LEARNING MADE EASY

ZeroFOX Special Edition

Social Media Protection

for dummies®
A Wiley Brand

Learn about social media risks

Protect accounts from hijacking

Keep your business safe

Compliments of ZEROFOX®

James C. Foster
Spencer Wolfe
Clara Gustafson

About ZeroFOX

ZeroFOX, the innovator of social media and digital security, protects modern organizations from dynamic security, brand, and physical risks across all social platforms, including social networks, mobile, web, and collaboration platforms. Using global data collection and artificial intelligence-based analysis, ZeroFOX protects modern organizations from account takeovers, impersonation attacks, targeted phishing attacks, credential compromise, data exfiltration, brand hijacking, executive and location threats, and more. Recognized as a Leader in Digital Risk Monitoring by Forrester, the patented ZeroFOX SaaS Platform processes and protects millions of posts, messages, and accounts daily across the social and digital landscape.

Led by a team of information security and high-growth industry veterans, ZeroFOX has raised almost $100 million in funding from NEA, Highland Capital, Silver Lake Waterman, Redline Capital, and others, and has collected top industry awards such as the RedHerring North America Top 100, SINET16 Champion, Dark Reading’s Top Security Startups to Watch, Tech Council of Maryland’s Technology Company of the Year, and the Security Tech Trailblazer of the Year.

Social Media Protection

ZeroFOX Special Edition

**by James C. Foster,
Spencer Wolfe, and
Clara Gustafson**

for dummies®
A Wiley Brand

Social Media Protection For Dummies®, ZeroFOX Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-119-45961-3 (pbk), ISBN 978-1-119-45960-6 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. Some of the people who helped bring this book to market include the following:

Development Editor: Michelle Krasniak

Project Editor: Martin V. Minner

Editorial Manager: Rev Mengle

Senior Acquisitions Editor: Amy Fandrei

Business Development Representative: Ashley Barth

Production Editor: Vasanth Koilraj

ZeroFOX Contributors: Spencer Wolfe (lead author), Clara Gustafson, Benjamin Snowdon, Allison Cannavino, Evan Blair, Sara Ayoub, Daniel Wilkinson, Paul Coe, Amelia Peklar, Chaim Sanders, the ZeroFOX Alpha Team, and James C. Foster

Table of Contents

Introduction

Welcome to *Social Media Protection for Dummies*! This book teaches you how to build a social media protection program so you and your organization can use social media securely.

In this book, you learn about potential risks exposed by social media to individuals and businesses alike. Every day, hackers use social media in harmful ways — ways that affect you! That's why having strategies to protect yourself and your organization before something bad happens is more important than ever.

About this Book

Social Media Protection for Dummies, ZeroFOX Special Edition, is your comprehensive guide to protecting yourself and your business from risks introduced by social media. After reading our in-depth walkthroughs, you will understand how anyone, from a casual user or a small business owner to an information security professional at a Fortune 100 organization, can build an effective social media protection program.

Foolish Assumptions

In writing this book, we assume that you

- Are aware of the general differences among Twitter, Facebook, YouTube, Instagram, LinkedIn, and the other popular social networks, and that you can create or find an account on each.
- Recognize that social networking is becoming increasingly relevant to you, your family, your business, and your customers.
- Either worry about the safety of yourself, your friends, and your family on social media, or work in a role that deals with risks on social media, including information security, marketing, risk and fraud, and others.

How to Use This Book

This book is divided into six chapters:

- Chapter 1, “The Rise of Social Media”
- Chapter 2, “Safeguarding Your Social Media Accounts”
- Chapter 3, “Protecting Your Brand and Customers from Risks”
- Chapter 4, “Managing Fraud, Risk, and Compliance”
- Chapter 5, “Protecting Your Organization Against Security Threats”
- Chapter 6, “Ten Tips for Building a Social Media Protection Program”

Icons Used in This Book

Throughout this book, we provide special icons to call attention to important information. Here’s what to expect:

TIP

This icon identifies helpful suggestions and advice you may find useful at some point.

REMEMBER

This icon is used when something is important to call attention to and bears repeating.

WARNING

This icon is used when you should heed our advice to avoid potential pitfalls.

TECHNICAL STUFF

We use this icon to call out information that we wanted to share, but it is more technical and may be confusing for some readers. Have no fear though . . . it’s okay if this is a little over your head!

Where to Go From Here

If you don’t know where you are going, we’d recommend grabbing a cup of coffee and starting with Chapter 1. However, if you see a particular topic that piques your interest, feel free to jump ahead to that chapter. Each chapter is written to stand on its own, so you can start reading anywhere and skip around as you see fit.

IN THIS CHAPTER

- » **Exploring social media's global growth**
- » **Diving into the rise of cybercrime**
- » **Protecting your accounts from hackers**

Chapter 1 The Rise of Social Media

The most recent and profound development in digital communication is the global adoption of social media. The majority of top social networks continue to see rapid growth in monthly active users (MAUs), and Facebook boasts billions of users across its platforms. Try imagining it this way: If Facebook's users all lived in the same country, it would be the most populous on Earth.

In this chapter, we present some fascinating statistics about how social media has changed the way people communicate.

Everybody is Using It . . .

According to Adweek, the average person will spend more than five years of his or her life on social media. Pew Research Center reports that 79 percent of online adults in the United States have a Facebook account. Furthermore, two-thirds of those users log in every day.

Social media has also exploded as a business communication platform because, in our connected world, almost all consumers engage with brands online. In fact, 81 percent of consumers' purchasing decisions are influenced by their friends' social media posts.

Brands have taken note: According to the 2017 CMO Survey, nearly one-fifth of marketing budgets are spent on social media. Social media has played a pivotal role in elections, revolutions, business transactions, personal and professional relationships, and the global distribution of cat videos.

. . . Including Criminals

Social media's rising popularity presents cyber criminals a fresh battleground, ripe for exploitation. Given the relational nature of social media, the virtual proximity of hackers to their victims has never been closer. Social media attacks such as identity theft, consumer scams (for example, fake coupons), phishing, malware distribution, and account hijacking have skyrocketed in recent years.

Security experts agree: According to Norton, only one in ten employees open unsolicited emails, but nearly one in three accept unsolicited friend requests on social media. McAfee reports that employees experience cybercrime more often on social media than any other business platform, including email.

Cisco's most recent Annual Security Report revealed that Facebook scams are the #1 most common way to breach a network, and, according to a Panda Security report, 20 percent of businesses are infected by malware directly through social media. The University of Phoenix published that 66 percent of U.S. citizens have had an account hijacked.

These risks can have massive financial implications. A recent Symantec survey reports that a social media incident costs an organization an average of $3,588,611.

These numbers should raise warning flags for both businesses and individuals. Ultimately, social media lowers a hacker's barrier to entry. Even an inexperienced hacker can create a fake persona, find targets, and rapidly spread malware or phishing links to billions of people across the globe. Worst of all, the targets have never been more numerous or trusting.

Social media attacks can be intimidating to understand and incredibly costly to detect and defend against. It's time to learn from the professionals and deploy the ultimate social media protection program. Chapters 2-6 of this book detail how everyone — from individuals to information security teams at Fortune 100 organizations — can protect themselves on social media.

