friend might not be in the picture at all (presumably the person lives in the house pictured here). Or the friend can be pictured from behind.

It's great to see Facebook providing an innovative way to authenticate users beyond asking the standard "mother's maiden name" questions in situations where a mere password is insufficient.

The photo-based "social CAPTCHA" feature means that by incorrectly tagging people, users of Facebook undermine others' chances at correctly answering the photo challenges. It also means that you should be careful when "friending" people if you don't know them or, at least, if you don't know how they look.



Facebook supports optional one-time password authentication.

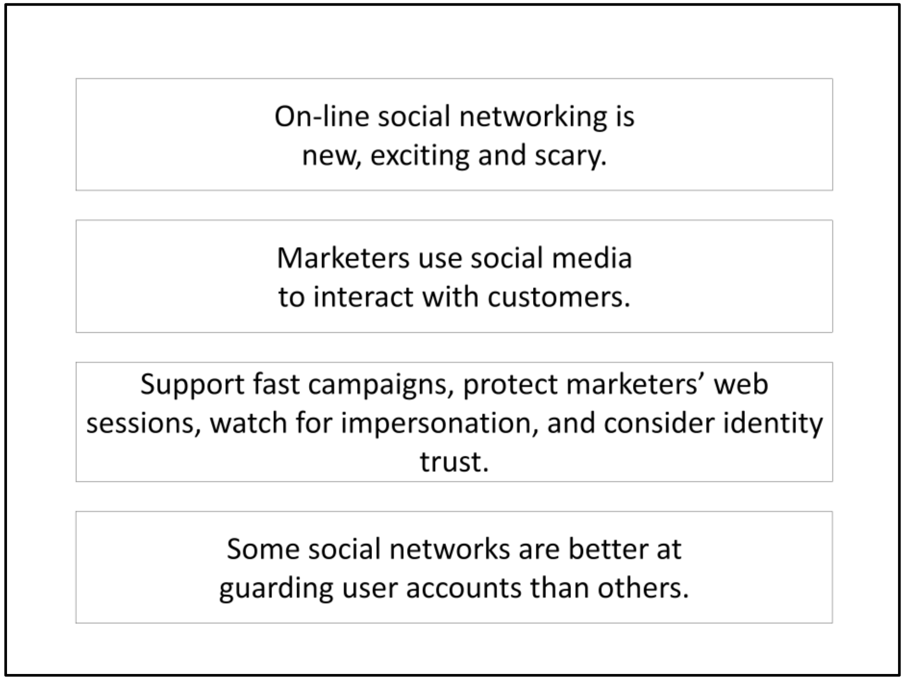
Your Facebook One-time password is 7KGWJNdf (valid for 20 min)

Facebook also allows its users to use one-time passwords (OTP) for authentication. The optional feature allows security-conscious Facebook users to request a one-time password prior to logging in from an untrusted system, such as an Internet kiosk.

If your mobile number is registered with Facebook, you can request a one-time password by texting the letters “otp” to 32665 (FBOOK) from your mobile phone. Facebook will respond with a message like the one shown on this slide. You can now use the specified one-time password instead of your regular password to login to Facebook within the next 20 minutes.

Because this feature is optional, it is unlikely to be used by many people. However, it is good to see Facebook thinking along the lines of strengthening controls around its user accounts.

Overall, though, the OTP feature is not as useful as it might appear. For details, see http://blog.zeltser.com/post/1319041093/why-facebook-one-time-passwords



On-line social networking is new, exciting and scary.

Marketers use social media to interact with customers.

Support fast campaigns, protect marketers’ web sessions, watch for impersonation, and consider identity trust.

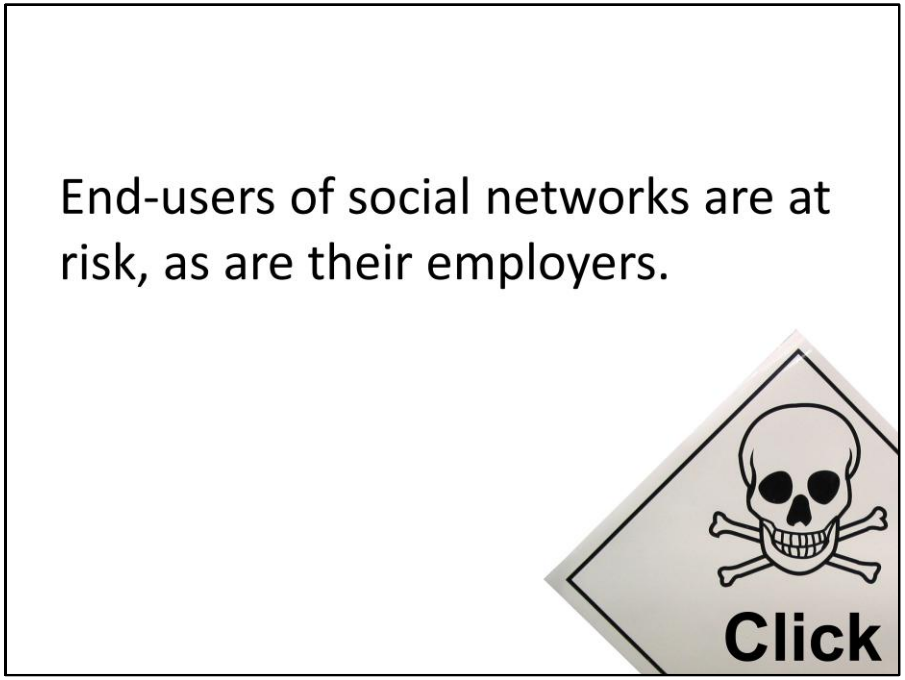
Some social networks are better at guarding user accounts than others.

Time for a check point.

We began by outlining the reasons why social networking is an old concept that has evolved into something new due to the arrival of the web and social networking sites. The world of on-line social networking is filled with promise. Yet, because it is in many ways a new paradigm for social interactions, it carries a number of risks.

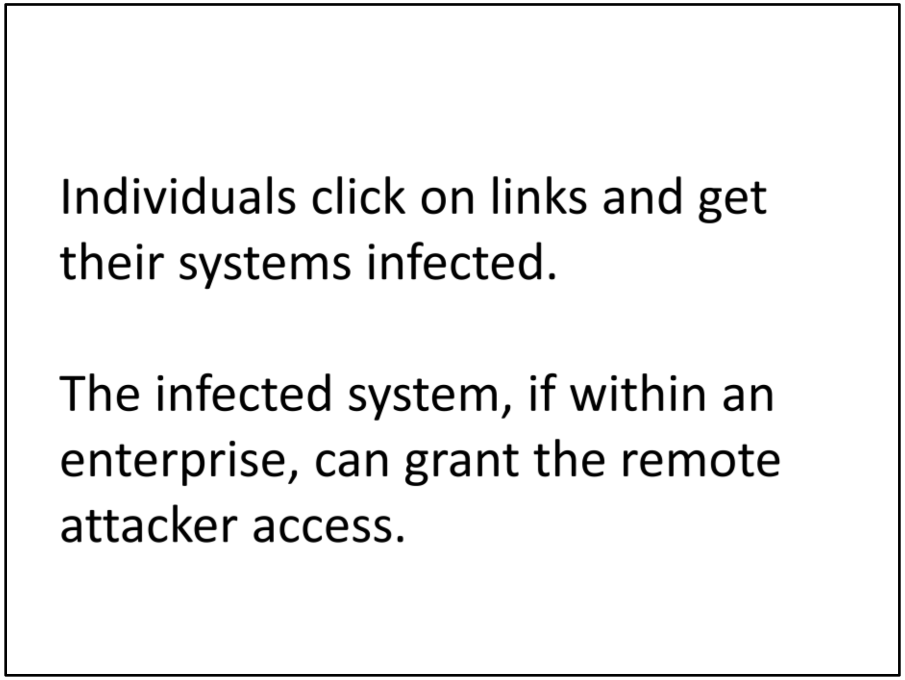
We discussed how marketers are starting to use social media to spread the reach of their brands and interact with consumers outside of the company’s own website. I encouraged you to become familiar with your organization’s marketing activities, so you can be prepared to support rapid on-line marketing campaigns, help protect your company’s brand and safeguard marketers from the exposure to on-line social networking threats.

We also touched upon the practice of delegating user authentication to social networking sites. I pointed out that some social networks are better at guarding user accounts than others.



End-users of social networks are at risk, as are their employers.

The next category of risks I'd like to explore are those involve end-users of social networking sites placing themselves, as well as their employers, at risk as the result of their social networking activities.



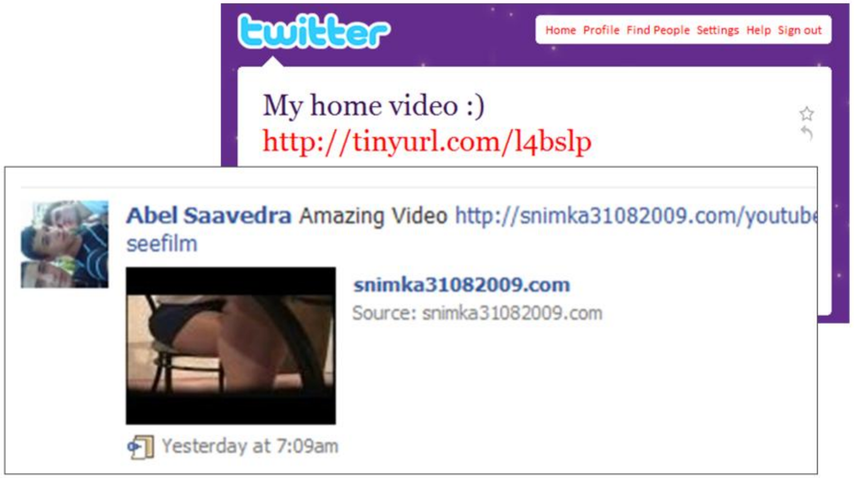
Individuals click on links and get their systems infected.

The infected system, if within an enterprise, can grant the remote attacker access.

People are social creatures. We like to exchange information and share experiences. In the world of email, these tendencies often entail sending email with attachments of documents and photographs, and also sharing links to sites we find useful or exciting. Because email is allowed to go through most network security perimeters, attackers send emails to their victims, too, tricking them into opening attachments and clicking on links that lead to malicious websites.

In the world of on-line social networking, people share links... A lot. If you are following a friend on Twitter, LinkedIn or Facebook, you are likely to click on the link that your friend shares, because you trust his taste and recommendations. Unfortunately, your friend might inadvertently share a link to a malicious website; alternatively, his account might have been compromised and is being used to spread malicious links.

If the user gets infected as the result of following a link on a social networking site, the remote attacker might be able to gain control over the user's system and use it for further attacks.



