WHITE PAPER

proofpoint™

A GUIDE TO CORPORATE SOCIAL MEDIA SECURITY

TOP 5 CORPORATE SOCIAL MEDIA RISKS AND HOW TO PROTECT YOUR FIRM

TABLE OF CONTENTS

INTRODUCTION

With rapid business adoption of social media as a core public communication channel, organizations are increasingly exposed to an array of internal and external security risks. Fraudulent Facebook accounts impersonate major brands to sell counterfeit products. Bogus LinkedIn profiles trick employees into divulging sensitive data. Corporate Twitter accounts are hijacked to defame the brand and distribute propaganda. In response, the FBI, Gartner and many other security analysts cite social media as one of the fastest growing security threats. Bottom line—social media provides bad actors with a direct link to customers, employees, and brand equity that they can easily exploit—all without the trouble of evading firewalls or IPS systems. After all, why hack a database when you can just ask an employee or customer for a password via social media?

It's important for security teams at organizations with significant social media presence to gain an understanding of this new attack surface and develop a plan to protect the business. The purpose of this paper is to help security teams in this effort. We'll provide a review of the top social media security attack techniques. We'll explain how those techniques translate to risk (data theft, brand fraud, etc.) And, we'd provide immediate steps that can be taken to protect the organization.

"12% of the complaints submitted in 2014 contained a social media trait. Complaints involving social media have quadrupled over the last five years"

FBI Internet
Crime Report 2014

"Manually distributed malware via social media and in response to phishing will be the greatest growth category."

Gartner 3 Year
Security Trends 2015

WHY IS SOCIAL MEDIA AN ATTRACTIVE ATTACK VECTOR?

Unique attributes of Facebook, Twitter, LinkedIn, and other social channels make it a hacker's dream environment relative to alternate corporate communication attack channels like corporate Web sites and email.

Reach—A single social post can reach thousands of corporate employees and customers. In comparison, an attacker needs to send thousands of emails to reach a similar audience and, in the process, risks drawing the attention of email security systems. In addition to these economies of scale advantages, social media provides attackers the flexibility to target employees and customers.

Context—Attackers use publicly available corporate social media content to identify lists of employees, roles, colleagues, partners, and projects. They then incorporate this contextual information to craft social engineering elements that make attack lures appear legitimate. Users are far more likely to click on social links from someone they believe is a peer or an official representative of a corporate brand than a random email from an unknown source. And, they are far less conditioned to be wary of a link in social media than in email.

Lack of Controls—Few (if any) enterprise social media security controls stand in the way of attackers today. In contrast, Web attacks require circumventing network firewalls, IPS systems, Web firewalls, and even database monitoring systems. Malicious email requires circumvention of very mature email security technologies.

Effort—Social media provides a free and easy path to success. Setting up a fake social media profile and posting malicious content to a corporate social media page can be accomplished in minutes.

SOCIAL MEDIA ATTACK METHODS

When it comes to getting the "biggest bang for their buck" in accessing corporate social accounts, attackers have honed their skills. There are three, main methods that bad actors employ to target corporate social media: fraudulent accounts, account hacks, and malicious content.

FRAUDULENT ACCOUNTS

A fraudulent social media account is a bad-actor created account that mimics an actual brand or employee account. Fraudulent accounts are used to sell counterfeit goods, phish credentials, redirect consumers to competitive offerings, drive advertising revenue, distribute adware, embarrass the brand, and generally perpetrate scams of every flavor. Dozens of fraudulent accounts are typically linked to major brands at any given time.

Figure 1: Fraudulent accounts phish credentials, sell counterfeit goods, collect personal data, scam customers, and embarrass the brand

Example—Customer Support Credential Phishing

One fraudulent account scheme we see frequently employs fake customer service accounts to phish customer account credentials. We have seen this scheme used to steal customer account credentials at banks, retailers, game services, among many others.

1. A customer tweets a question (for example. "I lost my lost password") to a Twitter customer service account—for example @MajorBankHelp.
2. An attacker monitoring @MajorBankHelp sees the question and tweets a "response" directly to the customer from a fake Twitter account with a slightly different name. For example, the fake name might be @MajorBank_Help. The account appears otherwise identical (logo, images, etc.) to the real account. Often attackers target after-hours support inquiries in order to engage before actual representatives see the request.
3. The attacker's tweet includes a link to a bogus website asking the customer to login to resolve their issue (e.g. reset their password, etc.). When the customer logs in to the bogus site, the attacker captures credentials to the customer's actual bank account.

This scheme enables attackers to access customer account data without the trouble of penetrating bank infrastructure or even delivering a phishing email to the bank's customer. Why bother hacking through layers of security controls or sending thousands of emails when you can steal the same data by asking a customer to hand it over? For more detail on this scheme check out this blog.

