Social Media Security Guide for Small Business

A Tactical Guide and Checklist to securing your social media and corporate brand

When was the last time you received spam on social media? What about a friend request from a questionable account or a person you don't personally know with no mutual friends?

One Norton study found that a whopping 65% of internet users are victims of cybercrime.

Even more interesting — was when they more recently found that 40% of individuals have become victim to some form of a social media cybercrime.

That's almost one in two.

Social media threats are on the rise and continuously evolving. Now more than ever it's essential for individuals and companies to protect themselves from becoming vulnerable to attacks on personal information and sensitive data.

The purpose of this article is to detail information on the various forms of threats facing individuals and organizations today on social media and to also help educate you on the various ways in which you can strategically and proactively work to protect yourself against them.

Social EngineeringYou may have heard of the term social engineering before — but are you familiar with what the term means within the context of information security? Social engineering involves the use of deception in order to manipulate individuals into exposing personal information for the purpose of using such information illegally.

Social engineering is in fact the popular and most prevalent of social media threats out there and the tactics and methods used vary widely. Generally speaking, information is leveraged in order to create and establish trust with a specific individual or account over a period of time.

Once this sense of trust is established, the attacker looks for ways to gain valuable information from the victim such as internal server names, project information or data.Again, the methods vary widely, with perhaps one of the most popular being tricking a victim into opening an infected file or clicking on a link which has the ability to drop a backdoor into the individual's computer.

These methods are constantly being tweaked and adjusted to become more effective and complex in nature, which is why consistent monitoring of key employee information and company accounts is essential.

Targeted Phishing Attacks

These attacks are focused threats which are done in order to exploit critical information or money from a victim. The attacker leverages fear, anxiety or plain old unawareness by tricking the victim into disclosing personal information.

A few years back there was a prevalent phishing attack that hit Facebook compromising countless accounts of unsuspecting individuals and organizations. This threat started out as an innocuous email from a Facebook friend of the user, notifying visitors to visit a Facebook link which was infected.

Facebook rapidly took action in order to blacklist the domain, however there were countless copycat threats spawned as a result of its success.

Some of these threats will even duplicate a social media platform's login page in order to get you to enter in your personal information such as your email and your password. Many individuals don't double check the contents of a URL in a search browser, which can sometimes be the only way to pick up on the fact that it's fraudulent.

In March of last year a phishing attack on Twitter targeted 10,000 DoD employees with what was coined "expertly tailored messages" by Time Magazine.

Some employees were even interestingly enough breached on account of their family members, with one individual being compromised due to his wife clicking on a link to a vacation package on her own Twitter account after exchanging messages with friends about things to do over the summer with their children.

Attackers are getting more and more savvy by the day and there are no longer any excuses for companies to allow themselves and their customers to remain vulnerable to such vicious threats.

Fraud

Fraudulent and duplicate accounts are all too common on social media platforms where there is often an abundance of personal information. This is one of the main reasons why individuals and companies should be extremely wary about the personal connections which they make within the social media sphere.Back in 2010 a fraudulent account by the name of Robin Sage was created by attackers who persistently sought to make connections for the purpose of exploiting valuable information and data.

Many individuals accepted these connections without even knowing who this fraudulent individual was or the devious actions behind the account. To make matters worse, many of these connections were with organizations serving in the military, government and even security firms.

There are four main types of social media fraud:

1. Fraud against customers
2. Recruiting Fraud
3. Fraud against employees
4. Counterfeit goods

Fraud against customers include scams which target customers usually do so by identifying a brand's follower base and segmenting them based on information shared on the social network. This helps to further target and tailor their attacks, thus giving them a higher probability of success.

These scams usually promise customers a reward of sorts and uses false credentials (i.e. a logo) in order to impersonate a brand.

Recruiting fraud on the other hand has become prevalent with the ever-expanding use of online recruiting. Sites such as LinkedIn are particularly subject to compromise as they target the business force.

These often involve “pay-to-play” recruitment scams and can seek to exploit money from the victims by collecting fraudulent application fees or personal information via applications in order to sell it for identity theft.

These scammers consistently monitor job sites and often target young and unsuspecting individuals fresh into the job pool.

