proofpoint™

SOCIAL MEDIA PROTECTION

BRAND FRAUD

REPORT

TABLE OF CONTENTS

INTRODUCTION

Businesses are investing more than ever in social media. Organizations are expected to spend $35.98 billion on social media advertising in 2017, up nearly 50% from 2015 totals.[1]

This influx of money has created an ideal setting for cyber crime. Fraudsters create fake accounts to steal data and disrupt business. Some are as simple as unwanted protest accounts. Others might link to phishing and malware. Through fraudulent accounts, criminals can swipe all kinds of personal information: bank logins, credit cards, and even Social Security numbers. Regardless of their methods or goals, fraudulent accounts hurt your brand and your customers.

The pool of potential victims is huge. The number of social media users is expected to grow from 2.04 billion worldwide in 2015 to 2.55 billion by 2018.[2] That's about a third of Earth's population.

Fake accounts are one the most common social media security challenges for enterprises. In our 2014 research, we found that Fortune 100 companies are a popular target for fraud. Some 40% of Facebook accounts and 20% of Twitter accounts that claim to represent a Fortune 100 brand are unauthorized. We researched these issues further in Q2 2016 to understand how this business risk has evolved.

This inaugural Social Media Brand Fraud Report reveals the current state of social media fraud. It uncovers fraudsters' motives and methods. And it details types of fraudulent accounts. The report also recommends ways to protect your social presence from this pervasive security risk.

[1] eMarketer: Social Network Ad Spending
[2] eMarketer: Social Network Users Worldwide

METHODOLOGY

From April through June 2016, we researched the prevalence and types of fraudulent social media accounts. Our objectives were twofold:

- Identify the categories of fraudulent brand accounts
- Measure the scope of this growing threat

For our research, we selected 10 top brands from different industries.[3] The selected brands are leaders in their field and have an active social presence with an average of 33.7 million followers across major social platforms, including Facebook, Twitter, YouTube, and Instagram.

Based on our massive body of customer data, as well as deeper research into the nearly 5,000 accounts associated with these 10 brands, we found that social media fraud is on the rise. Our findings highlight the need for companies to protect themselves from these constant and growing security threats on social media.

KEYFINDINGS

Cyber attackers don't stop with web, email, or mobile apps. Social media has become a prime attack target due to a large user base and corporate ad spending. Companies have embraced social media as an essential marketing communications tool. And they continue to build out their social presence. In fact, 38% of companies plan to spend more than 20% of their total ad budgets on social media channels.[4]

This focus makes social media a lucrative and attractive target for cyber criminals. One of the most effective methods is fraudulent accounts. Scammers set up fake social media accounts to masquerade as corporate brands and defraud fans.

Our Q2 2016 Social Media Brand Fraud Key Findings further confirm our earlier research: companies must continuously be on the hunt for social media fraud and manage these risks in a way that scales.

Here are our key findings:

- We detected nearly 600 new fraudulent accounts each month in Q2 2016.
- Of the 4,840 social media accounts associated with 10 top brand names,19% were fraudulent.
- Of the 902 fraudulent accounts associated with 10 top brands, nearly 30% were scams or offers for counterfeit products and services.
- 4% of 10 top brand fraud accounts exist for one or more of the following: phishing for personally identifiable information (PII), malware, protest, and satire. While 4% may seem a small percentage, these accounts can be dangerous to your customers and brand reputation.
- Counterfeit and knockoff product offerings represent 11% of 10 top brand fraud accounts.
- Social media phishing is the fastest growing social media threat: we have already seen a 150% increase this year vs. the same period in 2015.

FRAUDULENT ACCOUNT TYPES

10 Top Brands

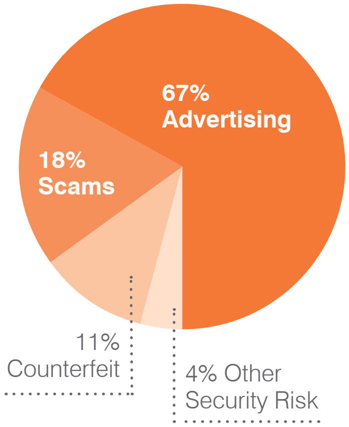


Figure 1: Scams and counterfeit products and services account for nearly 30% of fraudulent accounts in our research on top brands

AVERAGE # OF FRAUD ACCOUNTS

Per Month

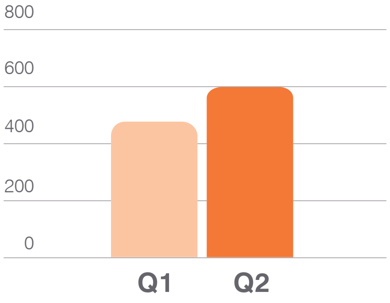


Figure 2: Social media fraud increased by 20% in Q2 vs Q1 of 2016

[3] Brands Researched: BMW, Capital One, Chanel, Amazon, DirecTV, Nike, Samsung, Shell, Sony, Starbucks. These brands appeared on the Brand Directory list of top brands for 2015.
[4] Altimeter: The 2015 State of Social Business

FRAUDSTERS' MOTIVES & METHODS

Well-meaning employees create some unauthorized accounts. These employees may not be familiar with your social media policy. This type of account is more of a nuisance than a security threat. Clear guidance about social media policies will help address this issue.