IN THIS CHAPTER

- Securing your social media accounts
- Understanding each social network's built-in security options
- Configuring advanced security settings

Chapter 2 Safeguarding Your Social Media Accounts

Your social media accounts are an important extension of your identity, whether you have millions of followers or just use social media to keep tabs on your high school friends. Your accounts likely contain personal data, which makes keeping your accounts safe and secure even more critical.

An unsecured social account can lead to both online and offline risks and criminal activity. An identity thief might use your publicly posted information to guess the recovery questions for your bank account. A cyber criminal might circulate a tailored phishing message related to your interests, hobbies, or family to grab your attention and convince you to click, ultimately stealing your account credentials. A burglar might find your address and rob your house while you post pictures from your Bahamas vacation. A wily hacker might break into your social accounts, read your sensitive direct messages (DMs), install malware on your laptop, and further target your connections, such as friends, family, and coworkers.

In this chapter, we talk about how to start safeguarding your social media accounts.

The Basics: Securing Your Account

The good news is that securing your accounts is relatively easy. The first part of the process involves some basic principles that apply to every account you own:

- **Set up two-factor authentication.** This is one of the best ways to protect your account from hijacking. With two-factor authentication enabled, hackers require access to both your phone *and* your password to take over your account. So even if hackers figured out your password, they would also need to hack into or physically possess your phone.
- **Be wary of suspicious direct messages and connection requests.** Fraudulent accounts, misleading messages, and shortened links are common techniques hackers use to attack their victims.

  TIP

  Make sure to check that accounts are "verified" when following high-profile users. In general, if something seems too good to be true, then it probably is!
- **Assume that anything you post is fair game for hackers to exploit.** Hackers make informed guesses about passwords and account recovery questions to hack into accounts. Studies show that more than 50 percent of account recovery questions can be answered by mining data from a user's social media accounts. For example, if the security question is, "What is your pet's name?", and you routinely post about your cat Munchkin, you have given hackers exactly what they need.

  TIP

  Consider using incorrect information to answer your recovery questions.

  REMEMBER

  Minimize the information you post online, or at least apply the appropriate privacy settings so only close friends or connections can see private information.
- **Use a strong, unique password for each social network, and change it regularly.** Try an encrypted password manager like LastPass or Dashlane to make managing passwords easier.

  Using a single password across all your accounts doesn't cut it. Use long, randomized passwords with a mix of numbers, letters, and symbols. Remember: The longer your password, the stronger and better it is!

TIP

When you're creating a password, *length* is more important than *entropy* (or the randomness of the characters). A long password consisting of all lower-case letters is more secure than a short password with lots of special characters, uppercase and lowercase letters, and numbers. Try creating a nonsensical sentence or phrase that you can remember, but an attacker can't guess.

- **Make sure you're signing in to the real social network website.** Hackers commonly create a website that looks like a real social media site, but it is actually an entirely different page meant to steal your username and password. Make sure you always use **https://** when typing a URL into the browser's address bar. This creates a secure connection to the sites you visit.

REMEMBER

When possible, type URLs into the address bar rather than clicking links. Hackers frequently use shortened URLs on social media to trick users into going to fake sites instead of real ones. That's why it's good to get in the habit of checking whether your connection with the site is secure by hovering over the site's URL in your browser address bar.

- **Keep your device's software, social network mobile application, and browser up to date.** Ensure your mobile phone, computer, and operating systems are updated to maximize your chances of avoiding an attack. Technology and device vendors such as Apple, Google, and Microsoft regularly provide new, more secure software versions and updates — always update! Consider using additional security and encryption tools and processes on your device, such as disk encryption or anti-virus technologies.
- **Encourage your friends and family to be mindful of security measures, too.** The safer your personal network is, the safer you are.

Tips for Advanced Users and Business Account Owners

Sometimes, certain methods to protect social media accounts are sufficient for the everyday user but aren't enough for businesses.

Here are some more advanced account protection options that go beyond the basics:

- **Use a data breach research tool, such as HaveIBeenPwned, to verify you haven't already been affected by a breach.** Even if you're careful online, attackers frequently breach websites or services that you may have used. Keep track of websites where you have accounts that could be affected by a breach. For example, if your PlayStation account gets compromised and you use a similar password for Facebook, make sure to change both passwords.

  TIP

  Register for an account monitoring service to ensure your online data is safe.
- **Configure account monitoring for unexpected activity.** Many people do not discover that their account was compromised until long after the breach occurred. This delay lengthens the exposure time, which, in turn, maximizes the damage an attacker can do. Monitoring services, such as ZeroFOX, can quickly notify you when your account exhibits signs of compromise and help you regain control over your account when there are unexpected account changes or activity.
- **Stay up to date on the latest social media scams and tactics.** Attacks are always evolving, and it's tough to stay on top of everything that's happening. Monitoring services release regular notifications on the latest social and digital media threats, as well as how to avoid them. These services also keep you updated on any changes you need to make to keep your social media accounts secure.
- **Have communication and action plans in place.** Each social network has different support processes in place for reporting and remediating account hacks, security threats, or vulnerabilities. Familiarize yourself with each network's procedure so you can act quickly and appropriately if you notice suspicious activity.

To-Do's for Each Social Network

Every social network has different levels of functionality and customization for privacy and security. Here is a run-down of what top social media platforms have to offer.

Facebook

You can protect your Facebook account in a number of ways, including these:

- **Use Facebook's security checkup tools to walk you through your security settings.** These tools emphasize all the key parts of your account and the changes you should make to improve security and privacy. Configure login notifications and take action when you receive an alert for unexpected account access (a login attempt that you didn't initiate).

  WARNING

  Remove unused applications connected to Facebook because many of them can access personal details that you don't want to share. Make sure every connected application is one with which you meant to share details and grant Facebook profile data access.

- **Be careful about which friend requests you accept.**

  TIP

  Regularly reassess your friend lists by examining which connections seem suspicious or are no longer relevant to your network. Limit inbound friend requests from strangers by changing the Facebook setting called, "Who can contact me?"

  TIP

  Review birthday alerts found in your notifications every day, and remove friends with whom you are no longer close. This is an easy way to regularly comb through hundreds of connections without allocating time upfront.

- **Tighten up your content privacy settings.** Always ensure that posts and pictures you are tagged in have limited visibility settings in place. Do not post pictures that indicate you're currently away from your home, business, or office for an extended period.
- **Watch out for fake accounts, pages, apps, and games.** These may look like the real thing, but are frequently used for nefarious purposes like propagating scams or phishing users. Remember, if it looks too good to be true, it probably is.

Twitter

One of the best ways to keep your Twitter account secure is by closely monitoring who you interact with. For example:

- **Only follow people you trust.** Pay attention to who you're following because following a malicious account will expose you to more spam, scams, phishing links, and other questionable content.
- **Only allow followers you know and trust, and be careful about what you post.** Twitter is one of the most public social networks. It was built to maximize your personal brand exposure, which means you're also maximizing the visibility of the information that you post. For example, tweeting that you're traveling for the week can leave your home or office open to burglary.

  TIP

  Tweeting any personal information means it's fair game for everyone to see. A good rule of thumb is if you wouldn't be comfortable shouting the content of your tweet off a balcony to a busy street below, then you should think twice about posting.