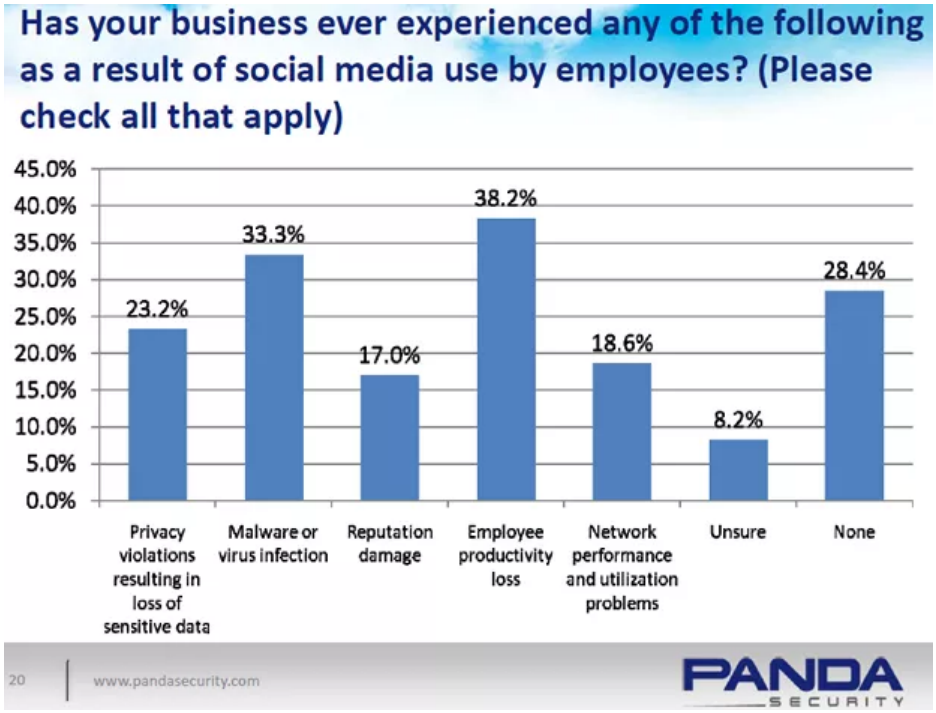
Fraud against employees is often carried out in the form of a fraudulent business associate seeking information or assistance. For instance, they may take on the identity of a human resources manager in the company and seek to get an employee to disclose confidential company information, sensitive data or government ID numbers.

Many times the threat may originate not from a fraudulent account, but from a compromised real account, making it even more difficult for the individual to ascertain the legitimacy of the situation.

Counterfeit Goods

This form of fraud can be particularly devastating to a company’s bottom line as scammers will often leverage branded hashtags and company keywords in order to expose their products to a large mass of potential buyers.

Unfortunately for organizations, responsibility largely rests on the shoulders of companies to seek out, identify and report this type of activity. But if a company doesn’t have a protection program in place, or is not actively and consistently seeking out the existence of such a threat, then it makes it particularly challenging for a platform to appropriately mitigate such threats.



Malware

Social media is rife with an abundance of malware and other threats which are creatively transferred via a wide array of methods such as links, infected documents or other means.

Malware is primarily designed to make money illegally by stealing personal and valuable data and information from unsuspecting individuals and organizations. The term “malware” is an umbrella term, which describes any form of malicious code in general.

Types of malware include viruses, which are similar in theory to viruses within the biological realm, as they are primarily designed to both duplicate and spread. Most viruses are located within an executable file where an individual must open said file in order to allow the virus to spread and cause damage.

Trojans are harmful piecees of software that often looks legitimate and is used for the purpose of stealing personal information or gaining access to your personal computer systems.

Ransomware is malicious code that is meant to incapacitate your systems and hold your valuable information hostage while demanding a ransom in order to release it.

Spyware is the quite and unsuspecting threat lurking within a computer system. It is used to quitely collect and store information, including keystrokes via “keylogging” in order to steal sensitive data and personal information such as passwords, credit cards and bank account information.

Worms replicate rapidly and are often spread through computer networks from one computer to another. They differ from viruses in that they don’t require the user to spread them from a specific infected host file because they are a form of software themselves.