ACCOUNT HACKS

Social media "account hacks" refer to a complete takeover of a brand's social media account by a bad actor. The attacker gains administrative access to a corporate social media account, locks out other administrators, and begins posting malicious content to an audience who think the content is coming from a trusted brand. The root cause of a social account hack most commonly is simply poor password management practices: weak passwords, unprotected/lost password lists, stolen devices, etc. But many other account hack vectors exist, including disgruntled employees, poor access management practices, man-in-the-middle, and insecure social apps connected to the account.

Hacked accounts are often used to hijack a large news media audience in promotion of a cause (e.g. terrorism or politics). They are also being used to embarrass brands, steal account contact lists or use the hack as a stepping stone to gain deeper access to the company network. For well-known brands, account hacks are typically a public relations crisis with the potential to seriously damage the brand and its community. Newsweek, Chipotle, Delta Airlines, the U.S. Central Command, Sony, The International Business Times, Crayola, and The New York Post are just a few organizations who have suffered from negative publicity due to account hacks in the past year alone.

Security teams are typically brought in as part of a clean-up fire-drill to clean up after a hack. That effort typically involves shutting down the account (or all accounts), forensic investigation, researching social media security best practices, and implementing a plan to prevent future hacks. It all has to happen fast because the business needs to get those accounts back up and running. This should sound familiar for security teams who have had to deal with a hacked Web site. In this way, social media has become just like the Web site, email, or any other business application. The business depends on it, so it has to remain available.

Figure 2: The security team is asked to clean up the mess when hacked accounts embarrass the brand, distribute propaganda, or steal data.

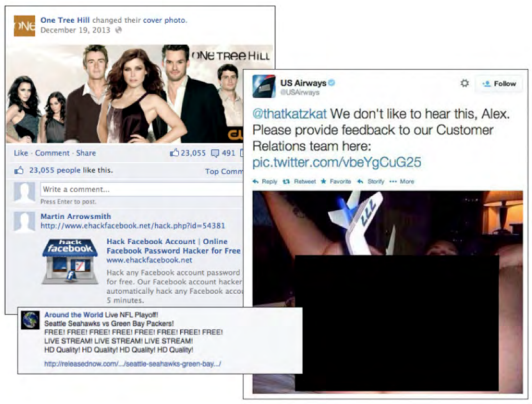

Figure 3: Bad actors post spam, malware, phishing links, and inappropriate content in social media comments

MALICIOUS CONTENT

Malicious content is the simplest of social media attacks. The attacker simply posts malware links, phishing links, spam, brand bashing, porn links, hate speech and other damaging content as comments on a legitimate brand or employee social account. By posting malicious content to brand accounts, hackers and scammers effectively drop "attack bait" into a massive pond of potential victims. It's also important to note also that malicious content attacks can be crafted to target both customers and employees following brand pages. Not only does malicious content represent a security risk to the brand, but it undermines the business value of social media.

TOP FIVE ENTERPRISE SOCIAL MEDIA SECURITY RISKS

From data theft, to counterfeit products (brand fraud), to simple brand bashing—there are dozens of risks linked to the social attack methods described above. In the following we've identified the top five risks for enterprise security professionals.

1. Network or Data Breach

Attackers use social media to target employees and sometimes customers as an entry point to breaching your organization's network and/or data. Social media not only provides the attacker with an open communication link to employees and customers, it provides them with the context (hobbies, movies, sports, friends, employer, etc.) needed to craft social engineering elements that dramatically increase success rate. Below are a few real-world examples.

- **Facebook Service Spoof:** The attacker creates a bogus Facebook service account (using the Facebook logo and other recognizable design elements), comments to corporate pages asking administrators to reset passwords, and points to a link. Users follow the link to a page that prompts for Facebook credentials and asks for verification with email credentials. The attacker then has both Facebook and email credentials to gain deeper enterprise access.
- **Malware Bait:** The attacker sends a link to a corporate Twitter page with a promise for content that might interest employees at the target firm. For example, the attacker posts to an entertainment industry account with a link to view a cool, live-music video for one of the company's artists. Prior to watching the video, the viewer is asked to update the video player software, which instead installs a key logger.
- **Bogus LinkedIn Profile:** The attacker creates a LinkedIn profile mimicking an actual (or fictional) executive and sends connection requests to individuals who self-identify as working at the target firm. When employees accept the connection request, the attacker uses the relationship to establish trust with additional employees, share infected files (e.g., a macro-infected résumé), phish credentials, gather competitive intelligence, and other activities that support the attacker's goal. Penetration tests taking this approach see surprisingly high response rates from employees who are far too inclined to accept LinkedIn connection requests even when it comes from a fictional person. [1]

2. Customer Account Breach

Your customers can be high-value targets for hackers who use social media to gain access to their accounts and the privileges associated with those accounts. Think about what your customer accounts could offer a hacker: personal information for identity theft, credit card numbers, product purchases, access to financial accounts, rewards points, and more. Also consider the public relations and recovery effort necessary when those accounts are compromised.