  REMEMBER

  Regularly review your own followers, especially if you have multiple accounts — professional and personal — and thoroughly track new followers on all accounts.
- **Tweets are searchable unless security features are enabled by the user.** If you only want to share content with your close friends, make sure you enable the "Protect my Tweets" feature and set your account to private. You can see that your profile is private if a lock icon is appended to your name on your profile.

  TIP

  If your account is not private, turn off the Tweet Location setting so that your location is not exposed to the public when you post tweets.

Instagram

Take proper safety precautions when using Instagram. Here are some key steps to follow:

- **If your account is not private, all posts and comments are visible to any Instagram user.** Keep that in mind when posting information about your business or anything that could be considered sensitive.

- **Allow only those you know and trust to follow your account.** If you manage a corporate account, you may want to verify the users following your organization and post wisely.

  TIP

  When protecting your brand's followers, choose to automatically hide offensive comments so that inappropriate content isn't visible to your followers.
- **Ensure that no personally identifiable information is available on any of your posts or in your biography.**
- **Report accounts that misuse hashtags or handles, or spread other "spam"-related content.**

LinkedIn

Because LinkedIn is for professionals, it is popular among hackers targeting your employees and business. Here are some guidelines to keep in mind:

- **Only establish connections with people you know and trust.** Consistently review your connections to ensure you're comfortable with all the people in your network.

  It is easy to grow your professional network, but do so only if the accounts you're accepting are valid. Even if the connection request contains a tailored message about meeting at a recent networking conference you attended, make sure that the profile is real and inspect the longevity of the account and its mutual connections.
- **Do not open links sent from connections whom you do not know or trust.** Sending messages on LinkedIn is easy, so be wary about what you accept and from whom.
- **Be wary of sales or recruitment messages that contain links, ask for sensitive data, or request payment.**

YouTube and Google+

Two other "Big Six" social media sites, YouTube and Google+, also require caution. Follow these steps:

- **If setting up an account for a younger family member, enable Restricted Mode.**

- **Ensure that private videos posted to YouTube are designated either as Unlisted or Private.** Unlisted videos can be accessed by anyone with the link, but are unsearchable within the social network and do not appear on your channel.

REMEMBER

Private videos are accessible only to YouTube users whom you invite to the video.

EIGHT STEPS TO TAKE RIGHT NOW

You don't need to finish this book before you can take control of your security on social networks. Here's a checklist of steps you should take right now:

1. **Change your passwords.** Make sure to change them at least three times per year or as frequently as possible.
2. **Enable two-factor authentication** for all your personal and business social media accounts.
3. **Ensure personal information is kept private** — including email address, mobile phone number, physical address, and date of birth. It is a best practice to make this information invisible to anyone other than yourself.
4. **Do not publish sensitive details** about your job and workplace.
5. **Regularly review your lists** of friends, followers, and connections.
6. **Make your friends, followers, and connections lists private.**
7. **Regularly search for impersonations** of you or affiliated organizations, brands, businesses, family members, and employers.
8. **Ask your employer for the corporate social media policy** to ensure you are compliant with work-related social media guidelines. If your company doesn't have a formal policy, suggest that one be created.

IN THIS CHAPTER

- **Identifying social media risks to your business**
- **Protecting your brand and social sales channel**
- **Securing customers from fraud and scams**
- **Building a social media brand protection program**

Chapter 3 Protecting Your Brand and Customers from Risks

Social media has become one of the most critical elements of a successful marketing mix, offering marketing and sales teams the ability to directly engage with millions of prospects and customers. Nearly every consumer uses social media, and brands are competing for all the same impressions and conversions.

In this chapter, we provide an overview of how a brand's reputation can suffer on social media, as well as how account impersonation is one of the most common hacker methods.

Why Protect the Brand?

Earning customer loyalty is a difficult endeavor. According to Accenture, 78 percent of consumers report they are retracting brand loyalty at a faster pace than three years ago. In fact, McKinsey reports that only 13 percent of customers are truly loyal and don’t shop around. Furthermore, consumer commitment is at an all-time low: Keeping customers engaged is costly given consumers’ desire for new, fresh content. All of the above makes the protection of customer trust — and ultimately their wallets — even more critical.

To make matters worse, the ways that brands are damaged are increasingly diverse and difficult to combat. Customer scams can come from malicious individuals impersonating a brand or its representatives. Other issues arise when customers unwittingly post sensitive personal data to a company page or a social media troll spams corporate accounts with inflammatory content.

REMEMBER

Other types of risks can originate from *inside* an organization — for example, when an employee unintentionally discloses sensitive corporate information or intentionally slanders the business on social media.

Building and preserving brand reputation has never been more important or more difficult. Organizations are responding in kind: A recent Forrester survey reports that reputational risk is the second most pressing organizational risk, behind only information security and privacy risks. In fact, social media risks span all three: reputational, information security, and privacy.

Account Takeovers

Account takeovers, also known as account hijacking, are a popular hacker technique in which an attacker gains access to a business-owned, consumer, or corporate user’s social media account to post malicious, slanderous, or embarrassing content.

Account takeovers are the worst-case scenario for marketing teams. In an instant, a company’s primary tool for brand building becomes a weapon against it and its loyal followers. Hackers post scam and phishing links, send malware via direct messages, and disseminate fake promotions to followers.

A hacked business account undermines consumer confidence in a company’s security practices. The results can be particularly damaging for companies in highly-regulated industries like finance, e-commerce, or healthcare, or in any sector where security is a competitive differentiator. Additionally, a breached account can lead to a massive PR crisis that costs time, money, and followers.

Ultimately, a company is left with a seriously damaged reputation and diminished ability to engage customers and prospects online.

How often do accounts get hijacked? Independent research claims that over 600,000 accounts are hacked each day. Norton reported that one-fifth of social media users reported having at least one account hacked. A more recent University of Phoenix report puts that figure even higher, stating that two-thirds of all U.S. adults have had accounts hacked!

Securing a social media account, like securing a company website before it, involves collaboration. We strongly encourage marketing, IT, and security teams to work together.

REMEMBER

The more people who have access to an account, the more at risk you are. Limit access to limit exposure!

Some social networks, like Facebook and LinkedIn, require users to access a company page via an individual account. We recommend that teams regularly review account access, including third-party apps, and remove unauthorized or unused users and apps.

CASE STUDY: BREACHED APPLICATION LEADS TO COMPROMISED ACCOUNTS

In early 2017, hundreds of social media accounts were hijacked by cybercriminals. After a contentious week of deteriorating relations between the Netherlands and Turkey, cyber criminals posted aggressive messages about the Netherlands, using swastikas and calling the Dutch “Nazis.” The hacks stemmed from a vulnerability in a third-party application, Twitter Counter.

The breached accounts included many global brands and well-followed, verified accounts including Forbes, the official Bitcoin Blockchain account, Sport City gyms in Mexico, Starbucks, the European Parliament, UNICEF, Nike, and Amnesty International, as well as many personal accounts.

The attack propagated through a third-party app, proving that password updates alone don’t offer enough protection. Social media and information security teams must adopt a more comprehensive approach to fully securing accounts.