My home video :)
http://tinyurl.com/l4bslp

Abel Saavedra Amazing Video http://snimka31082009.com/youtube
seefilm

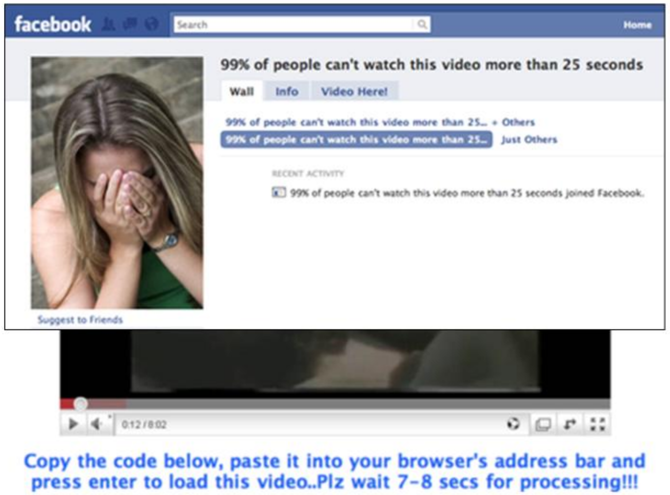
snimka31082009.com
Source: snimka31082009.com

Yesterday at 7:09am

Koobface propagation

An example of malware that propagated using social networking sites is Koobface . It spread by including links to malicious websites in Twitter and Facebook profiles. Once the potential victim clicked on the link, he or she was typically directed to a website that attempted to trick the person into installing malware. A common tactic involved presenting the user with a message that to view the video, a Flash Player upgrade was required. Of course, the executable the person was presented was not Flash Player, but was malware.

For additional details about malware that distributes links through social networking sites, see:
http://blog.zeltser.com/post/2794828444/malicious-links-on-social-networking-sites



99% of people can't watch this video more than 25 seconds

99% of people can't watch this video more than 25... + Others

99% of people can't watch this video more than 25... Just Others

RECENT ACTIVITY

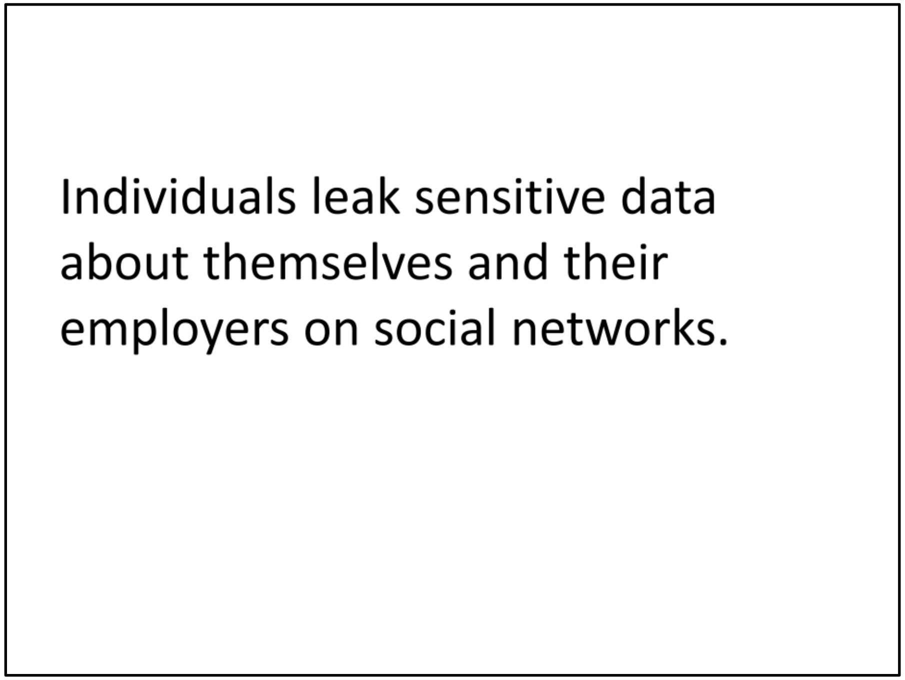
99% of people can't watch this video more than 25 seconds joined Facebook.

Copy the code below, paste it into your browser's address bar and press enter to load this video..Plz wait 7-8 secs for processing!!!

Source: AVG

In another example of malware spreading through Facebook, malware dared victims to click the link to get them hooked. It then asked the person to copy and paste JavaScript—this action hijacked the person’s Facebook session and used it to spread this malware to the person’s Facebook friends. (See http://thompson.blog.avg.com/2010/07/remote-control-facebook.html)

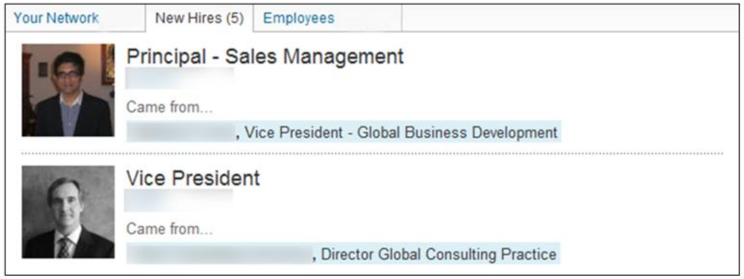
According to AVG, “you are taken to a page which automatically tells all your friends that you like the app, and it posts that link to your status.”



Individuals leak sensitive data about themselves and their employers on social networks.

Another way in which users of social networking sites put themselves and their organizations at risk is by leaking sensitive data. This usually occurs without the person realizing that they are engaging in risky behavior, because an individual fact in itself might not constitute sensitive data. However, taken in aggregate, bits of information can be used for malicious purposes.

Data aggregated by LinkedIn is useful for social engineering.

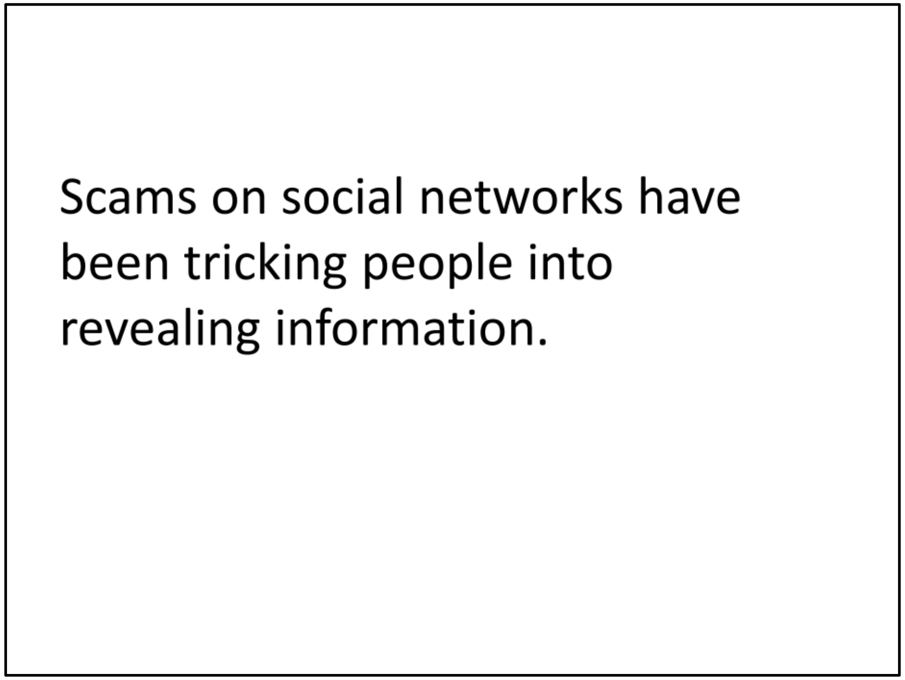


Principal - Sales Management
[redacted]
Came from...
[redacted], Vice President - Global Business Development

Vice President
[redacted]
Came from...
[redacted], Director Global Consulting Practice

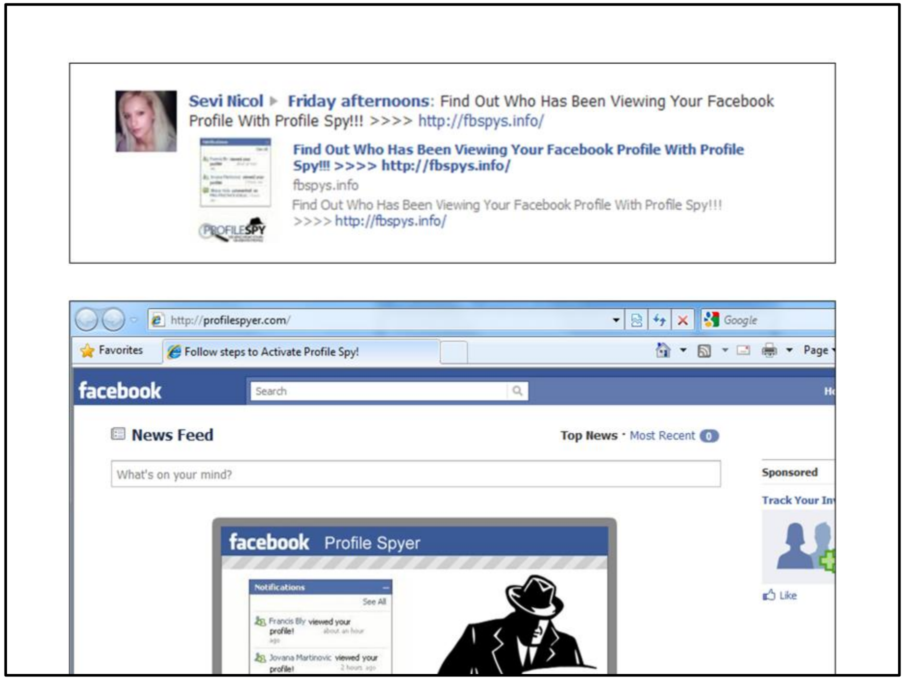
For example, LinkedIn automatically generates a company profile based on the information provided by the company's current and former employees. For instance, when a person joins a company, he might update his LinkedIn profile to reflect the job change. An attacker can see who is joining the targeted organization by going to that company's LinkedIn profile. This can be useful information: in particular, new hires are prime targets for social engineering, because they don't know much about the new organization and are very open to new connections and experiences.

For details about how LinkedIn can be used for profiling companies, see https://isc.sans.edu/diary.html?storyid=4213



Scams on social networks have been tricking people into revealing information.

Social networks are a fertile ground for scams that trick people into revealing sensitive data. This is, in part, because people tend to be in the open frame of mind when socializing on these sites. This is also partly the case because sharing information subtly is encouraged in the context of social networking sites, such as Facebook.