But many unauthorized accounts are fake brand accounts. They are created solely to defraud your customers or undermine your brand. Bad actors create these accounts for financial gain or to protest your company and create negative brand sentiment.

Other fraudsters prey on customers who try to engage with your brand. They target customers using fake customer service accounts, phony sweepstakes, and more. We found that 19% of 10 top brand accounts are fraudulent. We expect this trend to expand more broadly into mid-market and enterprise brands.

Some are motivated by a political agenda and create fraudulent accounts to attack a brand’s image. Most often, they closely imitate the brand to make fun of the company or its customers. These protest accounts diminish brand value and create a negative or even hostile experience for customers.

FRAUD METHODS

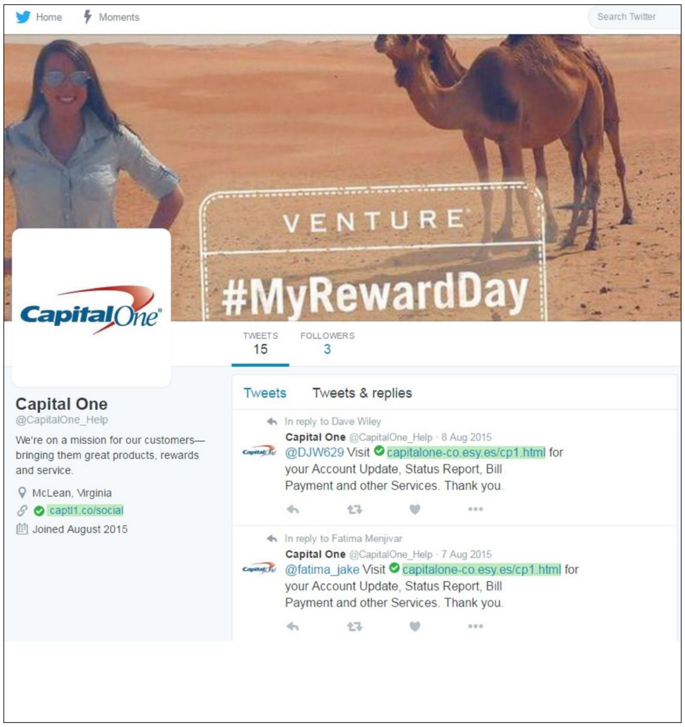
Social media fraudsters target users with the same “bait” they use in other cyber attacks. This includes legitimate-looking content with offers that appear too good to pass up. Some even appeal directly to users for their credit card or account details.

Common social fraud methods include creating fake accounts that:

- Promise free or discounted gifts
- Offer customer support or software updates

Fake accounts so closely resemble the real corporate account that telling them apart can be difficult for novice users. They often retain the company’s look and feel, including official logos. The only difference might be something as small as one character in the Twitter handle, such as @askmajorbank vs. @ask_majorbank.

And what about verified accounts?“Twitter and Facebook verify accounts to confirm that they really belong to the brands or people depicted. A verified account gets a blue checkmark badge next to the account name.