TIP

Marketing teams can also leverage a password management tool to share passwords securely among the team. For a full, network-by-network guide to securing social media accounts and tightening up existing security settings, see Chapter 2.

Brand Impersonations and Scams

Brand impersonations are any fraudulent or fake account masquerading as a brand or an official representative of a brand — such as a customer support agent — usually with the intent of scamming customers or launching cyber attacks. Brand impersonations are easy to create, and attackers can immediately select targets from the list of users who follow or engage with the authentic account. For this reason, a company's most active, loyal customers are often hit the hardest. See Figure 3-1 for an example of a customer service account being impersonated, as well as the hacker's phishing attempt.

Scams are attempts by hackers to fool customers into believing they are interacting with your organization, only to steal or extort their data or money. Scams include fake coupons, money-flipping offers, fraudulent promotions, malicious credit card services, technical support fraud, sales promotions, job advertisements, and much more.

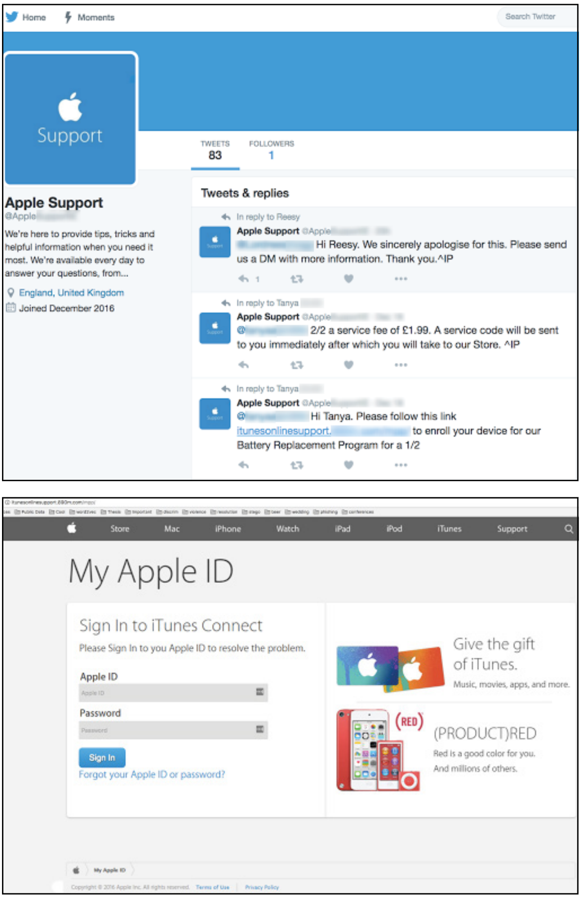
REMEMBER

You can lose an immense amount of business if even a fraction of customers fall victim to one of these scams — especially if those customers refuse to engage with your company in the future.

Because the cost of a scam is the lifetime value of a customer, a successful social media scam campaign at scale can be incredibly costly. Many organizations, especially retailers or those in the travel industry and financial services, reimburse their customers the cost of the scam, either from a legal obligation or as a gesture of good will.

Finding fake accounts in the wild can be daunting. Companies can manually search for their brand name and flag any potentially malicious accounts for removal. However, this approach is inefficient and doesn't comprehensively solve the problem. For example, scammers often impersonate company representatives such as technical support agents instead of the brand itself, which makes identification harder for brand protection teams.

Moreover, this approach is not continuous because an attacker can create, launch, and subsequently take down an attack in a matter of days or hours. Unless organizations search at the exact right time, most attacks are missed.



Apple Support
@Apple[redacted]

We're here to provide tips, tricks and helpful information when you need it most. We're available every day to answer your questions, from...

England, United Kingdom
Joined December 2016

Tweets & replies

In reply to Reesy
Apple Support @Apple[redacted]
[redacted] Hi Reesy. We sincerely apologise for this. Please send us a DM with more information. Thank you.^IP

In reply to Tanya [redacted]
Apple Support @Apple[redacted]
@[redacted] 2/2 a service fee of £1.99. A service code will be sent to you immediately after which you will take to our Store. ^IP

In reply to Tanya [redacted]
Apple Support @Apple[redacted]
@[redacted] Hi Tanya. Please follow this link itunesonlinesupport.[redacted] to enroll your device for our Battery Replacement Program for a 1/2

My Apple ID

Sign In to iTunes Connect

Please Sign In to you Apple ID to resolve the problem.

Apple ID: Apple ID

Password: Password

Sign In

Forgot your Apple ID or password?

Give the gift
of iTunes.
Music, movies, apps, and more.
(RED)
(PRODUCT)RED
Red is a good color for you.
And millions of others.
My Apple ID
Copyright © 2016 Apple Inc. All rights reserved.
Terms of Use
Privacy Policy

FIGURE 3-1: Scammers impersonate support account to direct customers to phishing pages. For example, the login page on the bottom is fake.

TIP

Automation provides a powerful solution. Social media protection tools can analyze account names, handles, bio fields, images, and more to determine if an account is fraudulent, in real-time and at scale. Advanced algorithms can also tell the difference among parody accounts, fan accounts, and truly malicious ones.

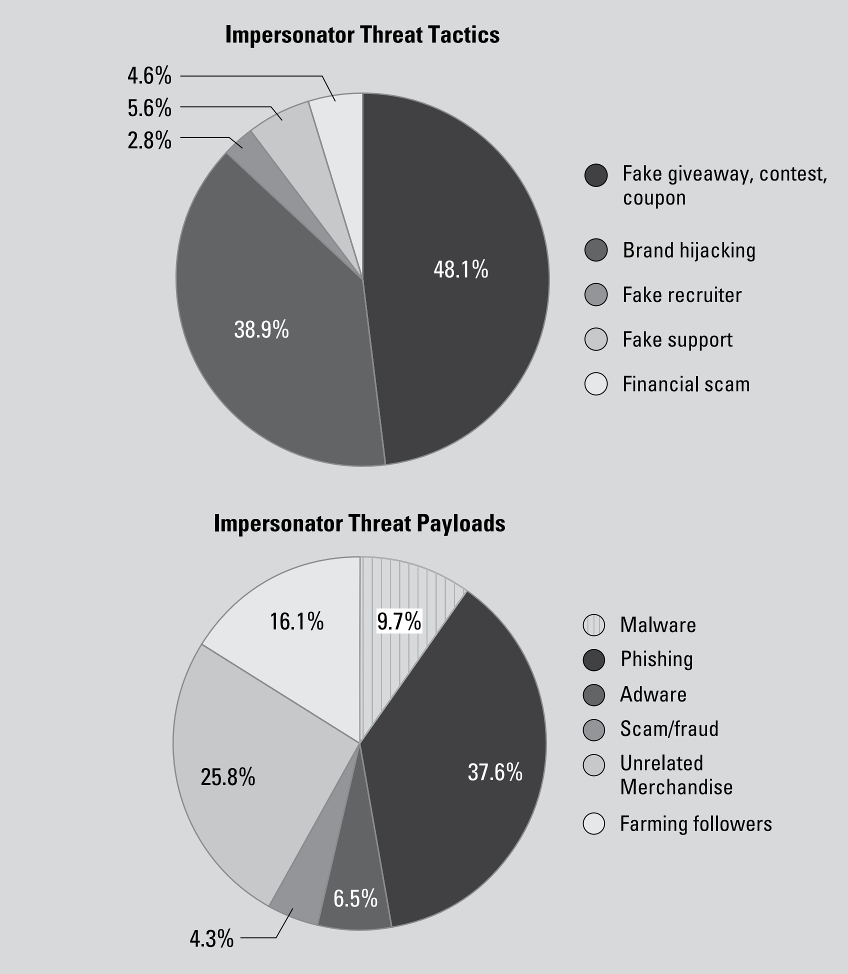
WHAT ARE ALL THOSE FAKE ACCOUNTS UP TO?