Sevi Nicol ▸ Friday afternoons: Find Out Who Has Been Viewing Your Facebook Profile With Profile Spy!!! >>>> http://fbspys.info/

Find Out Who Has Been Viewing Your Facebook Profile With Profile Spy!!! >>>> http://fbspys.info/

fbspys.info

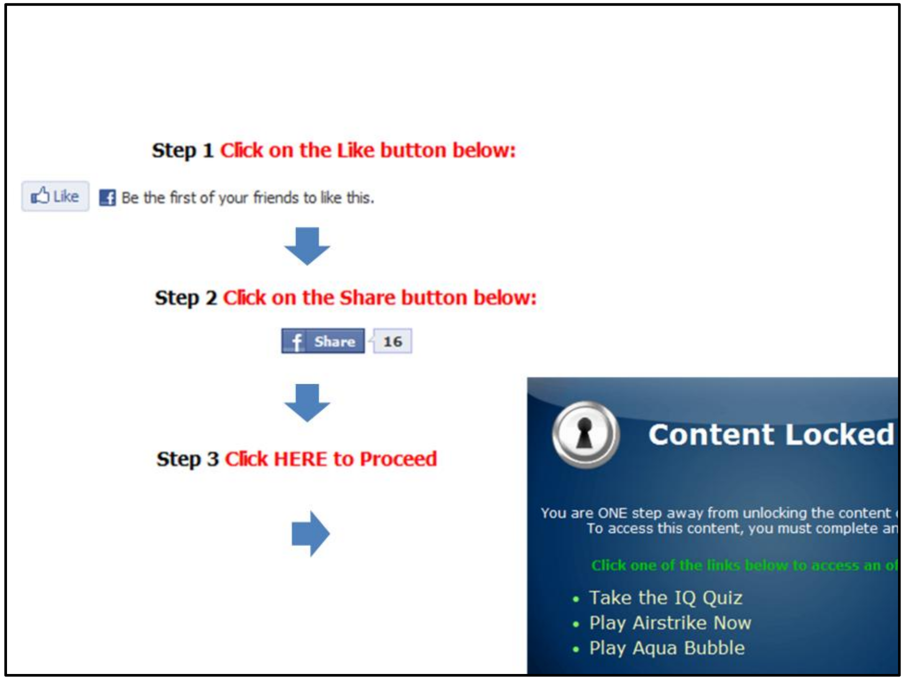
Find Out Who Has Been Viewing Your Facebook Profile With Profile Spy!!! >>>> http://fbspys.info/

Francis Bly viewed your profile! about an hour ago

Jovana Martinovic viewed your profile! 2 hours ago

Consider a scam that promises Facebook users to find out who has been viewing their Facebook profile. The implication is that the user can get access to these details (that feed the narcissist in all of us) by installing the Profile Spy application.

The scam attempts to trick the victim into revealing personal details, including a mobile phone number. The malicious site shows a fake Facebook page in the background, to make victims think they are within the "walled garden" of Facebook…



Step 1 Click on the Like button below:

Be the first of your friends to like this.

Step 2 Click on the Share button below:

Step 3 Click HERE to Proceed

Content Locked

You are ONE step away from unlocking the content
To access this content, you must complete an

Click one of the links below to access an of

- Take the IQ Quiz
- Play Airstrike Now
- Play Aqua Bubble

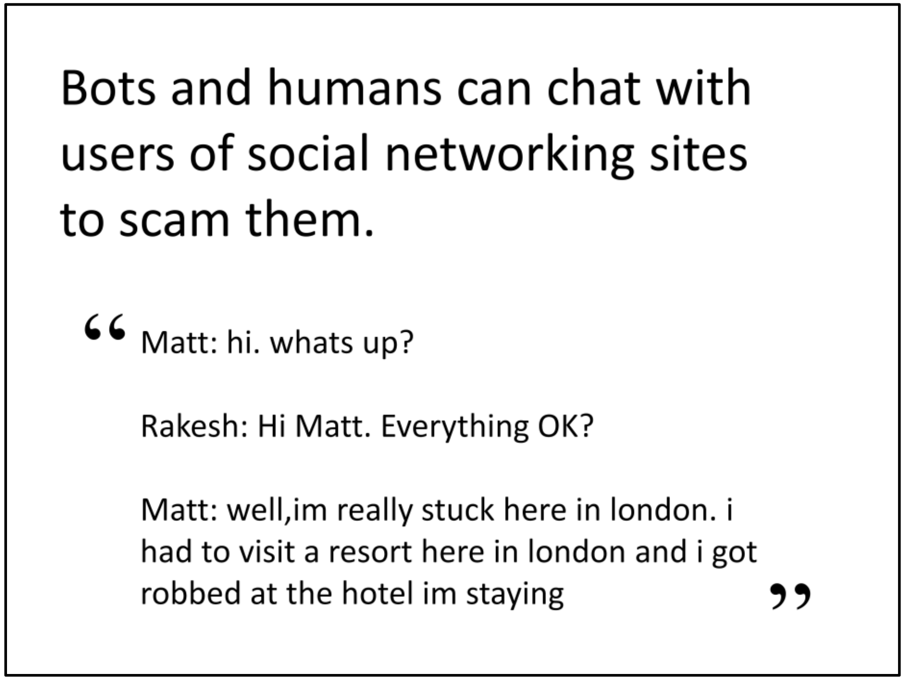
Under the promise of providing the magical Profile Spy application, the scammer’s website requests that the user click the Like button. This helps promote the Facebook page set up for the Profile Spy application, because the more people “liked” the page, the more legitimate it appears to future victims.

The site also requests that the person click the Share button. This shares the link to the Profile Spy website with the victim’s friends on Facebook.

Lastly, the person is asked to fill out some surveys that ask for contact information and other details to, presumably, sell that data to third parties.

The promise of the Profile Spy application is never fulfilled, sorry.

For links to more perspectives on the Profile Spy scam, see: http://blog.zeltser.com/post/1137736287/profile-spy-scams-on-facebook



Bots and humans can chat with users of social networking sites to scam them.

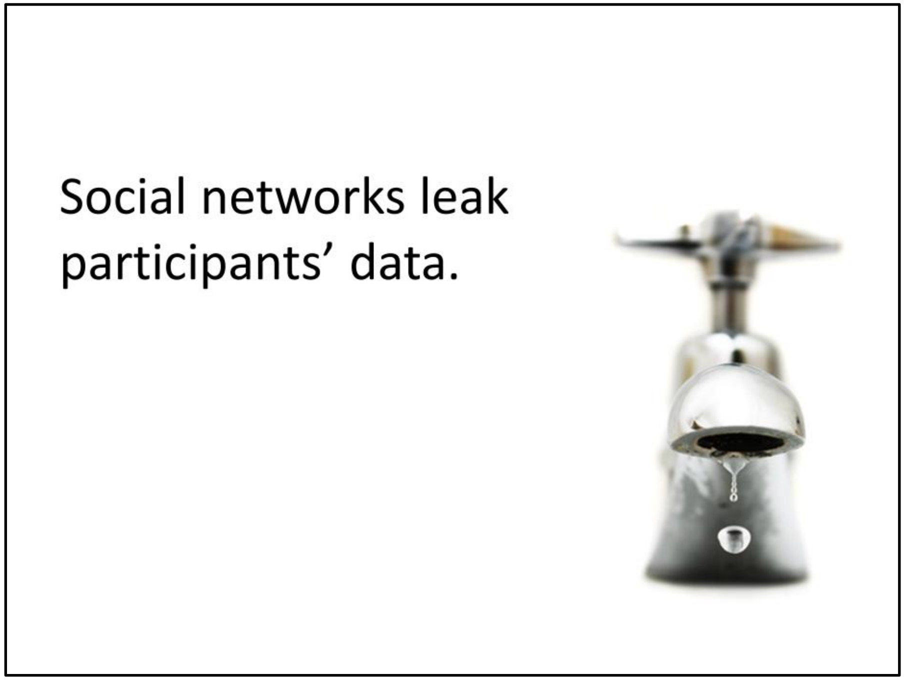
> “Matt: hi. whats up?
>
> Rakesh: Hi Matt. Everything OK?
>
> Matt: well,im really stuck here in london. i had to visit a resort here in london and i got robbed at the hotel im staying”

With low-cost labor available throughout the world, scammers can employ humans for chatting with victims on social networking sites while keeping their costs relatively low.

One example of this was documented by Rakesh Agrawal, who described the classic “I’m stuck in London scam” that was conducted via Facebook chat. The scammer used a compromised Facebook account in an attempt to solicit emergency funds from the victim’s friend. The excerpt from the transcript is on this slide.

The scammer was using Matt’s Facebook account and, as far as I can tell, was a human being. However, such interactions could have easily been automated using a chat bot.

For additional details regarding this, see: http://blog.zeltser.com/post/2822651353/bots-chatting-on-social-networks

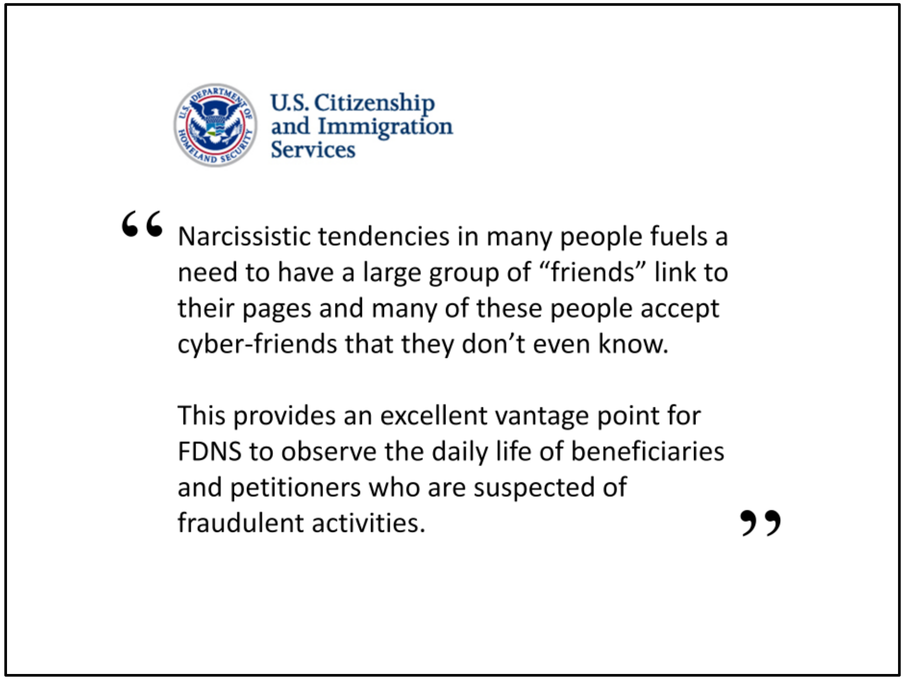


Social networks leak participants’ data.

Users of social networking sites are often to blame for putting themselves at risk by clicking on links or by sharing sensitive information. However, social networking sites themselves have been known to leak the data of their users.

These leaks can take the form of the social networking site providing a feature that is misunderstood by its users: for instance, the users might not understand who has access to their photos or status updates.

The leaks can also take the form of social networking sites providing sensitive data to third parties without the users’ knowledge or consent.