Cross-site Request Forgery (CSRF) is a technique of sorts that’s used to spread a complex social networking worm by exploiting the “trust a social networking application has in a logged-in user’s browser”. If the social network isn’t checking the referrer header, the attack can easily “share an image in a user’s event stream that other users might click on to catch/spread the attack”.

Obviously downloading files from unknown, unverifiable or even questionable sources is a major way in which we can help to stave off harmful threats.

However, attackers are becoming more and more savvy with their methods and making it harder and harder for unsuspecting victims to be able to tell the difference between a legitimate file and link or an illegitimate one.

One unintentional exacerbator to this is the growing preference for shortened URLs.

These URLs are used for convenience in place of their longer counterparts, however, the problem with this is that when URLs are shortened, often, essential identifying information regarding the source of the URL is lost.

A popular website called Bitly can turn any URL into a short, convenient version. For example, we can take the following URL:

https://www.visioneerit.com/the-top-10-reasons-why-gary-vee-is-winning-the-marketing-game/

...and with the help of Bitly, transform it into a more compact, convenient version of the following:

https://bit.ly/2o9l9KE

Now, generally speaking, this is great — especially for social media and digital marketing purposes because condensing the content gives you the ability to use it in places such as social media posts, whereas before, you were unable to.

However, the problem with this lies in the fact that you are no longer able to identify the destination of the URL. Before, with the original version, you can clearly see the name of the website and the subsequent page that you are being directed to.The shortened version on the other hand does not make this information visibly perceptible and as a result, you are at a significantly greater disadvantage when it comes to being susceptible to clicking on links which contain spam, malware or viruses of some kind.

Unintentional Leaks

Sometimes, no matter how hard we try to prevent becoming subject to the risk of threats, we still end up compromised because sometimes — we are our own worst enemies.

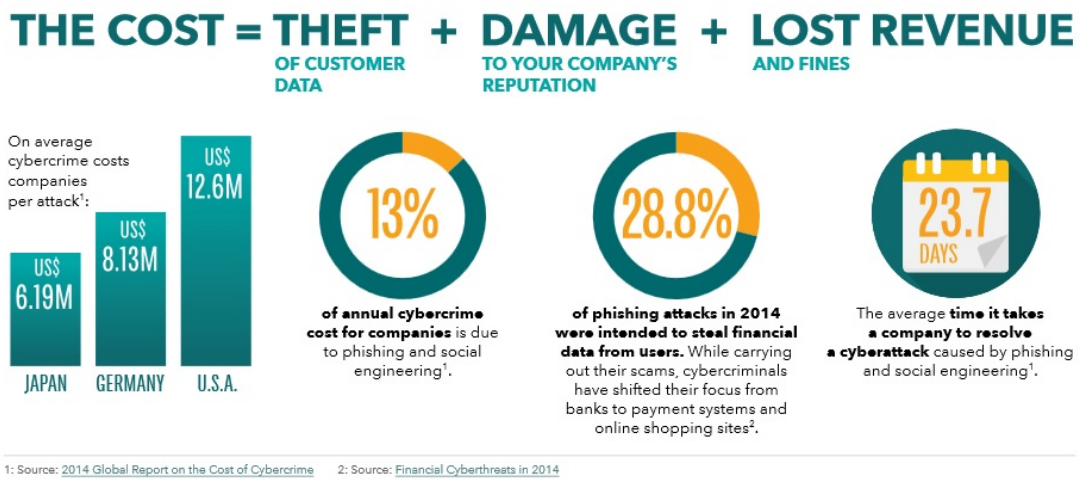
Unintentional leaks happen all too often as the result of “oversharing” and can have devastating effects on companies. The same old story of an employee accidentally revealing information assumed to be uncritical only to compromise an entire organization happens time and time again.
This could be something as simple as an employee’s spouse complaining about the amount of overtime the employee has been putting into a particular project, to casually revealing a firewall product or discussing details regarding a Web proxy product being used in passing.

Even information as seemingly insignificant as such can clue attackers in on the details of an organization’s security measures or software and leave them vulnerable.