In a study of 40,000 fraudulent social media accounts, the ZeroFOX Alpha Team researched what impersonators do on social media, what kind of attacks they perform, and how they spread their campaigns to unsuspecting users. The tactics used were devious and diverse, ranging from traditional social engineering ploys to attackers actually contributing advertising dollars to proliferate the scam and reap higher rewards. See the accompanying figures for more details.

Traditional payloads such as phishing and malware were common, but there were also a larger set of threats unique to impersonations on social media. These included unseen scams, fraud, brand abuse, and follower farming.

Here are some of the findings:

- In the last two years, the overall number of impersonators increased 11x.
- Nearly half of all malicious social media impersonators disguise their payload as a fake coupon or giveaway using the brand to attract promotions seekers, thus targeting a brand's most loyal customers.
- More than one-third of all malicious social media impersonators send their target to a phishing page to steal social media account credentials, credit cards, and personal information.
- Some impersonators spoofed the social networks themselves, offering fraudulent "verification" services and the authentic "blue checkmark" service meant to distinguish popular real accounts from fake ones. Verification impersonators are systemic across social media and were found on all social networks.
- Impersonators regularly wipe accounts and leave them dormant to avoid detection between attack campaigns. They later return to these accounts and weaponize them in new ways.
- Impersonators post links to other social networks with malicious links and payloads. This kind of cross-network pivoting makes it difficult for the primary network to detect abuse.



Offensive Content

Offensive content is any content that violates brand or community guidelines pertaining to profanity, pornography, hate language, competition, or violence. Examples include a disgruntled follower or troll posting racial slurs on a Facebook page, spam posted in a YouTube comment, or a customer unwittingly disclosing personally identifiable information (PII) on LinkedIn.

Marketers must watch their owned social media assets for unwanted content. Marketers should continuously monitor accounts featuring a profile or "wall" that can be posted to or commented on, such as Facebook, LinkedIn, and Instagram, and remove or hide any content that might harm or offend customers.

Rogue Accounts

Any organization with a decentralized brand — such as franchises, organizations with multiple physical locations, highly diversified conglomerates with sub-brands, or organizations that market products and services separately — run the risk of accounts being created outside the purview of the marketing or customer support teams. Rogue accounts are also common for organizations that have rebranded or restructured their social media strategy.

Some social networks, notably Facebook and LinkedIn, automatically generate location pages when users tag themselves at a business location. Although these accounts are not malicious in the same sense as impersonations, they can confuse customers and draw attention away from business accounts.

TIP

Rogue pages can be merged into owned pages or the company can request that the social network remove them. This review process is critical for centralizing traffic through a single account or set of accounts. We recommend using an automated platform to help address this problem at scale.

MARKETING TEAM CHECKLIST

Here are some actions for teams looking to protect their brand on social media:

- **Work with the IT and security departments to establish a social media protection program.** The size, scope, and responsibilities of the team will vary based on your industry, risk tolerance, and most pressing threats. See Chapter 6 for a step-by-step process for building a social media protection program.

- **Adopt a social media management platform like Hootsuite Enterprise to centralize all your social media publishing activity.** This allows every member of the marketing team (or other groups that may have a need to publish on social media) to access the same accounts while using their own individual login credentials. Regardless of whether or not you use a management platform, be sure to mandate (through your pre-defined social media policy) the use of two-factor authentication.
- **Regularly audit all third-party applications that have been granted permissions on corporate social media accounts.** Organizations should have a protection platform in place that can both identify when an unapproved application is operating their accounts and restrict the third-party applications to a predefined list.
- **Identify accounts impersonating your brand.** Use a social media protection tool like ZeroFOX to identify accounts that use your logo or messaging to carry out malicious activity. The definition of an impersonator varies from network to network, but all social networks provide the ability to remove accounts violating their Terms of Service. This process can be automated with a social media protection tool.
- **Work with the customer support and PR teams to build a rapid response team.** When something goes wrong, marketing and PR teams must have a plan in place to address the fallout. The security team should own the remediation component of the plan.
- **Monitor business accounts for inbound sensitive or offensive content.** Business accounts on platforms like Facebook, Instagram, and LinkedIn allow page owners to moderate content. Establish community guidelines for offensive and sensitive content. The ability to immediately block, hide, and delete content is even better; some social networks offer this capability, or try using a social media protection tool.
- **Monitor brand hashtags for abuse.** Social media protection tools can flag when scammers and cyber attackers leverage your hashtags to spread threats to your social ecosystem.
- **Work with the security team to create robust security settings for brand accounts.** See the detailed steps in Chapter 2 as a springboard for securing accounts. These are the first, least expensive, and most effective steps in preventing an account hijacking.
- **Report threats and abuse to the social media networks for takedown.** Networks will take down anything in violation of their Terms of Service, including customer scams and impersonations.

IN THIS CHAPTER

- Establishing risk tolerance
- Understanding social media governance
- Exploring the different types of social network fraud
- Maintaining compliance on social media
- Leveraging tailored social media training and protection for employees

Chapter 4
Managing Fraud, Risk, and Compliance

Fraud, risk, and compliance teams own the complex responsibility of proactively navigating social media challenges, which are complicated by an inherently dynamic, real-time dataset that is typically offsite and not owned by the business.

Issues range from inbound fraud that targets company stakeholders — such as customer scams and recruitment fraud — to outbound risks such as executives posting non-compliant content or employees leaking sensitive information. The most difficult task in addressing these "unknown unknowns" is identifying them before they cause lasting damage. Moreover, scams, fraud, tactics, and risks change rapidly, and predicting the future of risk is nearly impossible.

In this chapter, we take you through the different types of fraud and show you several ways you can protect your organization.

The Four Main Types of Fraud

Not surprisingly, social media fraud is diverse.

Fraud against customers

For scammers, social media is a powerful new tool to exploit a specific, bulk group of users such as a brand's followers or a business' customers. Social media allows scammers to target these users because a brand's follower lists can be easily identified. Scammers can further subdivide a brand's customers into segments — such as single mothers, the military, or holiday shoppers — based on the information they share with the social networks, all in the interest of making an attack more specific, and therefore more successful.

REMEMBER

Customer-targeted scams usually tease users with a lucrative reward and use the false credibility of a brand's logo to indicate that a fraudulent offer is legitimate.