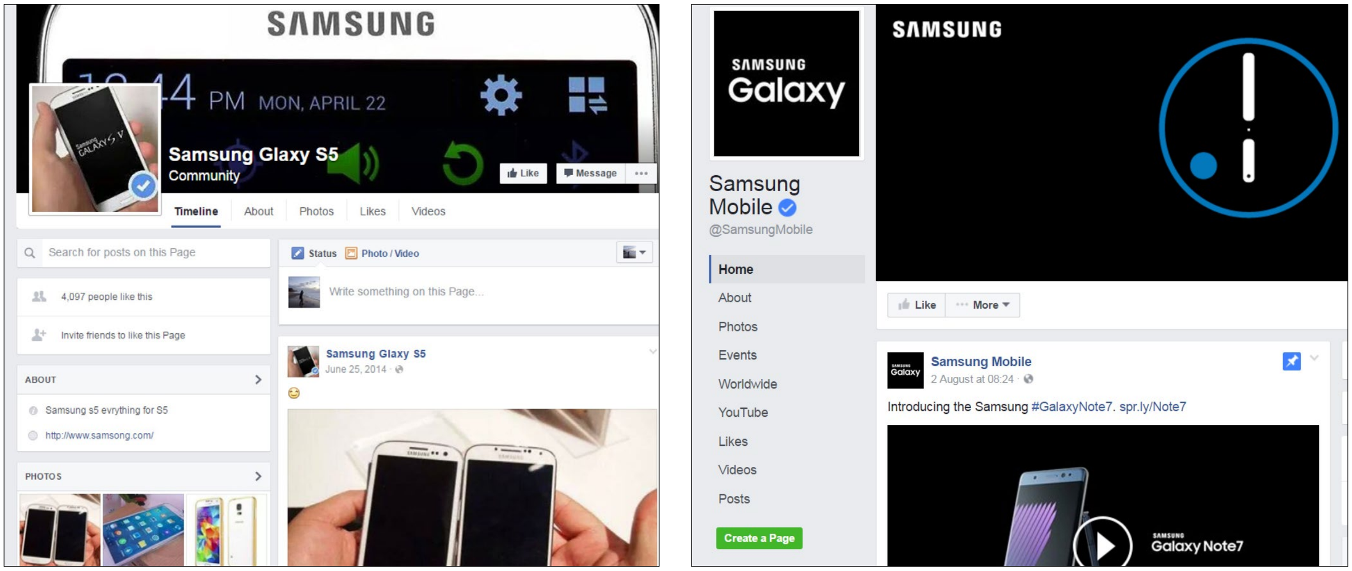
Capital One
@CapitalOne_Help
We're on a mission for our customers—bringing them great products, rewards and service.
McLean, Virginia
✓ captl1.co/social
Joined August 2015

In reply to Dave Wiley
Capital One @CapitalOne_Help · 8 Aug 2015
@DJW629 Visit ✓ capitalone-co.esy.es/cp1.html for your Account Update, Status Report, Bill Payment and other Services. Thank you.

In reply to Fatima Menjivar
Capital One @CapitalOne_Help · 7 Aug 2015
@fatima_jake Visit ✓ capitalone-co.esy.es/cp1.html for your Account Update, Status Report, Bill Payment and other Services. Thank you.

Figure 3: CapitalOne_Help is an example of a fraudulent customer service account created by cyber criminals to defraud unsuspecting customers

Although Twitter and Facebook verification help combat fraudulent accounts, verification is not foolproof. The blue verified badge does not appear in tweets or posts. What’s more, many customers don’t know what the badge means. Fraudsters often mimic the verified badge. They include the blue checkmark in their profile or background images. Even users aware of the badge may not notice that it is in the wrong spot.



4,097 people like this
Invite friends to like this Page
ABOUT
Samsung s5 evrything for S5
http://www.samsong.com/

Samsung Glaxy S5
June 25, 2014

Samsung Mobile
2 August at 08:24
Introducing the Samsung #GalaxyNote7. spr.ly/Note7

Figure 4: Example of a fraudulent Samsung Galaxy account on Facebook. A fake verification badge appears on the left, while the authentic Samsung Galaxy account appears on the right.

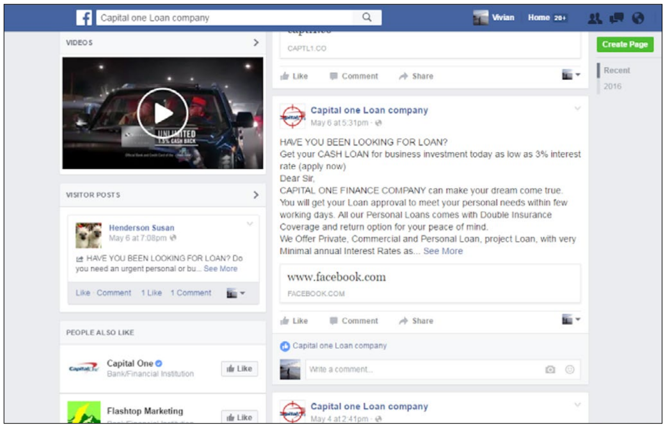
FRAUDULENT ACCOUNT TAXONOMY

Social media fraudsters attack brands in a myriad of ways. Here’s a look at the main types of fraudulent accounts and examples of how some brands have been affected.

Phishing

Social media phishing is the fastest-growing social media threat, increasing 150% from 2015 to 2016. These accounts imitate your brand, product pages, or customer-support pages. The end goal is to bait your followers into giving up their account login details, credit card numbers, or other sensitive information—usually though convincing lookalike login pages.

Fraud is costly. Compromised banking account or credit card numbers can mean large financial losses. And once you’ve lost your customers’ trust, you may never win it back.