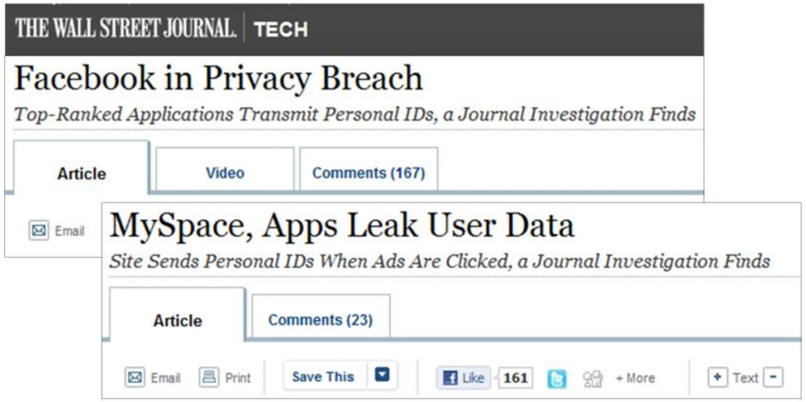
U.S. Citizenship
and Immigration
Services

> “Narcissistic tendencies in many people fuels a need to have a large group of “friends” link to their pages and many of these people accept cyber-friends that they don’t even know.
>
> This provides an excellent vantage point for FDNS to observe the daily life of beneficiaries and petitioners who are suspected of fraudulent activities.”

Numerous entities, both friendly and not, realize how much information about individuals can be harvested from social networks. For instance, a memo issued by the U.S. Citizenship and Immigration services, encouraged Fraud Detection and National Security (FDNS) agents to “friend” beneficiaries and petitioners on social networking sites.

According to the memo, this practice “gives FDNS an opportunity to reveal fraud by browsing these sites to see if petitioners and beneficiaries are in a valid relationship or are attempting to deceive [United States Citizen and Immigration Services] about their relationship. Once a user posts online, they create a public record and timeline of their activities. In essence, using MySpace and other like sites is akin to doing an unannounced cyber ‘site-visit’ on a [sic] petitioners and beneficiaries.”

For details on this memo, see http://www.eff.org/deeplinks/2010/10/applying-citizenship-u-s-citizenship-and



THE WALL STREET JOURNAL. TECH

Facebook in Privacy Breach

Top-Ranked Applications Transmit Personal IDs, a Journal Investigation Finds

MySpace, Apps Leak User Data

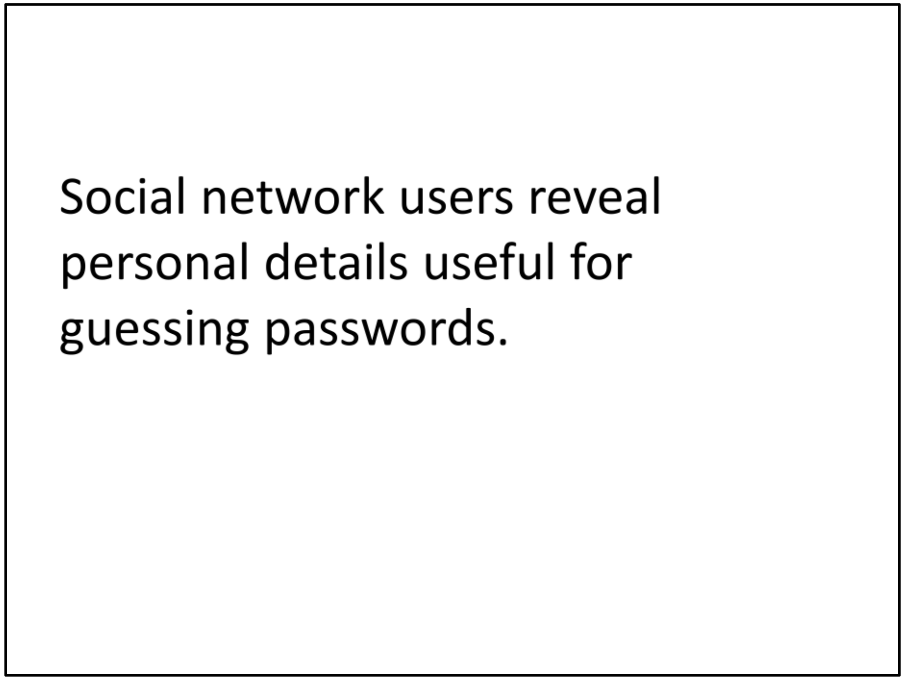
Site Sends Personal IDs When Ads Are Clicked, a Journal Investigation Finds

http://fb-tc-2.farmville.com/flash.php?...
fb_sig_user=681016252

Social networking sites might leak data when interacting with other web applications. For instance, some Facebook applications were found to reveal to advertisers the user ID of the Facebook user. The ID was—supposedly inadvertently—passed as the “fb_sig_user” parameter in the HTTP “referer” header. (For more details, see http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html and http://www.freedom-to-tinker.com/blog/harlanyu/facebook-apps-leaking-user-identities)

MySpace was discovered to have a similar data leak. (See http://online.wsj.com/article/SB10001424052702303738504575568460409331560.html)

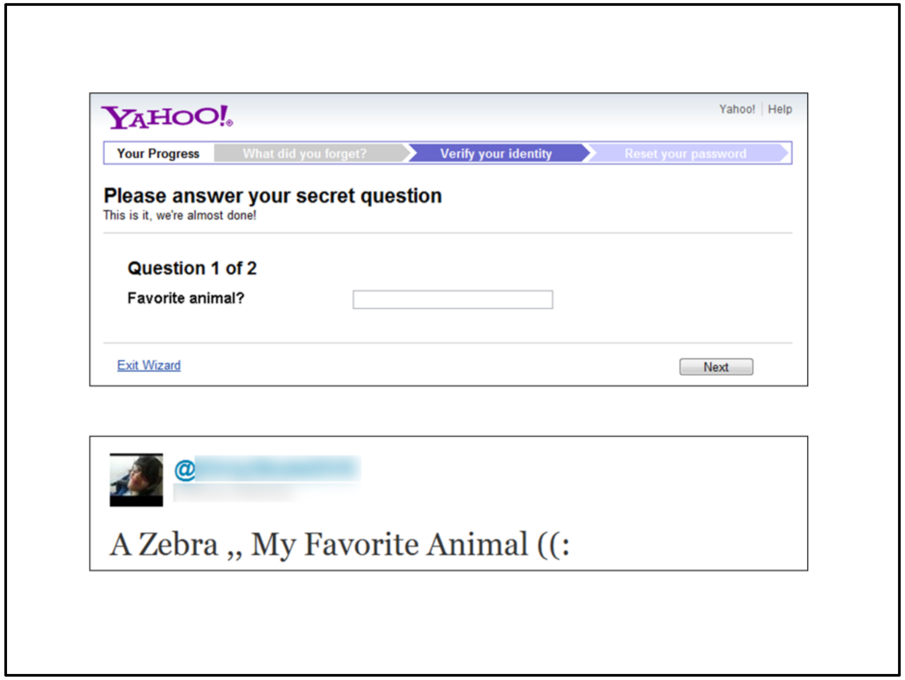
Knowing the social network user’s ID, a third-party site can look up that user’s profile details, which may include the person’s name, sex, and friend details.



Social network users reveal personal details useful for guessing passwords.

The data that users of social networking sites reveal about themselves can be used by attackers to guess or request passwords. For instance, publicly-available information about Sarah Palin was used to reset her Yahoo mail password. (See http://www.wired.com/threatlevel/2008/09/palin-e-mail-ha/)

For additional details on how attackers may profile user passwords using social networking sites, see http://www.securestate.com/Downloadables/Documents/Whitepapers/Profiling_User_Passwords_on_Social_Networks.pdf



Please answer your secret question

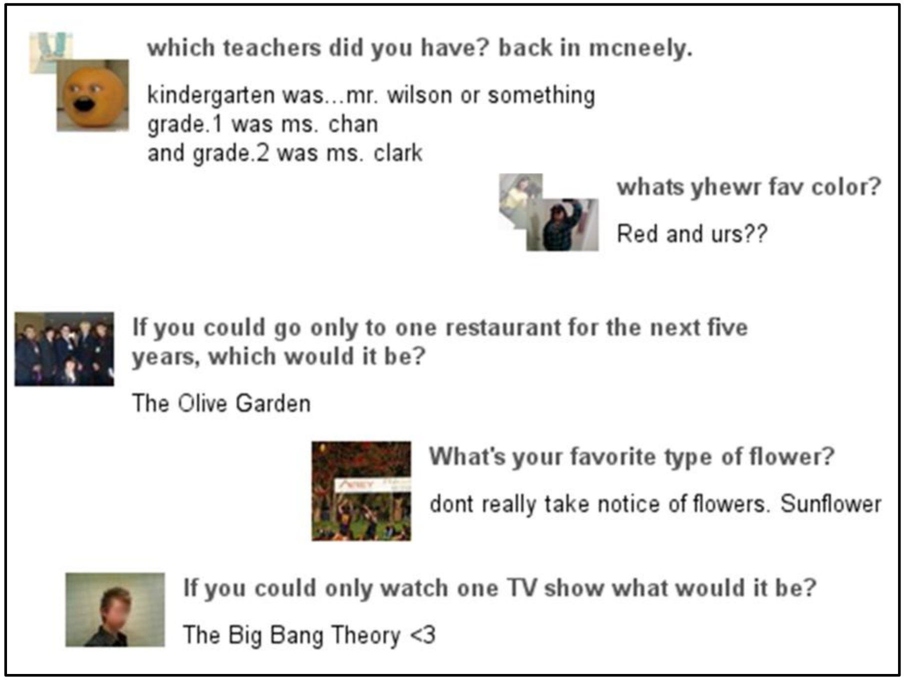
This is it, we're almost done!

Question 1 of 2

Favorite animal?

A Zebra ,, My Favorite Animal ((:

Consider a scenario where the attacker wishes to get access to the target's Yahoo account. One way to accomplish this is to succeed at answering the targeted person's password reset questions. In the example on this slide, one of the questions is "Favorite animal?" The attacker may be able to look through the victim's social networking history to see whether he or she posted about animals.



which teachers did you have? back in mcneely.

kindergarten was...mr. wilson or something
grade.1 was ms. chan
and grade.2 was ms. clark

whats yhewr fav color?

Red and urs??

If you could go only to one restaurant for the next five years, which would it be?

The Olive Garden

What's your favorite type of flower?

dont really take notice of flowers. Sunflower

If you could only watch one TV show what would it be?

The Big Bang Theory <3

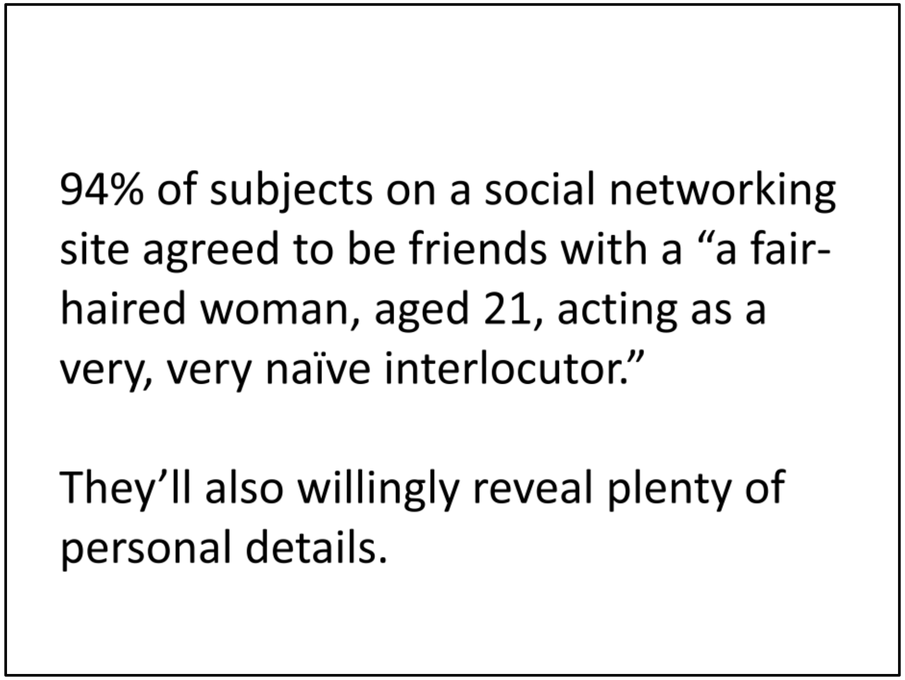
Formspring is a social networking site that's especially popular among teens. It encourages its participants to to ask and answer deeply personal questions. When a new user signs up, he is presented with a list of questions to "seed" his profile, such as:

- Who's the most overrated musician?
- What video game have you played the most?
- What's the furthest you've ever traveled?