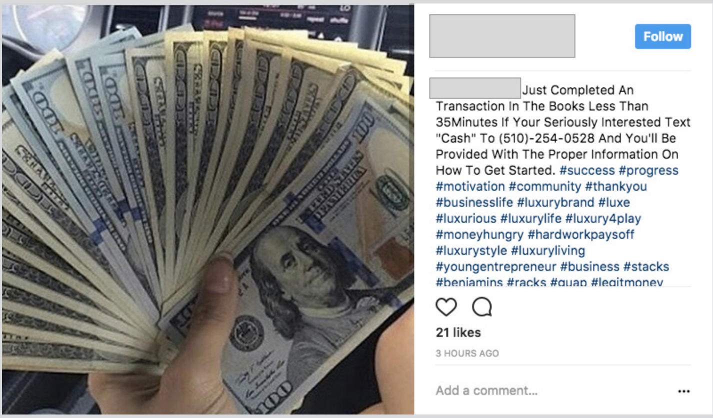
These scams thrive on social media because they are easy to create, cost effective, and can be distributed to the target audience at scale. Even a non-technical scammer, located anywhere in the world with nothing more than an Internet connection, can create a group of fake accounts that are built to lend credibility to one another and launch a coordinated scam campaign.

Given social media's scale, scammers are bound to tempt some targets to bite. By imitating a company, the scammer explicitly targets the company's current or would-be customers, resulting in missed revenue, support costs, and lost business.

CASE STUDY: FINANCIAL CRIME THRIVES ON SOCIAL MEDIA

Over a four-month period, the ZeroFOX Alpha Team identified thousands of scams targeting major financial institutions and their customers across Instagram. The team analyzed Instagram posts in relation to 37 of the biggest U.S. financial institutions. The study encompassed more than 2 million posts from the last two years.

The schemes, called *money flipping scams,* extort victims into sending money or disclosing banking information. The scammer promises to "flip" the victim's money and return a huge profit. They use Instagram to advertise services with pictures of money, luxury goods, and drugs, as well as hijacking hashtags to target a bank's consumers. The accompanying figure shows a typical money flipping scam. At the end of the day, the banks often eat the cost, resulting in considerable financial loss for consumers and banks alike.



[redacted] Just Completed An Transaction In The Books Less Than 35Minutes If Your Seriously Interested Text "Cash" To (510)-254-0528 And You'll Be Provided With The Proper Information On How To Get Started. #success #progress #motivation #community #thankyou #businesslife #luxurybrand #luxe #luxurious #luxurylife #luxury4play #moneyhungry #hardworkpaysoff #luxurystyle #luxuryliving #youngentrepreneur #business #stacks #benjamins #racks #guap #legitmoney

21 likes

3 HOURS AGO

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.

Recruiting fraud

As organizations increasingly use social media sites to recruit and engage talent, those with malicious intent can leverage that same medium for financial gain or other types of theft.

REMEMBER

Pay-to-play recruitment scams are easy to perpetrate and often used to exploit individuals making a career change. Scammers target prestigious, high-paying industries such as tech, oil and gas, or financial services, pretending to be recruiters from those industries. Scammers collect fraudulent application fees or coerce applicants to disclose sensitive information that can later be sold or exploited for identity theft.

Fake recruiters continuously monitor job sites for new targets. Scammers also tend to target individuals who are fresh out of school and eager to land their first job. These characteristics make this group particularly vulnerable because they usually feel pressure to find employment and want to make an engaged and positive first impression with a potential employer. Some scams even offer student loan or debt forgiveness to augment the urgency of the offer.

To facilitate a healthy environment where employers and candidates can engage, organizations can work to purge their social ecosystems of attacks targeting job candidates.

TIP

Companies should post their recruitment policies and procedures publicly to help reduce confusion. Moreover, they should actively search for and report fake accounts that target their job candidates.

Fraud targeted at employees

An organization's employees are also vulnerable to fraud and risk on social media.

Fraud targeted at employees frequently takes the form of a fake account masquerading as someone else in the organization, often a human resources (HR) manager or a supposed new hire looking for help. Predictably, employees are most often targeted on professional networks like LinkedIn. Fake HR managers ask for government issued identity numbers and other confidential or sensitive data and send malware-laced files disguised as paystubs.

Even more convincing than a fake account is a compromised real account. In these cases, the fraudulent request or malicious message in line with whatever conversation has been taking place originates from an otherwise legitimate and trusted source. Until the real account owner regains access to the account, there's no straightforward way for the connections to know they have been taken over.

Businesses can protect themselves through a combined approach:

1. Train employees to understand what information should be shared via social media.
2. Teach employees how to identify a fake or breached account.
3. Automatically identify employee-targeted fraud at scale.

A social media protection tool can automate fraud detection and remediation.

Piracy and counterfeit goods

No longer are counterfeit goods sold only on the main streets of major cities or in the dark corners of the Internet. Underground marketplaces have emerged on public channels, including social networks, fueled by the ability to create fake accounts and market goods just as the genuine brand would. The ultimate victims of these crimes are the bottom lines of the companies producing the authentic products.

Peddlers of stolen, pirated, or counterfeit goods (such as those seen in Figure 4-1) leverage company branded hashtags and keywords to get their wares in front of would-be real buyers.

Although piracy and counterfeiting violate social networks' Terms of Service, the onus is generally on a company to identify, report, and authenticate abuse. Organizations with robust controls to find and report piracy are protecting the integrity of their marketing efforts, maximize the return from their promotional efforts, and safeguard their customers from scams and cyber attacks piggybacking off stolen or pirated goods and content.

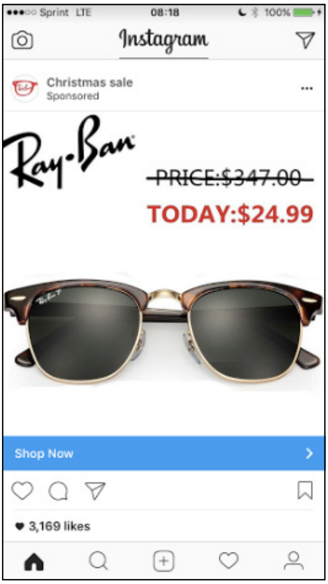


FIGURE 4-1: An example of counterfeit goods advertised on social media.

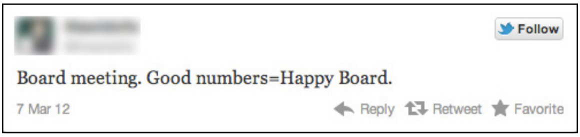
Compliance and Internal Risks

Compliance regulations, especially those governing information exchange and public disclosures, still apply within the purview of social media. The Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), Federal Financial Institutions Examination Council (FFIEC), Revised Payment Service Directive (PSD2), and Payment Card Industry (PCI) regulations, among others, must be enforced with regard to disclosure of sensitive information. Unfortunately, many companies do not have an internal policy in place to help guide both employee and executive social media usage.

Building, publishing, and training employees on internal policies is a powerful, cost-effective way to dramatically reduce internal risks across the board.

Risk and compliance teams need to work with marketing, security, human resources, and customer support departments to develop guidelines for safe, appropriate, and professional social media use. Again, the goal is not to dissuade employees and executives from engaging on social media, but rather empower them to be effective and responsible.

The nature of these policies varies based on the risks associated with the business. A healthcare organization, for example, might put the highest priority on protecting patient confidentiality, while a food conglomerate might want to identify posts about a particular physical location. Regardless of the nature of the risk, all organizations can benefit from a well-documented policy. Figure 4-2 is an example of what a CFO should *not* broadcast via social media.