Henderson Susan
May 6 at 7:08pm
HAVE YOU BEEN LOOKING FOR LOAN? Do you need an urgent personal or bu... See More
Like · Comment 1 Like 1 Comment

Capital one Loan company
May 6 at 5:31pm
HAVE YOU BEEN LOOKING FOR LOAN?
Get your CASH LOAN for business investment today as low as 3% interest rate (apply now)
Dear Sir,
CAPITAL ONE FINANCE COMPANY can make your dream come true.
You will get your Loan approval to meet your personal needs within few working days. All our Personal Loans comes with Double Insurance Coverage and return option for your peace of mind.
We Offer Private, Commercial and Personal Loan, project Loan, with very Minimal annual Interest Rates as... See More
www.facebook.com
FACEBOOK.COM

Capital one Loan company

Capital one Loan company
May 4 at 2:41pm

Figure 5: Fake Capital One phishing account on Facebook

EXECUTIVE IMPERSONATION FRAUD

Executive impersonation fraud began as an email-based attack method known as business email compromise (BEC). Fraudsters have achieved some big payouts, as seen in the recent attack on Etna Industrie in France. Cyber criminals repeat and build on what works, so it is no surprise that we're seeing the same kind fraud on social media.

What is it?

In executive impersonation fraud, the fraudster pretends to be a company leader to extract funds or sensitive information. (This type of fraud is also called "CEO identity fraud" and the "bogus boss" scam.) With a clear goal in mind, the impostor carefully studies the target. When money is the goal, the fraudster usually targets a senior member of the company's finance team.

Impersonators exploit human nature in two ways. First, they take advantage of the victim's trusting nature by assuming the persona of someone the victim knows and strives to please. Second, they impose time pressure, short-circuiting the victim's normal decision-making process.

How does it work on social media?

The fraudster starts the attack by creating a fake Twitter or LinkedIn account that looks like it belongs to an executive. The handle is usually a slight variation on the executive's real account. For example, if the executive's Twitter handle is @johndoe, the employee targeted by the scam might get a tweet from @john_doe. The fake Twitter account also usually features a bogus verification badge in the profile or background photo.

The fraudster then follows the employee's Twitter handle and sends a tweet or two to build trust. Once that trust is secured, the attack starts. The fraudster might tweet the employee, asking for an urgent money wire transfer. If the goal is corporate espionage, the fraudster asks for confidential information. This can include upcoming financial earnings or details about future product releases.

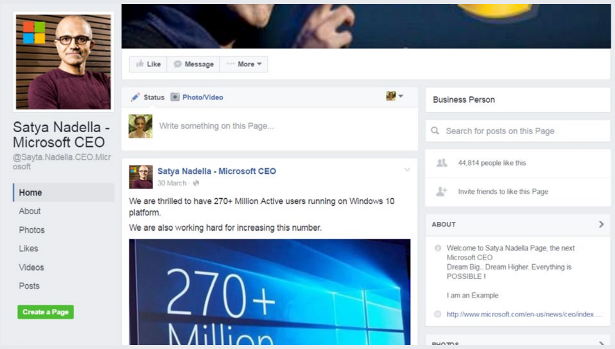
The fraudster pressures the employee to complete the transaction quickly. The impostor might tweet a request for the employee's email. Then to increase the urgency, the fraudster asks about the request again and again over Twitter and email. If the employee has access to the money or information, the only thing standing in the way is his or her caution and due diligence.

Stopping executive impostors

Preventing this kind of fraud on social media is a two-step process: finding social media accounts that are impersonating your executives and taking them down. Here are a few ways for marketing and security teams can reduce the risk.

Automate Detection

Tools such as Proofpoint SocialDiscover can automatically detect executive impersonators. SocialDiscover searches for and details all of the handles, profiles, and pages that are using your executives' information. It looks for authentic Twitter verification badges and identifies profile accounts that show signs of fraud.



Satya Nadella - Microsoft CEO
@Sayta.Nadella.CEO.Microsoft

Satya Nadella - Microsoft CEO
30 March

We are thrilled to have 270+ Million Active users running on Windows 10 platform.

We are also working hard for increasing this number.

Business Person

44,814 people like this

Welcome to Satya Nadella Page, the next Microsoft CEO
Dream Big.. Dream Higher. Everything is POSSIBLE !

I am an Example

http://www.microsoft.com/en-us/news/ceo/index....