This is especially the case considering the existence of what are coined “Advanced Persistent Threats” or “APTs”.

APTs strategically gather intelligence on specific individuals and find themselves at a large advantage due to the wealth of information available on social networking sites.

The perpetrators use the information gathered in order to place “more intelligence gathering” in the form of, for example, malware or trojans, in order to “gain access to sensitive systems”.



Solutions

So how does a company effectively protect themselves in the midst of so many complex, persistent and ever-changing threats on social media?

Platform-Specific

Of course the number one holy grail of all rules is that you should always use caution when considering which individuals to accept into your social networks. Individuals should also periodically review friends lists, connections and followers and be on the lookout for any suspicious accounts. Even then threats can still often come disguised as familiar faces.

Let’s face it — no two social media platforms are the same and as a result, there are unique threats presented on each one. As a result, we’ve included a quick list of platform-specific tips to help you on your road to greater social media protection.

Facebook

The great thing about Facebook is that the platform has a range of security checkup tools available for use located within a user's security settings. These tools work to improve security and privacy and can offer services such as login notifications when unrecognized devices are used to gain access to an account.

Periodically going through your account and removing unused and old applications is a must, as these often have access to personal information that should not be left out in the open.

Did you know you can limit the number of friend requests you receive by adjusting the "Who Can Contact Me?" setting? Given the astronomical rise in fraudulent accounts, this is an extremely useful option.

Another useful tip is making your friends, followers or connections lists private. This can help not only limit the amount of information a threatening source can retrieve from your profile, but it can also help protect those you know and love in the event you become compromised.

Lastly, it's always a good rule to limit the amount of visibility your page, posts and images have to the general public.

LinkedIn

LinkedIn is a particularly vulnerable platform due to the fact that it's a social media platform targeted towards the business professional demographic. Just like any other social media site, we cannot stress enough the importance of being wary about which personal connections you establish.

Sometimes this can be difficult, especially for those individuals and companies seeking rapid expansion and to spread brand awareness. Just remember to do your due diligence.

Also, always be wary of sales and recruitment messages that include external links, request money or personal information and never open links sent from individuals who you do not personally know.

Twitter

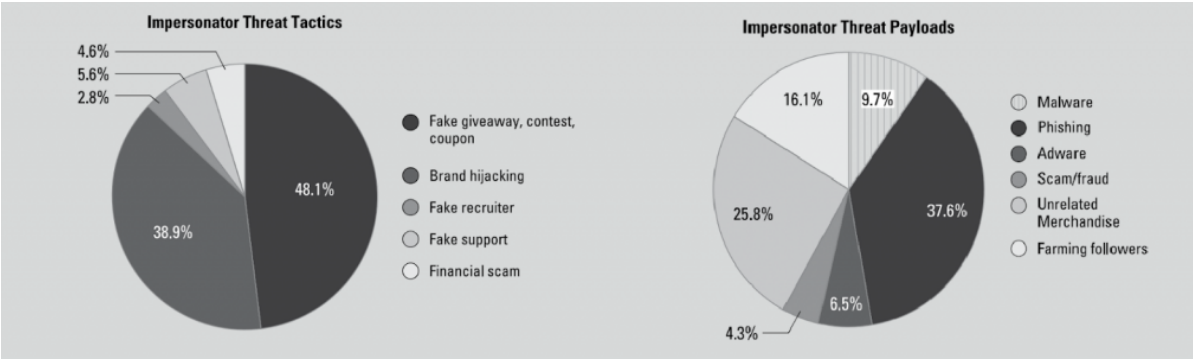
Did you know that Twitter was created in order to help maximize your personal brand exposure? Maximum exposure means maximum visibility and users should keep this in mind when posting personal information.Did you know that Tweets are also searchable? That's right — unless you've manually enabled certain security features to prevent this, aka the "Protect My Tweets" setting, and labeled your account to private, attackers get free roam of everything you've posted.

Instagram

Did you know that if your account isn't private, everything you post is visible to any user on Instagram? This is especially important to take into consideration when crafting employee policies for codes of conduct on social media.

When posting, be wary that the images do not include any personal information, data, specifics on location or any other content that may be used and leverage against you, your employees, customers or company.