Bad actors have a variety of social media methods at their disposal to trick your customers into providing them with credentials. One common technique uses fake social media accounts posing as your brand to make special offers to your customers. Some examples include:

- Fake customer service (e.g. download a fix for a known software bug)
- Fake promotional offers and contests
- Free loyalty program "points"
- Low-interest credit cards

In each case, customers are provided a link and are prompted to log into their account to access the offer. Instead of logging into your website, they are providing credentials to the attacker. For example, fake Twitter accounts were used to steal World Cup fans' logins for EA Sports and Xbox Live.[2] Similarly, a fake Qantas Facebook account enticed users to share their financial details for a chance to win a $1,500 travel voucher.[3]

3. Brand Damage

A company's brand reputation is the source of millions or even billions in revenue for many organizations. Organizations like Samsung, Microsoft, Verizon, ATT, Walmart, and Amazon all have brand valuations north of $50 billion.[4] Brand is the most important corporate asset for organizations like these and thousands of others. In parallel, most major brands have turned to social media to connect with their audiences. However, lack of control over social brand associations and security incidents also creates risk of brand damage. Brand damage via social media can take many forms.

- **Malicious and Offensive Content:** When deviants repeatedly post spam, profanity, hate speech, bullying, and pornography to corporate social media pages, it creates an unsafe environment that conflicts with almost any brand guidelines. Not to mention the fact that it drives away followers and undermines millions in social media marketing investment.
- **Fraudulent Accounts:** Imposters hijack brands with fraudulent accounts to sell counterfeit products, phish credentials, perpetrate a wide range of other scams. When fraudulent web sites or advertisers hijack brands outside of social, lawyers are activated to protect the brand and its customers. As social audiences grow, it's important that brands take the same actions in social that they do in print, Web, and other media.
- **Hacked Accounts:** Hacked social accounts are used to promote terrorist activity, political agendas, or directly embarrass the brand itself. Regardless of agenda, these events undermine confidence in the brand for millions of followers. Account hacks typically amplify brand damage given they often attract press coverage. Companies like Tesla, United Press International, Chipotle and Burger King all made the headlines when they fell victim to social account takeovers where hackers posted inappropriate, lewd, defamatory, and blatantly inaccurate content.

4. Downtime and Degradation

In a survey from Salesforce.com, 66 percent of the 5,000 marketers surveyed believe that social media is now core to their business, with the top three areas for increased spending all related to social media (social media advertising, marketing, and engagement).[5] For these organizations, social media is a critical application the business depends upon—just as it depends upon the website or CRM infrastructure. In such cases, social needs to be protected from threats that force downtime or degrade effectiveness, just as other critical infrastructure is protected. When attackers interfere with business processes that depend on social, it has a direct impact on the bottom line, lowering the return on social investments.

News media provide a good example of an organization that integrates social media into their core business process. Many news organizations rely on social not only to deliver news, but to collect source content submitted by the population (think storm videos, police videos, etc.). When a major U.S. news organization's social accounts were hacked, they were forced to shut down social more than a week while the security team regained control. During this downtime, the news team loses a primary source of content that the business relies upon.

We've seen similar examples with dozens of our customers. When a software developer's social media support account became polluted with spam, customers began calling phone support lines—a more expensive channel for the firm. Similarly, when social pages supporting a movie launch were hit with thousands of spam, profanity, and pornography messages, the movie studio not only lost control of their message but they also began to see a decline in engagement from their followers. In both cases, the firm's investment in social media is seriously undermined.

THE COMPLIANCE RISK OF SOCIAL MEDIA

Although not specifically security related, compliance is another area of significant enterprise social media risk. According to Forrester Research, there are more than 12 major regulatory bodies including FINRA, FFIEC, FDA, FTC, SEC, and NLRB that have defined rules for what businesses can and can't do on social media.[6] Monitoring for compliance with all these rules is a real challenge for many brands given hundreds of social accounts and massive message volumes. For more information on social media compliance challenges, check out our Fortune 100 Compliance Report.

5. Security Team Recovery Costs

A commonly overlooked impact of a hacked social media account is the recovery cost incurred by the security team. Often the security team is not engaged to help protect corporate social media accounts until a breach occurs. It then becomes an unplanned operation that has a distinct learning curve and disrupts normal security operations. The effort can be labor intensive for the security team, which must tackle an array of remediation elements, including:

- Lock down of all social accounts
- Removal of offensive content
- De-provision users and/or reset passwords
- Investigate the breach and identify root cause
- Deploy new security controls to prevent future breaches

TAKING STEPS TO PROTECT YOUR ORGANIZATION

Given increasing frequency of social media incidents, many security teams are starting to realize they need to address social media security within their organizations. This means taking steps to ensure the organization follows best practices, and creating processes to recover gracefully in the event that an incident occurs. Here are a few tips on how to get started.