By default, the answers the person provides are public. The user can change the privacy settings, but I suspect many people don't even think about this.

An attacker can locate profiles of targeted individuals, or might create a script to mine data in bulk. The collected details could be used to target people using social engineering techniques. Moreover, many of the questions answered by users of Formspring are similar to those used for resetting forgotten passwords.

For more on this, see: http://blog.zeltser.com/post/2908590250/changing-privacy-norms-and-security



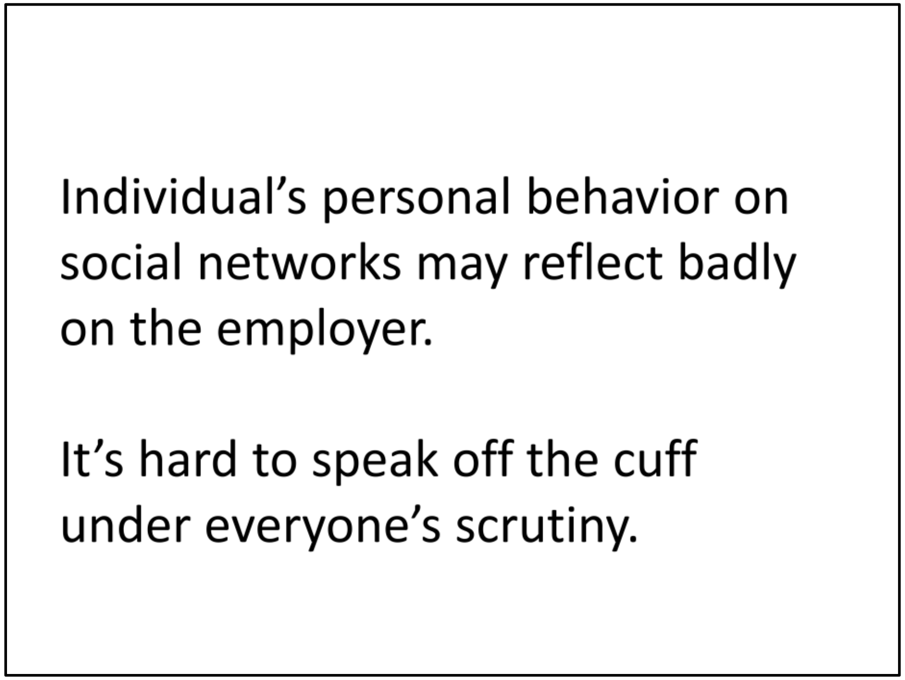
94% of subjects on a social networking site agreed to be friends with a “a fair-haired woman, aged 21, acting as a very, very naïve interlocutor.”

They’ll also willingly reveal plenty of personal details.

BitDefender conducted research to assess the extent to which participants of online social networks will accept a friend request from a stranger whose profile indicates that she is a young, attractive female.

According to BitDefender, “The results of this study suggest not only that social network users accept unknown persons in their group just based on a nice profile photo, but also that they are willing to reveal personal, sensitive information after a short online conversation”

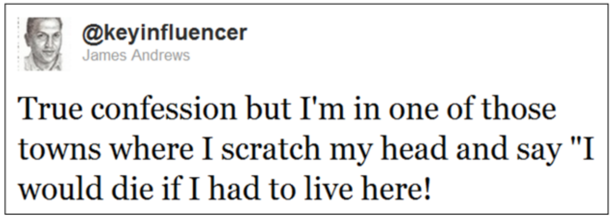
See:
http://bitdefender.com/files/News/file/Social_Networking_and_the_Illusion_of_Anonimity_BT.pdf



Individual’s personal behavior on social networks may reflect badly on the employer.

It’s hard to speak off the cuff under everyone’s scrutiny.

Individuals’ activities on social networking sites may reflect badly on the employer. People want to speak freely when interacting with their friends or colleagues on social networks. However, these sites archive and often make public the conversations, making the conversations subject to everyone’s scrutiny. It’s easy to say something that will offend someone, and might as the result taint the brand of the speaker’s employer.



@keyinfluencer
James Andrews

True confession but I'm in one of those towns where I scratch my head and say "I would die if I had to live here!

> “If I interpret your post correctly, these are your comments about Memphis a few hours after arriving in the global headquarters city of one of your key and lucrative clients… ”

Consider the incident where PR account executive James Andrews landed in Memphis to visit FedEx, which was among his employer’s largest clients. Reportedly, James’ goal was to discuss with FedEx the use of social media for communications.

After arriving to Memphis, James sent a Tweet that said: “I would die if I had to live here!”

FedEx employees—James’ clients—saw the Tweet and took offense to it, as you can see in the excerpt from their response.

For more details about this incident, see http://www.davidhenderson.com/2009/01/21/key-online-influencer/

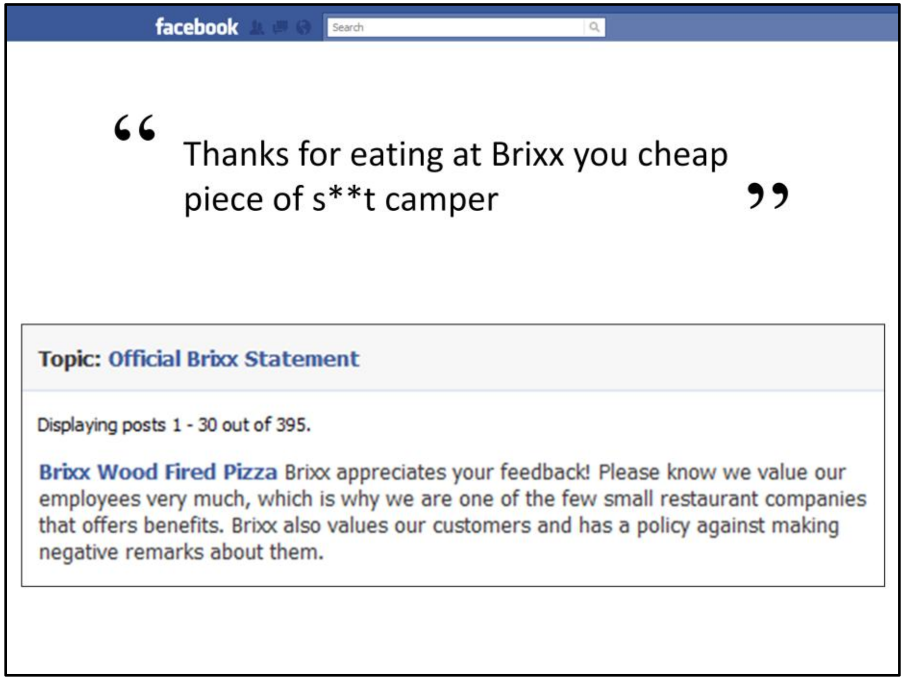
> “In videos posted on YouTube and elsewhere…, a Domino’s employee in Conover, N.C., prepared sandwiches for delivery while putting cheese up his nose…”

According to New York Times, two employee’s of Domino’s Pizza filmed a prank on the restaurant’s kitchen and posted it on-line. The video, viewed by over a million people, showed them preparing sandwiches “while putting cheese up his nose, nasal mucus on the sandwiches, and violating other health-code standards.”

They were fired and faced felony charges, while their employer was left with a major PR crisis on its hands.

For details, see http://www.nytimes.com/2009/04/16/business/media/16dominos.html.

You can view the video at http://consumerist.com/2009/04/dominos-rogue-employees-do-disgusting-things-to-the-food-put-it-on-youtube.html



“Thanks for eating at Brixx you cheap piece of s**t camper”

Topic: Official Brixx Statement

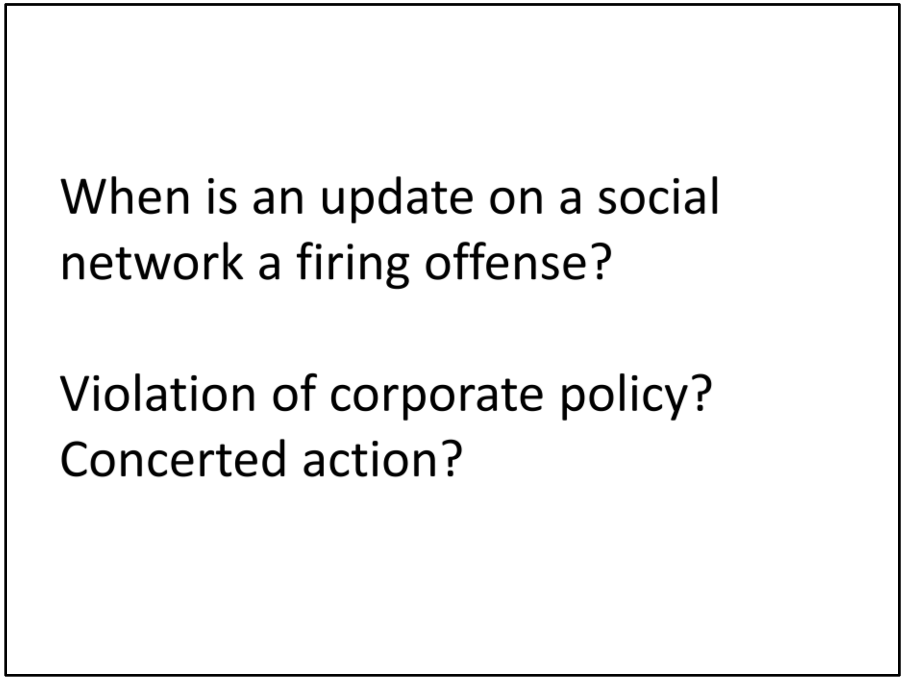
Displaying posts 1 - 30 out of 395.

Brixx Wood Fired Pizza Brixx appreciates your feedback! Please know we value our employees very much, which is why we are one of the few small restaurant companies that offers benefits. Brixx also values our customers and has a policy against making negative remarks about them.