Also, report accounts that you notice are misusing hashtags or handles or are propagating spam. If you're an organization, encourage your employees to do the same.



General

There are many suggestions on corporate protocol that can be taken into consideration in order to help minimize the risk associated with social media threats.

Companies should also take into consideration offering training and/or educational resources to employees in order to guide them on how to properly identify and report cases of threats or fraudulent activities. Employees should also be regularly briefed on proper codes of conduct for social media channels so as to help prevent unnecessary and unintentional information leaks.High-risk individuals such as executives are especially prone to attack and often times as a result, companies manage social media usage to a certain degree or periodically audit the social media usage of such individuals in order to remain proactive against threats.

Other options involve letting security-trained assistants to aid in the management of executive social media accounts.

Furthermore, companies should always be sure to enable two-factor identification for all business social media accounts and should always encourage changing passwords at least three times a year for maximum security.

Remaining transparent about your information gathering practices and policies to the public is also something to consider in order to help combat potential fraudulent activities targeted towards your customer demographic.

As one can imagine, in order to properly prepare for and protect yourself, your company, your employees and your customer base against social media threats, a great deal of consistently implemented work is involved.This is why it is always highly recommended that companies make use of a social media protection tool in order to help automate the process.

Social media protection tools can help companies save money and work more efficiently by continuously monitor your social channels, as well as those of key employees for compromise. These tools also can help identify targeted phishing attacks on social networks and mitigate what can quite easily become costly fraudulent activities.

Whether it’s copyrighted content which is being repurposed for malicious activity, brand impersonation, malicious links, hashtag hijacking or fake promotions to drive phishing pages, look for robust software that can help find and take down fraudulent accounts as well as help to uncover stolen information.

By the numbers:

- 2 Million — The number of pieces of content analyzed.
- 3 — The number of scams created for each one that is taken down.
- 80 — The percentage of scam posts with a lifespan greater than 45 days.
- 4,574 — The total number of unique scams identified.
- $435 Million — The estimated total that money flipping scams cost global banks each year.

Conclusion

Did you know that in 2016 social media phishing attacks increased 500% year-over-year? Regardless of the amount of effort you put into proactively protecting yourself or your company, the fact remains that social media is and will continue to remain a substantial cybersecurity risk for you and your business.

From phony Facebook updates to links to free vouchers and messages disguised as coming from colleagues, the threats range far and wide.
Now more than ever it's essential for you as an individual or organization to do everything in your power to be certain that your personal data and information remain safe.

Invest in a task force. Train your employees and executives and invest in a reputable and robust software program that can help you automate the security process so that you can have peace of mind even while you sleep

....Because let's face it — you spend enough time with social media on the brain as it is. So get proactive and , protected so you can devote as much time as you can to cute baby videos and funny dog vids instead of security breaches and company meltdowns.

Social Media Protection Checklist

So here is what you can do to help protect your social media accounts

Sources:

https://www.computerweekly.com/tip/Top-seven-social-media-threats

https://www.calyptix.com/top-threats/social-media-threats-facebook-malware-twitter-phishing/

https://www.itworld.com/article/2773490/security/facebook–fbaction-net–phishing-attack-in-progress.html

https://www.networkworld.com/article/2213704/collaboration-social/top-10-social-networking-threats.html

VisioneerIT

A guide to safer browsing

Social media threats are on the rise and they are continuously evolving..

65% of internet users are victims to cyber crime.

In more recent news, 40% of individuals have become victim to some form of social media cyber crime.

Social engineering is a very common social media threat..

Attackers use social engineering as a way to gain data from internet users by exposing them to information that appears to be trustworthy. Once the attackers have gained your trust, they use the data they have gathered maliciously.

Targeted phishing attacks- Threats that are meant to exploit a victim by deceiving them so they can release personal information or provide money.

When you start a social media page do these things first.

1. Make it a point to change your password frequently.
2. Do not share personal information that can easily identity you online(date of birth, address, telephone numbers etc..) ALWAYS! Keep your information private.
3. Use a two-factor authentication in order to protect the information on your social media accounts.
4. Do not post sensitive information about your workplace.
5. Check the list of people that follow you on your social media pages and most IMPORTANTLY, make your followers private.
6. Make it a constant thing to search for any fake pages that may be pretending to be you.
7. Become familiar with your employer's social media policy.