COLLABORATE WITH YOUR SOCIAL TEAM

We recommend that the security team reach out to the social media team and to establish a collaborative relationship in which the teams work together put the right safeguards in place. Ensure them that your goal is to simultaneously help social be more successful by building a safer environment and protecting the business from unnecessary risk. Collaboration is critical because accurately measuring business risk, defining process guidelines, training, and even deploying protective controls will require buy-in from the social team.

ASSESS YOUR SOCIAL FOOTPRINT AND RISKS

A prerequisite to implementing social media security is to gain an understanding of your social media footprint and risks. In addition to creating an inventory of known corporate and employee accounts, you'll likely discover accounts that have been created for regions or products that are unknown to centralized corporate social account owners. You're also likely to find fraudulent accounts created to rip off your brand and customers.

Once you've mapped the footprint, assess the risk of these properties to the business. What accounts are already impacted by spam, scams, compliance incidents, malicious links, and inappropriate content? Which accounts are most engaged with the public? What happens if they get hijacked or get taken offline? In a world of limited resources, proper risk assessment will help prioritize next steps.

Given that brand social presence often extends to hundreds or thousands of accounts, identifying social footprint and assessing risk can be a challenge. Automated tools are available to map your footprint and perform assessments of those accounts. This entire process can be done transparently—without disrupting social media operations or requiring additional effort from the social media marketing team. Click here for more information on how to identity your social footprint and assess risk.

EDUCATE EMPLOYEES

Deliver security awareness training covering how to avoid social media attacks, including: limiting connections to known contacts (especially on LinkedIn), identifying scams, and avoiding dangerous links. To be most effective, social media security education should be ongoing with periodic assessment of knowledge and vulnerability levels within the company. Deliver this training to corporate social media account owners as well as employees who represent the brand through their personal accounts (e.g., social brand advocates).

APPLY BEST PRACTICE SECURITY CONTROLS

Fundamental account and content security controls can go long way towards reducing social media security risk.

ACCOUNT SECURITY

- Use application controls to limit the apps that have access to accounts. This minimizes attack surface by reducing the apps that can be compromised.
- Apply account monitoring to detect unauthorized change or anomalous activity. Establish a process to quickly lock down accounts should such events occur.
- Define a user-provisioning process that limits account access to only those users with business need. This reduces the social attack surface by limiting the number of employees who can be targeted and credentials that can be lost.
- Consider two-factor authentication and/or single sign-on to reduce risk of compromised passwords.

CONTENT SECURITY

Define and enforce a content security policy that eliminates spam, malware, phishing, hate, abuse, and other dangerous content from social pages. For organizations limited to a handful of accounts with a limited amount of daily posts, human moderators may be sufficient to enforce this policy. For organizations with dozens of accounts subject to hundreds or thousands of daily comments, automated content security technology is the better approach. Look for solutions that can detect both inbound attack risks from outsiders, as well as outbound risks from employees.

Visit here for more information on how to apply social media account and content security controls.

CONCLUSION

In the past, social media security events were mostly minor disruptions with minimal impact on the business. Today, with organizations depending on social as a key element of business infrastructure, the stakes are higher. For those organizations, information security teams must protect corporate social accounts just as they would other business infrastructure. If an account gets hijacked, or an attacker uses social media to break into customer accounts, the security team needs to understand how it happened and how to respond.

Automated social media security technology can help your organization reduce the risks to your company's networks, data, customers, and brand. A pioneer in social media security and compliance, Proofpoint's team offers a patent-pending, cloud-based solution that allows your organization to centrally discover, audit, and protect its presence on the social web. To learn more, visit: www.proofpoint.com.

[1] "One CISO, One Fake LinkedIn Account; Here's What He Found Out About His Staff," Tony Loynes, ITProPortal, May 19, 2014.
[2] "World Cup Scammers Use Twitter to Steal Gaming Credentials," Doug Drinkwater, SC Magazine, May 21, 2014.
[3] "Facebook investigates a fake Qantas page using the airline's 'birthday celebrations' to convince customers to hand over personal details for the change to win a $1500 travel voucher," Melissa Hills, Daily Mail Australia, September 15, 2014.
[4] http://brandirectory.com
[5] "2015 State of Marketing," Salesforce, 2015.
[6] "The Forrester Wave: Social Risk and Compliance Solutions, Q2 2014," Nick Hayes, Forrester, May 7, 2014.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.