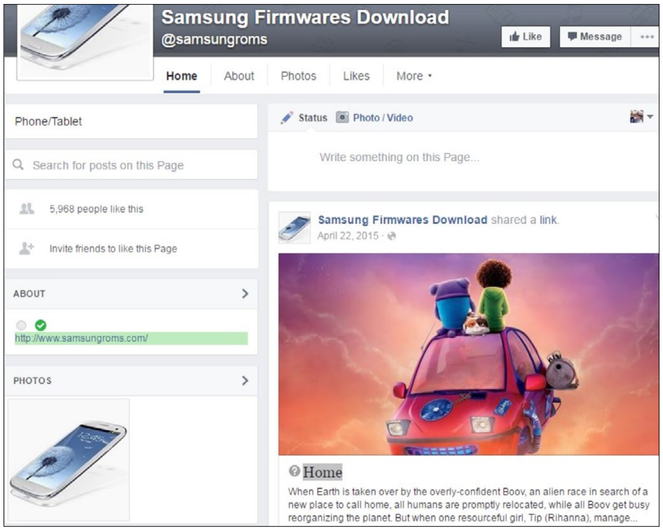
Figure 6: This fraudulent Facebook account impersonates Microsoft CEO Satya Nadella. It has nearly 45,000 followers.

Report Fraudulent Accounts to Social Networks

Once you've determined which social accounts are impersonating your executives, report them to social network platforms for removal. Also, tell your employees to be on the lookout. You can outsource the account takedown process to a managed security service such as Proofpoint Social Media Protection Managed Services.

Malware

Fraudulent malware accounts trick your customers into clicking links that infect their devices with ransomware, keyloggers, or botnets. Typically, the end goal is to harvest personal information from the device and then sell it in a cyber crime marketplace. In the case of ransomware, your customer's device is "held hostage" until the victim pays a fee. Fake brand pages filled with malware links create security risks for your customers and your brand.


Like
Message
Home
About
Photos
Likes
More
Status
Photo / Video
Write something on this Page...
Search for posts on this Page
Invite friends to like this Page
ABOUT
PHOTOS

Samsung Firmwares Download
@samsungroms

Phone/Tablet

5,968 people like this

http://www.samsungroms.com/

Samsung Firmwares Download shared a link.
April 22, 2015

Home

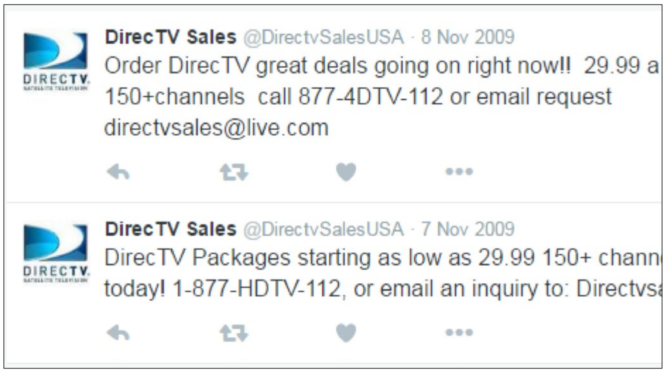
When Earth is taken over by the overly-confident Boov, an alien race in search of a new place to call home, all humans are promptly relocated, while all Boov get busy reorganizing the planet. But when one resourceful girl, Tip (Rihanna), manage...

Figure 7: This fake Samsung Firmware page is peppered with malware links

Scams

Many brand impostors create social accounts that prey on your customers' desire to get a good deal. Scam accounts promise discounts or promotions, collecting credit card numbers from customers trying to cash in on the bogus deal.

Scams are an especially worrisome type of fraudulent account. That's because the allure of a bargain speaks to human nature. It's consumer psychology to get excited about a deal, which gives scammers a strong chance of success. In our research on 10 top brands, 18% of fraudulent social media accounts were scamming attempts.



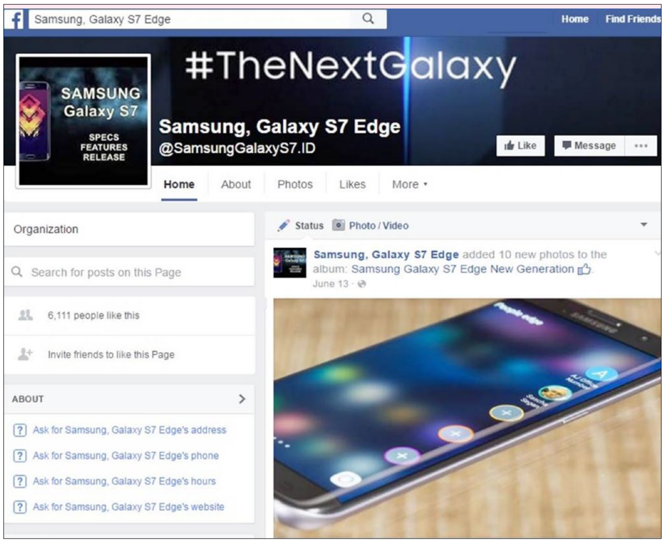
DirecTV Sales @DirectvSalesUSA · 8 Nov 2009
Order DirecTV great deals going on right now!! 29.99 a
150+channels call 877-4DTV-112 or email request
directvsales@live.com