According to Charlotte Observer, a waitress at the Brixx restaurant was fired for badmouthing her customers on Facebook. Reportedly, “a couple came in for lunch and stayed for three hours—forcing her to work an hour past her quitting time. And they left her a tip she thought was pretty measly—$5. Johnson did what most folks who need a good rant do nowadays. When she got home, she went on Facebook.”

For details, see http://www.charlotteobserver.com/2010/05/17/1440447/facebook-post-costs-waitress-her.html

Brixx was criticized on Facebook for firing the employee for this offense. The company defended its position on its Facebook page. You can view the response here: http://www.facebook.com/topic.php?uid=84618206631&topic=15353



When is an update on a social network a firing offense?

Violation of corporate policy? Concerted action?

The question of when a message posted on a social networking site constitutes a firing offense is hard to answer. For instance, according to the Harvard Business Review blog, Dawnmarie Souza, made disparaging remarks about her supervisor “on her Facebook page. In response to this status update, other employees […] posted comments supporting Ms. Souza and criticizing the supervisor.” She was fired for violating the company policy that “disallowed any employee from depicting the company in any way on social media websites without permission.” The National Labor Relations Board (NLRB) alleged that she was wrongfully fired siting the freedom of conducting concerted actions, which are protected “as part of the right to organize labor in order to discuss unionization of a company.”

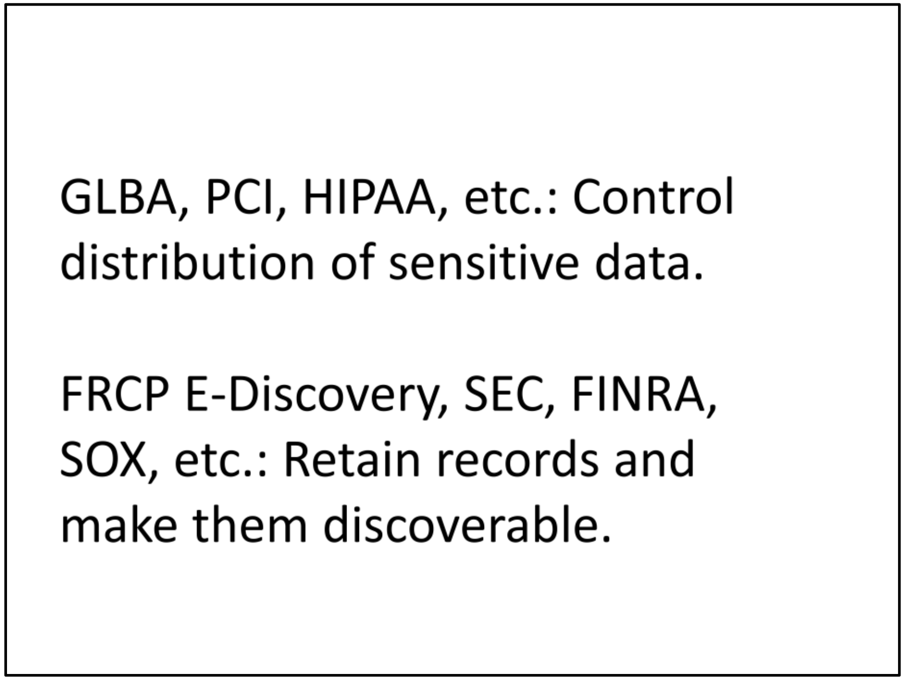
According to the New York Times, the employer agreed to settle the case with NLRB and promised to “revise its ‘overly broad rules’ to ensure that they do not improperly restrict employees from discussing wages, hours and working conditions with co-workers and others while not at work.”

http://blogs.hbr.org/cs/2010/11/when_are_facebook_updates_a_fi.html

http://www.nytimes.com/2011/02/08/business/08labor.html

Organizations are figuring out how to comply with regulations and standards that might apply to social networks.

Since on-line social networking is still a relatively recent phenomenon, organizations are still trying to figure out how to control it to stay compliant with applicable regulations and standards. Merely blocking access to popular social networking sites might not be practical, nor sufficient: employees can still access those sites from a non-corporate location and may engage in activities that put their employer’s compliance posture at risk.



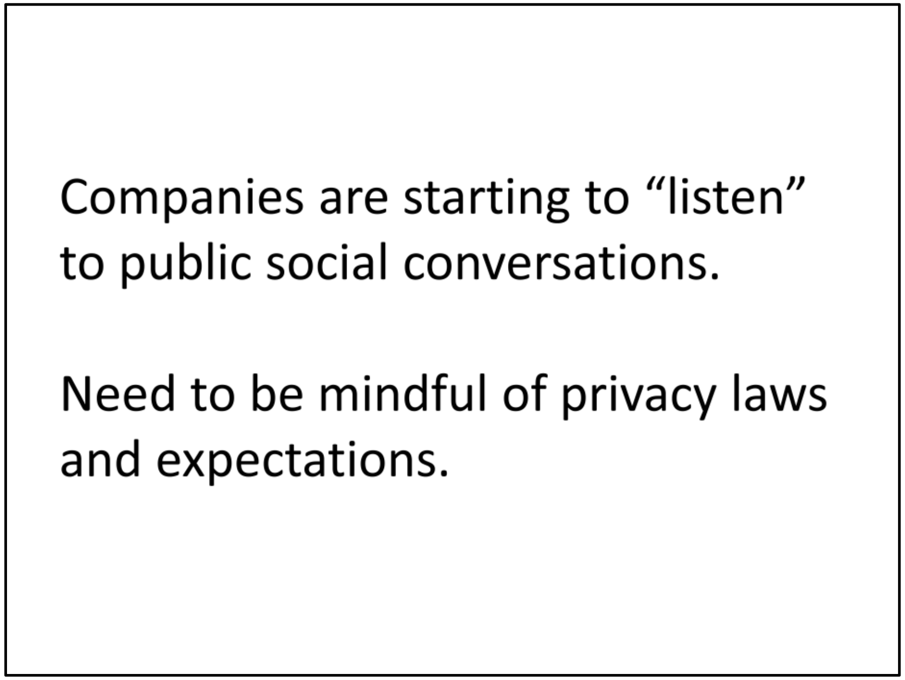
GLBA, PCI, HIPAA, etc.: Control distribution of sensitive data.

FRCP E-Discovery, SEC, FINRA, SOX, etc.: Retain records and make them discoverable.

Broadly speaking, regulatory and contractual requirements that are most relevant to on-line social networking fall into two categories: they might control the distribution of sensitive data and they might require the retention of records to make them discoverable.

Organizations need to consider how they will meet these requirements when their employees communicate and share data on public social networking sites. The challenge increased in the cases where the employees participate in these sites on their own time from home: they might still leak or refer sensitive company data, yet the company will have a hard time tracking their activities to meet compliance requirements.

For additional information regarding regulatory compliance in the context of on-line social networks, take a look at http://docs.bankinfosecurity.com/files/whitepapers/pdf/370_whitepaper_FaceTime_FINRA_SocNet.pdf

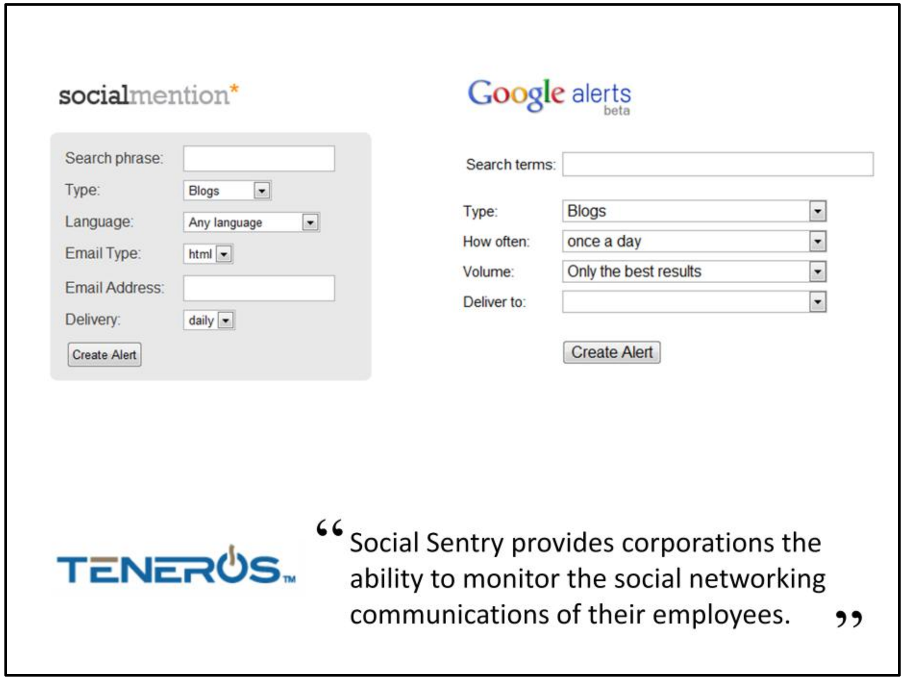


Companies are starting to "listen" to public social conversations.

Need to be mindful of privacy laws and expectations.

As the result of the need to mitigate the risks associated with on-line social networking, which we've been discussing in this presentation, organizations are starting to "listen" to conversation on social networking sites. Such monitoring looks for references to the organization, its data, products and brands. It also looks for activities associated with the company's employees.

When monitoring social networking activities of its employees, the organization needs to be mindful of laws that may guard privacy of the individuals, especially when on-line interactions occur outside of the corporate environment and equipment. For example, according to the New York Times, the German government proposed restricting how employees use Facebook profiles as part of the employee recruiting process. For details, see http://www.nytimes.com/2010/08/26/business/global/26fbook.html



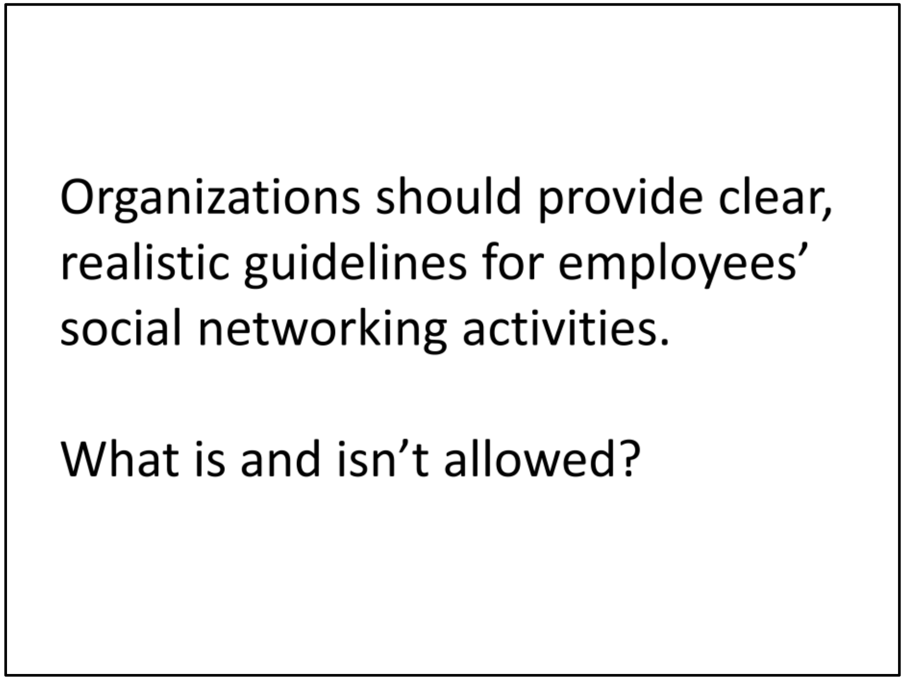
Search phrase:
Type: Blogs
Language: Any language
Email Type: html
Email Address:
Delivery: daily

Search terms:
Type: Blogs
How often: once a day
Volume: Only the best results
Deliver to:

“Social Sentry provides corporations the ability to monitor the social networking communications of their employees.”