Marketing Team Checklist

- [ ] Always consult with your security team before creating a social media protection program.
- [ ] All employees should use the same social media management platform when publishing materials on social media.
- [ ] Review any third party applications that have been given access to your company's social media pages on a consistent basis.
- [ ] Use social media as a way to find individuals who are trying to mimic your brand.
- [ ] Have a PR team in place in case anything goes wrong. Responding quickly is imperative!
- [ ] Monitor your organization's social media accounts for any outrageous or sensitive content so they can be hidden or blocked.
- [ ] Be on alert when using your brand's hashtags and flag any individuals that may be using them maliciously.
- [ ] Have a security team assist you with creating security settings for your social media accounts..
- [ ] If you come across any threats, make sure to report it to your social media network.

Checklist for Fraud, Risk, and Compliance Teams

1.Set guidelines for what employees can post online.

2.Have an acceptable use policy in effect for future candidates for your application process.

3. Advise the public and visitors to your website about how your company collects information.

4. Offer employee training so that your staff will know how to identify any fraudulent activity and as result, your employees will know how to handle it.

5. ALWAYS monitor all of your social media networks to lessen the chances of getting scammed.

6. Designate an individual with that is well versed in the organizations security practices monitor your social media accounts.

The four main types of social media fraud

- **Fraud against customers**- Scammers that mimic a known brand by targeting customers based on the information consumers have shared online.
- **Recruiting fraud**- Scammers that scope job seekers on job sites by collecting fraudulent application fees and personal data through applications so they can sell people's information for identity theft.
- **Fraud against employees**- A fraudulent business associate that seeks to gain information by pretending to be an employee in a corporation so they can get access to sensitive data.
- **Counterfeit Goods**- A fraudulent activity that takes place when a scammer uses a company's branded hashtags or keywords to expose consumers to their products

Information Security Team Checklist

- [ ] Collaborate with the executive, marketing and corporate teams to create a protection plan for your social media pages
- [ ] Establish a policy for employees so they will be aware of what type of information they can or cannot share online
- [ ] Offer training that will give employees the opportunity to learn how to use social media cautiously
- [ ] Discern which employees will be granted certain permissions on your social media accounts, this also applies to corporate users
- [ ] Install tools that will automatically detect cyber attacks and alert you if any of your company's information has been compromised
- [ ] Incorporate your social media information into your security system

Social Media Threats

Malware- Threats that can be transferred through links, documents and other means.

Trojans- Threats that may appear lawful but will steal your personal information or try to gain entry into your computer system.

Ransomware- A malicious code that will immobilize your system, seized your information and demand a ransom to release it.

Spyware- An unsuspecting threat where your information is collected quietly via “keylogging” to retrieve personal information such as passwords, credit cards and bank information.

Worms- They replicate very quickly and can spread from one computer to another.
Cross Site Request Forgery (CSRF) -The ability to exploit a logged-in user’s browser by spreading a social networking worm which can increase the risks of attacks if other users click on any links coming from the logged-in user.

Unintentional leaks- When an employee within a company accidentally reveals information that places an entire organization at risk
Advanced Persistent Threats (APTs)- A strategic way of gathering people’s information through malware and trojans in order to get access to sensitive systems

Corporate Security Checklist

- ☐ Collaborate with your team to include a situational awareness into your social media protection plan
- ☐ Monitor your company's social media usage
- ☐ Create policies that employees can refer to so they will know how to handle different situations
- ☐ Always monitor your social media pages for any risks

Social Media Protection Checklist

- [ ] Your social media pages should always be updated. Examples of social media pages are facebook, instagram, linkedin and twitter.

- [ ] Make sure that the corporate accounts follow the same user access guidelines like any other secure system in your organization.

- [ ] The Corporate passwords should be changed frequently.

- [ ] Review your users social media access every quarter.

- [ ] Establish policies that reflect your business demands and also set up guidelines for employees when using their personal accounts.

- [ ] Have a system in place that will alert you if it senses that your data has been compromised.