DirecTV Sales @DirectvSalesUSA · 7 Nov 2009
DirecTV Packages starting as low as 29.99 150+ chann
today! 1-877-HDTV-112, or email an inquiry to: Directvs

Figure 8: Example of a Direct TV scam account on Twitter

Counterfeit Products and Services

Counterfeit fraud accounts mimic your brand to sell knockoff or stolen versions of your products and services. This undermines customer trust in your brand and in the quality of your offerings. Counterfeit accounts also hurt sales. Counterfeit products and services accounted for 11% of the 902 fraudulent social media accounts we found among 10 top brands.



Samsung, Galaxy S7 Edge
@SamsungGalaxyS7.ID

Organization

6,111 people like this

Ask for Samsung, Galaxy S7 Edge's address
Ask for Samsung, Galaxy S7 Edge's phone
Ask for Samsung, Galaxy S7 Edge's hours
Ask for Samsung, Galaxy S7 Edge's website

Samsung, Galaxy S7 Edge added 10 new photos to the album: Samsung Galaxy S7 Edge New Generation.
June 13

Figure 10: Example of a counterfeit Samsung Galaxy account on Facebook

ANGLER PHISHING

Fraudulent customer service accounts are one of the most dangerous types of fake account. These accounts are used for a dangerous new phishing variation that we've dubbed "angler phishing."

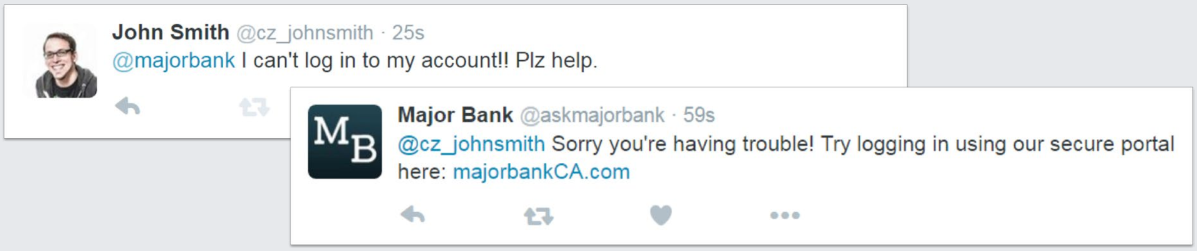
What is it?

Angler phishing attacks get their name from the anglerfish, which uses a glowing lure to entrance and attack smaller prey. In the case of social media fraud, the lure is a fake customer-support message that tricks your customers into revealing sensitive information such as login credentials.

How does it work on social media?

Cyber criminals create highly convincing fake customer service accounts. Then they wait for customers to reach out to your real Twitter account with a help request. The criminals often wait to strike on evenings or weekends, when your customer support team is less likely to monitor social media. When the criminals see a customer contact your brand's account, they hijack the conversation by responding directly to that customer through a fake support page.

The bogus support link in the message contains a link that leads to a convincing but fake version of your company's website. The bogus website asks for the customer's credentials, security questions and answers, or other sensitive information.



John Smith @cz_johnsmith · 25s
@majorbank I can't log in to my account!! Plz help.

Major Bank @askmajorbank · 59s
@cz_johnsmith Sorry you're having trouble! Try logging in using our secure portal here: majorbankCA.com

Figure 9: This mockup of an angler phishing threat is based on a real attack seen on Twitter

How to prevent angler phishing attacks

Angler phishing is a risk for any business that provides customer service on social media. The first step in combatting this threat is finding these fake accounts. Here are a few ways to reduce the risk:

Account Discovery

Angler phishing accounts can be created and taken down in a matter of hours or even minutes. So detecting them quickly is critical. Proofpoint's automated account discovery tool monitors the social universe around the clock; it notifies you as soon as anyone creates a new support account using your brand.