There are numerous free tools that can help organizations keep an eye on the conversations occurring on social networking sites. These include: SocialMention, Google Alerts, Twitter Search, Twazzup, CrowdEye, etc. Commercial tools include the various marketing campaign tracking tools, such as PostRank, and specialized products such as Social Sentry.

For additional thoughts on this topic, take a look at http://www.nytimes.com/2010/11/15/business/media/15social.html



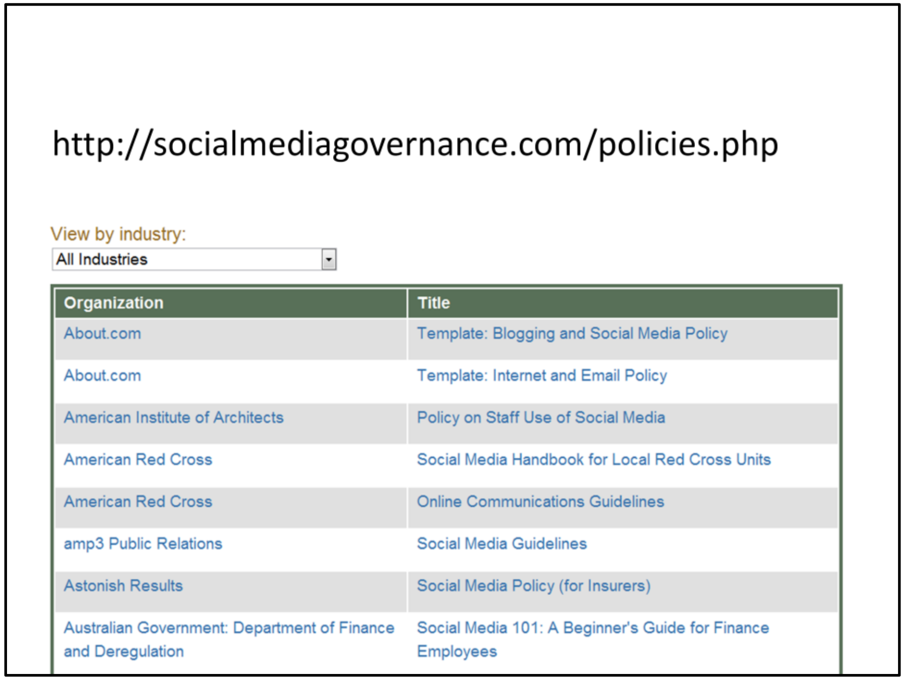
Organizations should provide clear, realistic guidelines for employees' social networking activities.

What is and isn't allowed?

If organizations expect their employees to act in a certain way on social networking sites, it's critical to document guidelines that will guide employees' activities. The guidelines (some might call them policies) should explain what is and isn't allowed and should provide examples.

It's very important that the guidelines be realistic; for instance, simply saying that employees are not allowed to access any social networking sites from work might work for some companies, but not others.

Some organizations ask employees to state in their social networking communications that the opinions they express there do not necessarily represent the views of their employer. However, some organizations consider this an unnecessary statement, assuming that it is implied.



http://socialmediagovernance.com/policies.php

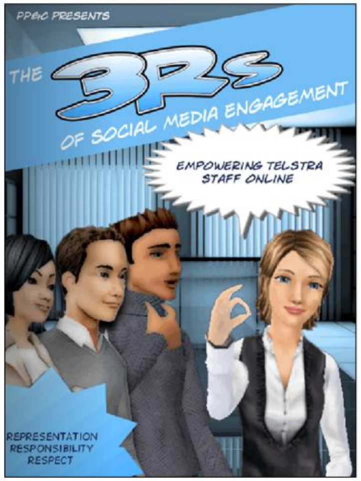
View by industry:

All Industries

Organization	Title
About.com	Template: Blogging and Social Media Policy
About.com	Template: Internet and Email Policy
American Institute of Architects	Policy on Staff Use of Social Media
American Red Cross	Social Media Handbook for Local Red Cross Units
American Red Cross	Online Communications Guidelines
amp3 Public Relations	Social Media Guidelines
Astonish Results	Social Media Policy (for Insurers)
Australian Government: Department of Finance and Deregulation	Social Media 101: A Beginner's Guide for Finance Employees

If you'd like to see how other organizations documented their social media guidelines or policies, take a look at http://socialmediagovernance.com/policies.php.

This site catalogs numerous documents that are made publically available by organizations in various industries. Use these as examples or templates for defining guidelines that are right for your company.



Organizations rarely provide training that is not boring.

In addition to documenting social media guidelines, it’s important to actually train your employees in following them. The training (and guidelines) is probably going to be different for those employees who are allowed to post on social networking sites on behalf of the company, in contrast with the employees who are active in social media as themselves.

Unfortunately, security training is too often very boring, and as the result is not memorable. To help your employees pay attention to and remember your social media training, make it fun. For example, Telstra provides its employees with social media training in the form of animations. They’re engaging and kind of fun. See for yourself at http://exchange.telstra.com.au/training/flip.html

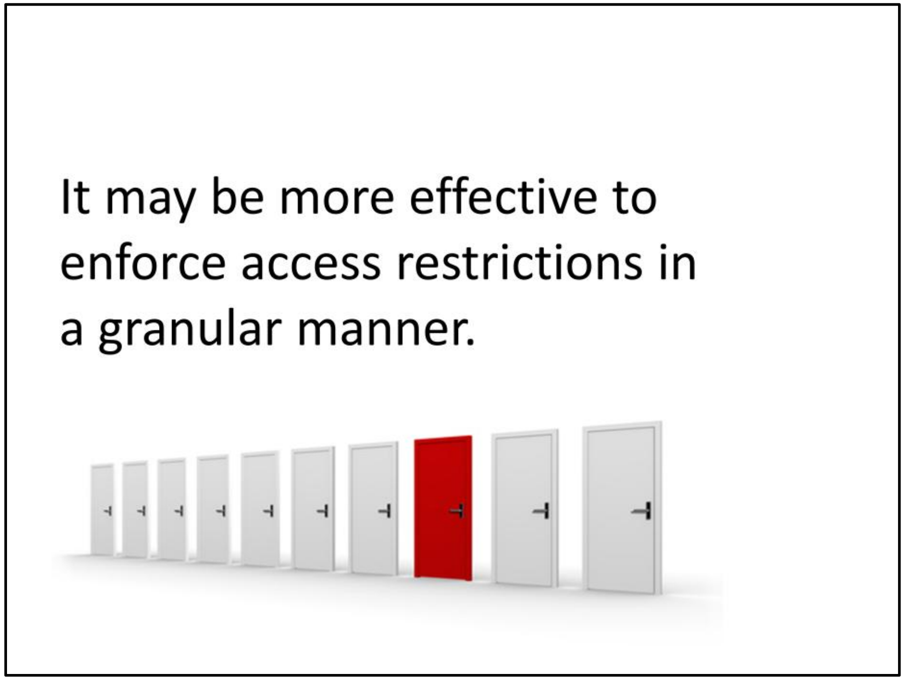
Blocking access to social networking sites not realistic for many industries.

Employees can still access from phone and mobile devices anyway.

Companies in some industries, such as financial services, may be in the position to fully block access to popular social networking sites from the corporate environment. This is unrealistic for many organization’s, just like many organizations allow their employees to browse the web so that they feel like human beings and so they can also research job-specific tasks.

In fact, as I outlined earlier, completely blocking access to social networking sites might be counter-productive: The employees will use these sites from home or from personal devices, which might address only some of the risks discussed in this presentation.

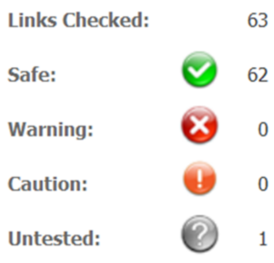
However, if employees access social networking sites from the corporate environment, the company stands a chance of controlling their activities to mitigate risks.



It may be more effective to enforce access restrictions in a granular manner.

Instead, consider adopting technological solutions that enforce the company’s social networking restrictions in a granular manner, allowing some actions, but not others. For instance, the tool could block attempts to post messages that include the company’s products or trademark terms. This approach is reminiscent of some data leakage prevention (DLP) strategies.

Web traffic security tools provide some browsing protection, but are still evolving.

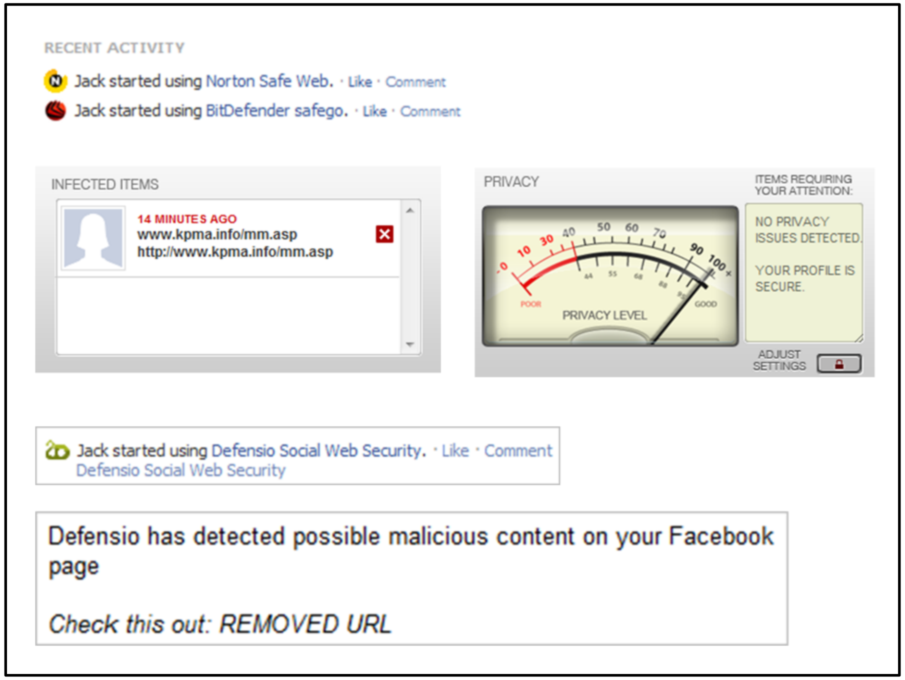


Links Checked:		63
Safe:	✓	62
Warning:	✖	0
Caution:	!	0
Untested:	?	1

Many organizations already deployed tools for securing browsing activities of their employees. These tools can mitigate some of the risks associated with navigating social networking sites. Such tools, including endpoint protection, anti-virus, and web filtering products, are improving their abilities to control users' interactions with social networking sites.