Board meeting. Good numbers=Happy Board.

7 Mar 12

FIGURE 4-2: This example tweet from the CFO of a publicly traded company resulted in the executive's firing.

An internal policy first assesses the potential severity and frequency of risks. For example, a full-fledged FFIEC violation is likely to be costly but is relatively uncommon. Conversely customer scams, although low-cost in isolation, occur in high frequencies and at scale. Assigning some comparative qualifications for risk based on your organization's tolerance allows for prioritization of risk.

TIP

Organizations should also consider establishing different policies for different types of stakeholders. A CFO may need to take more precautions than a summer intern would, and employees with access to sensitive data or systems may have different guidelines concerning what sensitive information they can share (for example, the types of systems used in the data center or financial software used in accounting).

A corporate social media policy might address issues such as:

- Sensitive company data disclosure policy
- How to engage with competitors
- How to engage with brand accounts
- Social selling
- Geotagging
- Offensive images and language
- Publicly criticizing the employer
- Sending sensitive corporate information between employees
- How to report abuse

At a minimum, the policy should outline goals for employee social media usage and specifics of how to achieve those goals. Different industries will have different tolerances for how actively these policies can be enforced.

Risk, compliance, and fraud teams should subsequently monitor for violations of internal policies— especially regulatory compliance.

TIP

Acting quickly on compliance risks can mean the difference between an errant post and full compliance violation.

Creating systems for executives, such as posting review cycles or outsourcing posting privileges to a security-savvy assistant, can also reduce issues. Automated, real-time visibility is critical for quickly responding to risky posts. For details on building a social media protection program, see Chapter 6.

CHECKLIST FOR FRAUD, RISK, AND COMPLIANCE TEAMS

Here are some actionable items for fraud, risk, and compliance teams looking to protect their social media presence:

- **Create and circulate policies specifying what can and can't be posted by employees or executives, relative to both regulatory compliance and internal policies.**
- **On the careers page of your company website, state your procedures for contacting candidates and declare a policy regarding paid applications.** Applicants need a single source of reference explaining how they should expect to interact with a prospective employer.
- **Inform the public about your information-gathering practices**. Publish a statement affirming that your organization will never ask for a user's account login or other personal information via social media. Educating potential victims is the number one way to stop scams.
- **Use victim-reported fraud to be more proactive.** This is most easily achieved when you have an authoritative presence on each social media platform. It also ensures that remediation happens quickly.
- **Provide employee training on what to look for and how to report.** Employees, who are often the most engaged advocates of your brand, are a great source of intelligence about risks if you train them effectively.
- **Proactively monitor social media and digital channels.** Identify fraud and compliance violations in real-time to reduce the risk of prolonged exposure. A social media protection tool can automate the identification of fraud and help report it to the social networks for removal. Although social networks are responsible for removing fraudulent content, the organization being exploited is responsible for identifying and reporting it.
- **Consider letting a security-trained assistant run executive social media accounts**. To ensure policy adherence at the highest level, some executives are happy to delegate their social media strategy to someone else in the organization.

IN THIS CHAPTER

- **Hardening your corporate social media accounts**
- **Utilizing social media to collect security intelligence**
- **Identifying different types of attacks**
- **Integrating social media into your security posture**

Chapter 5 Protecting Your Organization Against Security Threats

Information security teams are charged with securing their company's networks, data, and devices. These disparate components may be used or accessed by hundreds or thousands of employees, each presenting its own security risks. To make matters worse, employees' social media accounts introduce a massive additional layer of complexity and unique challenges. An average employee's social media account is unmanaged, unsecured, and accessible to *billions* of people. Most security teams have no direct access or visibility into this data and cannot effectively secure their assets, identify threats, and protect their people.

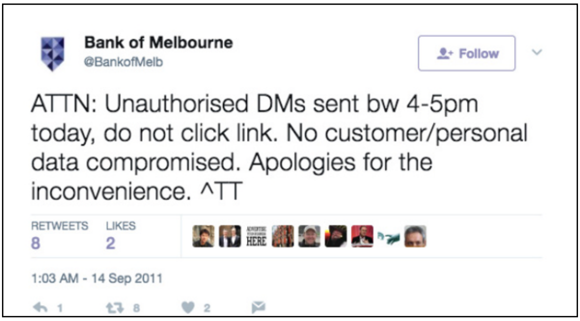
As organizations add new business technology platforms, standard practice dictates that information security teams secure them. Social media should be no different in this regard. However, as with other newer technology, securing social media accounts and a business' footprint have often been an afterthought given the minimal runway decision-makers have to consider the full impact of leaving a new technology unsecured. This is a mistake.

In this chapter, we discuss the methods hackers use to target corporations on social media. We also provide a checklist of steps to secure your corporate social media accounts.

Securing Corporate Social Media Accounts

Social media accounts are highly visible platforms for an organization to grow its brand, disseminate information to prospects, and engage with customers. In recent years, social media account hijacking has become a favorite tactic of cyber-vandals and "hacktivists." Marketing and support teams own and operate the company's accounts and often do not employ the most robust security procedures available. Attackers consequently find them to be easy targets.

Unlike with other IT assets, security teams can't pull the proverbial plug on a breached social media account. If the attacker's intention is to lie low and gather data from direct messages (DMs), as shown in Figure 5-1, or subtly engage customers with phishing links, the breach can go unnoticed for months, or even years!



Bank of Melbourne
@BankofMelb

ATTN: Unauthorised DMs sent bw 4-5pm today, do not click link. No customer/personal data compromised. Apologies for the inconvenience. ^TT

RETWEETS 8 LIKES 2

1:03 AM - 14 Sep 2011

FIGURE 5-1: An example of a breached profile that distributed malware through direct messages to the account's followers. This was the work of a cybercriminal group.

For a detailed look at securing social media profiles, review Chapter 2. Marketing and customer support teams are commonly the active owners of a business' social media accounts. However, they do not typically safeguard corporate accounts or the accounts of employees who use them, just as they are not responsible for a corporate website's security posture. Information security must work closely with them to set up security policies and procedures, educate the workforce, build policies, and regularly audit and review them. For instructions to create a full social media protection program, see Chapter 6.

Limiting Social Media as a Source of Hacker Reconnaissance

For a hacker, social media sites are excellent tools that can be used to help perform reconnaissance on a target organization. An attacker may learn which employees have access to critical systems or who has financial signing authority based on role descriptions, enabling them to craft a more precise attack.

Similarly, if a network engineer posts that she has Cisco firewall certifications, she can inadvertently give attackers the information needed to determine that there is a high probability their target organization uses that product.

REMEMBER

Personal information can also be readily weaponized by an attacker during a social engineering campaign. The more information an attacker can access about the victim's family, hobbies, home address, and personal connections, the better they can craft a unique spear phishing message.

Defending Against Social Media Cyber Attacks

Like email before it, social media is an incredibly powerful platform for a hacker to exploit targets and distribute a cyber attack. The nature of social networks makes a social media attack very different from traditional cyber attacks. The following are a few examples of why hackers are exploiting social media over email to launch attacks:

- Users log in more frequently and spend more time on social media than email.
- Social media is abused as a malicious delivery mechanism because it doesn't require the target to "open" it — as contrasted with an email attack in which the victim must open an attached file before the malicious software takes effect.