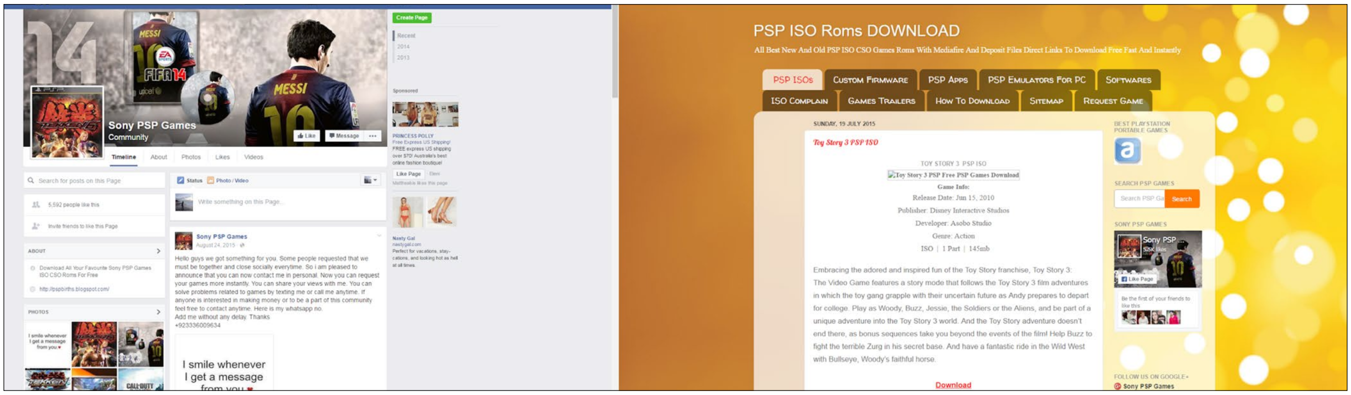
Inform Your Customers

Safeguarding your social media interactions with your customers is important. Proofpoint's Angler Phish Protection notifies you when a fraudulent account contacts one of your customers. Proofpoint can also help you work with social media networks to take the fake accounts down.

To learn more about how you can protect your customers and your brand, visit go.proofpoint.com/angler-phishing.

Advertising

Some fraudulent pages are created solely to generate ad revenue. Enterprising fraudsters use your brand identity to trick followers into visiting junk websites. These sites then spam customers with ads or download adware onto their computers. Advertising fraud accounted for more than two-thirds of 10 top brands' fraudulent accounts.



5,592 people like this

Invite friends to like this Page

Download All Your Favourite Sony PSP Games ISO CSO Roms For Free

http://pspbirths.blogspot.com/

Sony PSP Games
August 24, 2015

Hello guys we got something for you. Some people requested that we must be together and close socially everytime. So i am pleased to announce that you can now contact me in personal. Now you can request your games more instantly. You can share your views with me. You can solve problems related to games by texting me or call me anytime. If anyone is interested in making money or to be a part of this community feel free to contact anytime. Here is my whatsapp no.
Add me without any delay. Thanks
+923336009634

I smile whenever I get a message from you ♥

PRINCESS POLLY
Free Express US Shipping!
FREE express US shipping over $70! Australia's best online fashion boutique!

Nasty Gal
nastygal.com
Perfect for vacations, stay-cations, and looking hot as hell at all times.

PSP ISO Roms DOWNLOAD

All Best New And Old PSP ISO CSO Games Roms With Mediafire And Deposit Files Direct Links To Download Free Fast And Instantly

SUNDAY, 19 JULY 2015

Toy Story 3 PSP ISO

TOY STORY 3 PSP ISO
Toy Story 3 PSP Free PSP Games Download
Game Info:
Release Date: Jun 15, 2010
Publisher: Disney Interactive Studios
Developer: Asobo Studio
Genre: Action
ISO | 1 Part | 145mb

Embracing the adored and inspired fun of the Toy Story franchise, Toy Story 3: The Video Game features a story mode that follows the Toy Story 3 film adventures in which the toy gang grapple with their uncertain future as Andy prepares to depart for college. Play as Woody, Buzz, Jessie, the Soldiers or the Aliens, and be part of a unique adventure into the Toy Story 3 world. And the Toy Story adventure doesn't end there, as bonus sequences take you beyond the events of the film! Help Buzz to fight the terrible Zurg in his secret base. And have a fantastic ride in the Wild West with Bullseye, Woody's faithful horse.

Download

Sony PSP 5.5K likes

Be the first of your friends to like this

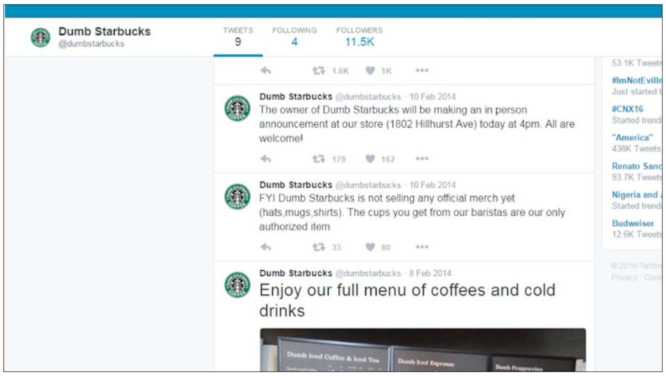
Sony PSP Games

Figure 11: Sony PSP Games is an advertising fraud account on Facebook

Brand Satire and Protest

Political groups and satirists may imitate your brand to embarrass or threaten your company and your customers. They also leverage the popularity of your brand to spread hate speech. These attacks erode the goodwill you've worked so hard to create.