For example, Norton Internet Security includes a Facebook application called Norton Safe Web, which scans links the user's friends share on Facebook to identify those that point to malicious sites.

Norton Safe Web screen shot on this slide is from http://community.norton.com/t5/Norton-Protection-Blog/What-s-new-in-Norton-Internet-Security-2011/ba-p/222807



RECENT ACTIVITY

Jack started using Norton Safe Web. · Like · Comment

Jack started using BitDefender safego. · Like · Comment

INFECTED ITEMS

14 MINUTES AGO
www.kpma.info/mm.asp
http://www.kpma.info/mm.asp

PRIVACY

ITEMS REQUIRING YOUR ATTENTION:

NO PRIVACY ISSUES DETECTED.

YOUR PROFILE IS SECURE.

Jack started using Defensio Social Web Security. · Like · Comment
Defensio Social Web Security

Defensio has detected possible malicious content on your Facebook page

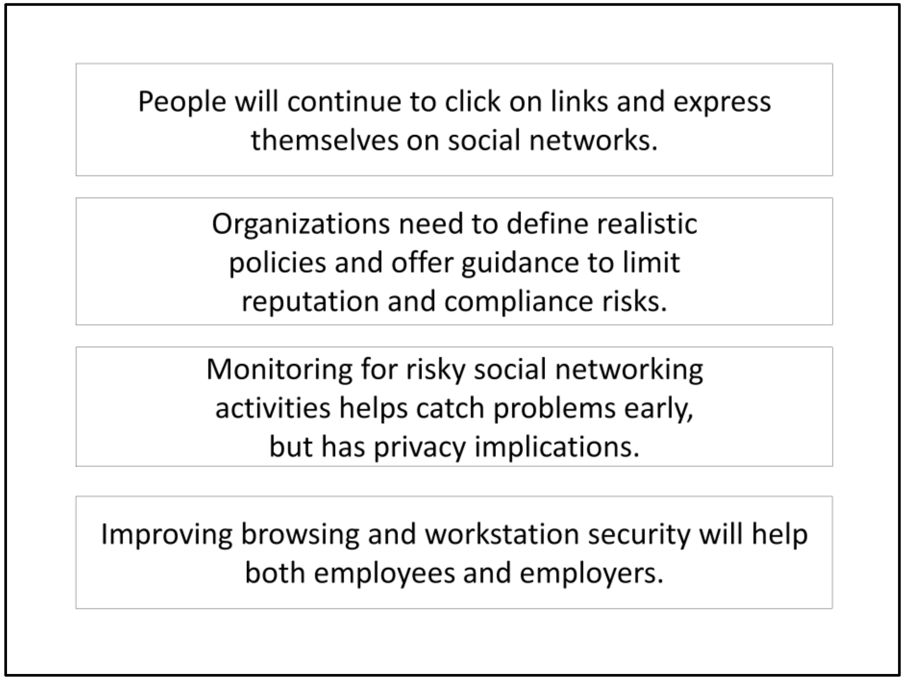
Check this out: REMOVED URL

BitDefender safego is another example of a Facebook app that is designed to improve security of the user's Facebook activities. It can flag the malicious links that the user or his or her friends post. BitDefender safego also aims at warning the user when his Facebook profile settings present a privacy risk.

Another product in this category is Websense Defensio. After installing the Defensio Facebook app, the user has the opportunity to customize a good number of settings, which specify what content Defensio should consider unwanted.

Unfortunately, due to the limitations that Facebook imposes on its apps, Defensio can only alert the use of the unwanted activity, rather than authomatically block the action or removing the content in real time. Defensio can issue the alert via email, which is seems to do within a minute or so of the unwanted behavior.

http://blog.zeltser.com/post/2132741436/facebook-antivirus-protection
http://blog.zeltser.com/post/3068518822/defensio-for-protecting-facebook



People will continue to click on links and express themselves on social networks.

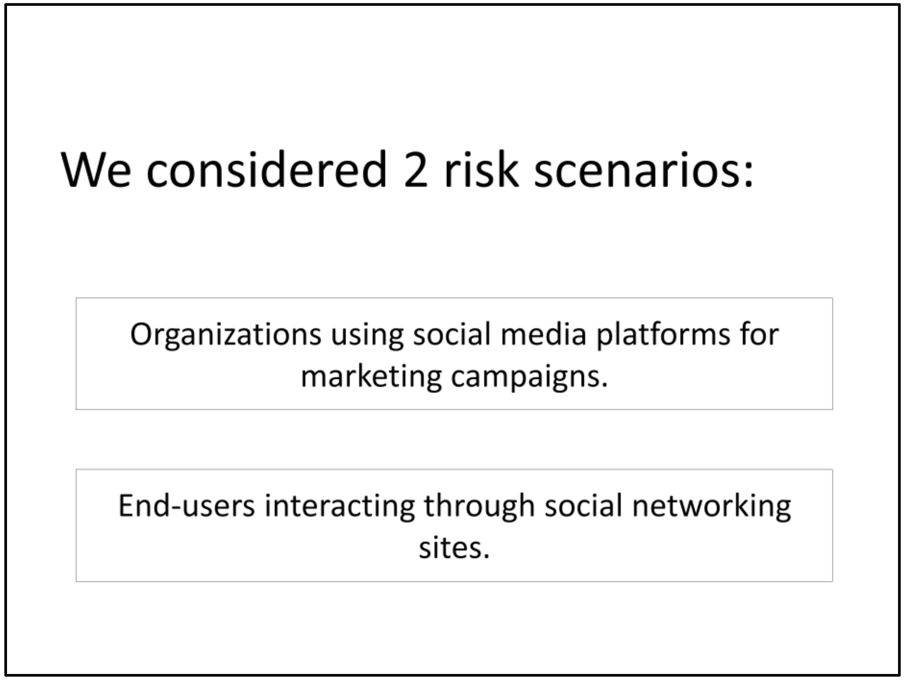
Organizations need to define realistic policies and offer guidance to limit reputation and compliance risks.

Monitoring for risky social networking activities helps catch problems early, but has privacy implications.

Improving browsing and workstation security will help both employees and employers.

We’ve been discussing a category of risks where individuals expose their organizations by participating in on-line social networking. People are social creatures, and will continue to share information and click on links. Sometimes this might be to the determent of their employers.

I emphasized the need to present clear documentation and training to guide employees’ social networking activities to limit reputation, compliance and other risks. I also outlined the need to monitor employees’ social networking activities to catch problems early, while being mindful of privacy implications. Lastly, I highlighted the need for technologies that can enforce the organization’s social networking policies and improve the security of employees’ web browsing experience.



We considered 2 risk scenarios:

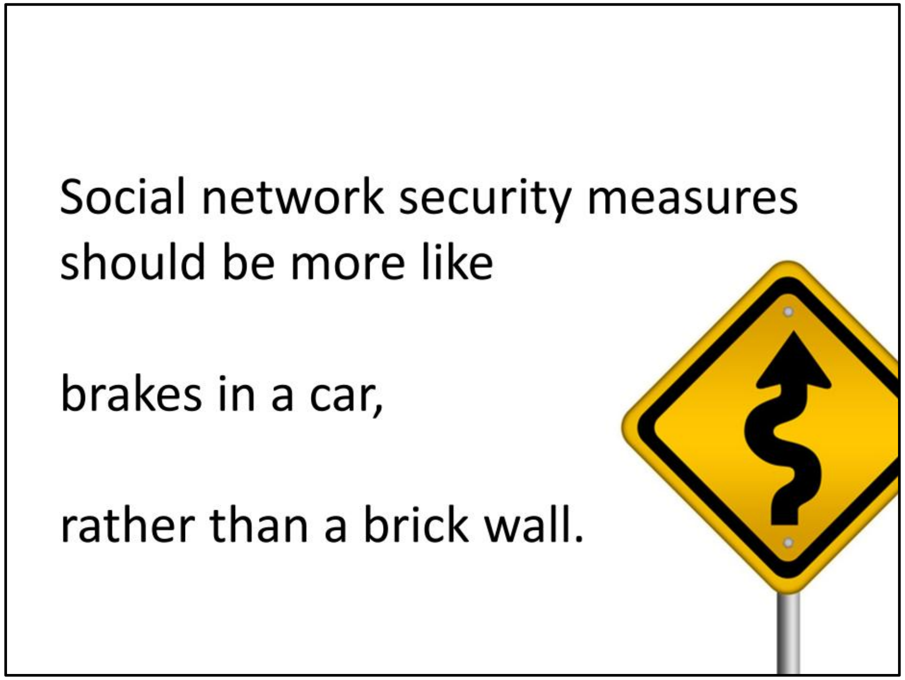
Organizations using social media platforms for marketing campaigns.

End-users interacting through social networking sites.

At a high-level, we considered two categories of risks:

- Those associated with organizations’ use of social media platforms for marketing campaigns and consumer interactions.
- Those associated with end-users’ interactions through social networking sites.

I outlined some of the factors that encourage organizations and individuals to participate in online social networking, and brought up a bunch of examples where such activities put employees and their employers at risk. Where appropriate, I recommended ways of mitigating these risks.



Social network security measures should be more like

brakes in a car,

rather than a brick wall.

Throughout the presentation I emphasized the need to understand how people in your organizations use social networking sites and what motivates them to do so. It’s hard to discuss with colleagues ways of securing social network interactions if you don’t know much about Facebook or Twitter. It’s hard to protect your company’s social media marketing activities if you don’t know how the company is trying to engage consumers through this medium and why.

I’d like to leave you with this final thought:

Security measures should be more like brakes in a car, rather than a brick wall. If your efforts to secure data and mitigate risks are seen as a wall that makes it impossible to conduct business, you’ll become irrelevant and will probably fail. However, if your security efforts are seen as allowing the organization to move fast, but let it slow down when a treacherous path requires caution, you just might succeed. This is the case in many areas of information security, including social networking.

Lenny Zeltser

blog.zeltser.com
twitter.com/lennyzeltser
lenny@zeltser.com

If you have any questions about social network security issues, please get in touch with me—I'll be glad to hear from you! You can find me on Twitter at http://twitter.com/lennyzeltser. I also maintain a security-focused blog at http://blog.zeltser.com.

Disclaimer:

The views herein are those of the author and do not reflect any official opinion or position of the author’s employer.

About The Author:

Lenny Zeltser leads the security consulting practice at Savvis. He is also a board of directors member at SANS Technology Institute, a SANS faculty member, and an incident handler at the Internet Storm Center. Lenny frequently speaks on information security and related business topics at conferences and private events, writes articles, and has co-authored several books.

Lenny is one of the few individuals in the world who have earned the highly-regarded GIAC Security Expert (GSE) designation. He also holds the CISSP certification. Lenny has an MBA degree from MIT Sloan and a computer science degree from the University of Pennsylvania. For more information about his projects, see www.zeltser.com.