To be sure, some social media activism is legitimate. But other brand-protest pages escalate from rhetoric to direct threats. Monitoring these pages and mitigating risks to your employees and physical offices is important.



Dumb Starbucks
@dumbstarbucks

Dumb Starbucks @dumbstarbucks · 10 Feb 2014
The owner of Dumb Starbucks will be making an in person announcement at our store (1802 Hillhurst Ave) today at 4pm. All are welcome!

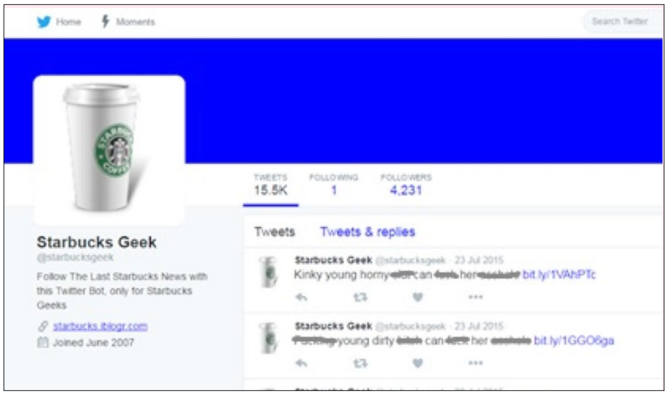
Dumb Starbucks @dumbstarbucks · 10 Feb 2014
FYI Dumb Starbucks is not selling any official merch yet (hats,mugs,shirts). The cups you get from our baristas are our only authorized item

Dumb Starbucks @dumbstarbucks · 8 Feb 2014
Enjoy our full menu of coffees and cold drinks

Figure 12: Example of a Starbucks brand satire account on Twitter

Pornography

Many fraudulent social media pages use your company's popularity to distribute adult content. This can include offensive text and pornography. This abuse of your professional image reflects poorly on your brand and drives customers away. In our research on 10 top brands, pornography accounted for 1% of the fraudulent social media accounts.



Starbucks Geek
@starbucksgeek
Follow The Last Starbucks News with this Twitter Bot, only for Starbucks Geeks
starbucks.iblogr.com
Joined June 2007

Starbucks Geek @starbucksgeek · 23 Jul 2015
Kinky young horny [redacted] can [redacted] her [redacted] bit.ly/1VAhPTc

Starbucks Geek @starbucksgeek · 23 Jul 2015
[redacted] young dirty [redacted] can [redacted] her [redacted] bit.ly/1GGO6ga

Figure 13: Sony PSP Games is an advertising fraud account on Facebook

CONCLUSION & RECOMMENDATIONS

Social media brand fraud is accelerating. The prevalence of fraudulent accounts is a real security threat to anyone engaging on social media.

One thing is clear: social media engagement has tangible benefits. It's no wonder more and more companies are connecting with their followers. The findings in this report serve as an alert on the importance of minimize the threats and protecting your brand. Getting a handle on social media fraud means putting security at the center of your social governance processes.

Here are five ways marketing and security teams can reduce the risks of fraudulent social media accounts:

1. **Identify ownership**
   Define the group within your organization that is responsible for finding and addressing fraudulent social media accounts tied your brand. The task may fall to a social media or security team member. Many companies do this best when security and marketing work together.

2. **Automate brand fraud detection**
   Monitor social networks for fraudulent accounts. Automated tools can streamline this effort. Make sure your tools can scan continuously and alert you whenever a new account is created that uses elements of your brand.

3. **Report fraudulent accounts to social networks**
   Establish a process for reporting fake accounts to social network platforms (Twitter, Facebook, YouTube, and so on) to request their removal. You can also engage a managed security service to help with the takedown process.

4. **Develop a response plan**
   Develop a response plan in the event one of your customers is falls victim to a fraudulent account. Your plan should describe how to respond to issues with scams, malware, and other types of fraudulent accounts. It should also include procedures for escalating issues and communicating with customers.

5. **Communicate Your Social Media Support Hours**
   Denote the hours your team monitors your social media support pages to provide live responses. Consider asking customers to submit inquiries only during posted social-media support hours. This can reduce the window of time available for bad actors to carry out their scams.

Do you need help reducing the risk of social media brand fraud? Proofpoint Social Media Protection solutions automate social media fraud detection. And they help manage other security and compliance risks related to branded accounts.

Visit go.proofpoint.com/sign-up-for-a-demo to get in touch with one of our social media experts.

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.

proofpoint™ www.proofpoint.com