- Social media's public access is abused by attackers to cull massive lists of targets and recipients.
- Social media's use of hashtags makes searching for specific words and phrases easier, and attackers abuse this to target those people almost effortlessly.
- Social media has a reputation among users as being safe and secure — a more trusted way of communication than email.
- Social media typically exists outside traditional perimeter and endpoint security.
- Social media is abused by attackers to remain anonymous.

Social media's networking capabilities are exploited by hackers in broad "spray-and-pray" methods as well as targeted attack methods against organizations and their customers.

Spray-and-pray

In a *spray-and-pray* attack, the attacker tries to disperse an illicit campaign by casting the net as wide as possible before isolating particular victims. In this approach, the victim first interacts with the attack message before the attacker fully engages individual targets.

Watering hole

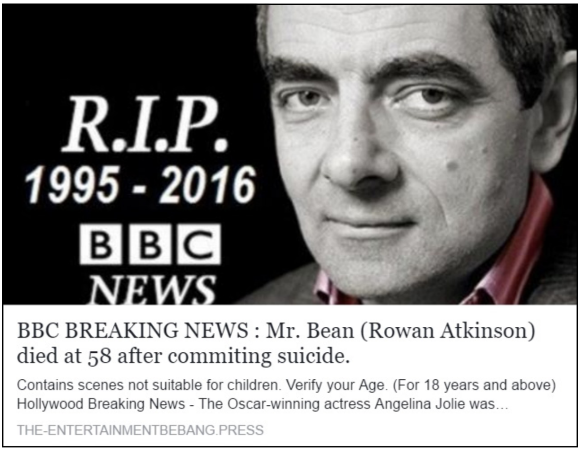
In a *watering hole* attack, a payload specific to an industry or other discrete group of victims is placed where a desirable victim is likely to organically find and engage with it. This type of attack can easily be dispersed to tens of thousands of users at a time — perhaps all employees of a single company — and quite often, attackers may not realize who their victim is within their targeted group until later in the attack's lifecycle.

Land-and-expand

In a *land-and-expand* attack, the attacker targets specific organizations or users, and subsequently seeks to expand to others within similar demographics and penetrable social circles. Using this model, the victim is targeted before interacting with any payload. Initially, the scope is narrow and "friendly." Attackers perform reconnaissance and select targets with the highest impact that fulfill end-goal requirements.

Knowing How to Proceed

Cyber attackers have demonstrated success using all three types of attacks — spray-and-pray, watering hole, and land-and-expand — and cyber attacks via social media continue to rise. Cisco reports that social media is now the most commonly used way to distribute malware, far eclipsing email. Clickbait, as shown in Figure 5-2, can be an innocent-looking method for malware.



BBC BREAKING NEWS : Mr. Bean (Rowan Atkinson) died at 58 after commiting suicide.

Contains scenes not suitable for children. Verify your Age. (For 18 years and above) Hollywood Breaking News - The Oscar-winning actress Angelina Jolie was...

THE-ENTERTAINMENTBEBANG.PRESS

FIGURE 5-2: An example of a malware-laced message shared as clickbait.

According to Norton, 40 percent of people have fallen victim to social media cybercrime. Barracuda's research also supports this trend, finding that 92 percent of social media users report receiving spam, 54 percent have received phishing links, and 23 percent have received malware. Furthermore, Cloudmark surveys reveal 40 percent of enterprises have fallen victim to social media spear phishing attacks, and Panda Security reports that 20 percent of businesses have been breached by malware from social media.

REMEMBER

Employees need to be aware of the multitude of ways hackers exploit social networking sites. Educating and testing the employee population is the first step in preventing social media cyber attacks. Concurrently, a security team should require a social media protection tool to automate the identification and remediation of threats.

Spoofed accounts and cyber attacks are in clear violation of social networks' Terms of Service, and the networks remove social engineering campaigns and malicious content when notified. Security teams must consistently monitor social media sites to rapidly identify inbound attacks targeting their personnel or customers, and implement a workflow for reporting threats to social media networks for removal.

TIP

Social media protection tools automate this process and allow security teams to block risks across the enterprise in real-time.

TECHNICAL STUFF

The attacks identified on social media sites are often unique, allowing security teams to identify new threats, correlate with existing security operation center (SOC) indicators, and strengthen existing security investments. The way this data is leveraged within an existing security framework varies greatly from company to company depending on existing tools, initiatives, and risk tolerance. Typically, a SIEM or robust visualization tool, like Splunk, is a good place to start.

Identifying leaked information on social media

The vast nature of social media represents, arguably, the greatest data source in the history of humanity, all organized and structured in a manner that is meant to be consumed. Security professionals should be aware of how data is leaked, intentionally or not, and how leaked data can be identified.

Employees leaking data can be an indicator of potential *identity access management* (IAM) modifications that the organization needs to make. If employee credentials or sensitive files are found on social media or the web, security teams can reset employee credentials or trace where potential data loss prevention (DLP) measures failed to prevent sensitive files such as medical records, intellectual property, or account information from leaving the network.

REMEMBER

Hackers often publicize or boast of their successes on social media. They also advertise stolen data they might be selling. Just as social media is a major driver of legal market activity, so too is it used by hackers to coordinate activities, communities, and markets.

Organizations can integrate sensitive information discovered on social media sites into DLP infrastructure to more quickly identify when a breach has occurred and efficiently begin remediation activities. Leaked or stolen data is traded in public purview more often than is realized. Attackers frequently choose to communicate in broad daylight rather than rely on the backchannels security professionals associate with illicit activity.

To address this, security teams must have continuous, real-time visibility into what is being posted about their organization on social media networks. A social media protection tool automates the process of identifying leaked data and programmatically passes that data to your perimeter security infrastructure.

Ingesting open-source intelligence

Hackers sometimes telegraph their intentions publicly before an attack occurs. Distributed denial of service (DDoS) attack planners have been known to use social media to coordinate the attack. Attackers, especially hacktivists, crowdsource attack participants by using hashtag campaigns and launch DDoS attacks on Twitter by posting IP addresses, domains, attack tools, the time of the attack, and the desired target.

TECHNICAL STUFF

Because attacks leverage social media for participation, security teams can prepare a protection strategy that entails coordinating with network teams, the incident response group, and internet service providers (ISPs).

Organizations and their representatives also put themselves at risk by the information they choose to share. Executives who discuss travel plans or a conference they are attending can open themselves up to greater risk. Even the posts of a family member can be weaponized to do harm. Publicly posted information on social networks is a gold mine for an attacker conducting reconnaissance.

Corporate security teams must spend time educating high-risk individuals on how to safely use social media. This involves an ongoing dialogue about how those individuals use social media, and what their risk tolerance is.

TIP

Corporate security teams should let high-risk individuals use social media as much as is safe given their role, vulnerability, and the local context, while providing automated protections to alert on risks.

INFORMATION SECURITY TEAM CHECKLIST

Here are some actionable items for information security teams looking to protect their businesses on social media:

- **Work with marketing, corporate security, and executive teams to have information security teams lead the development of a full social media protection program.** See Chapter 6 for a full dive into how to build a successful program.
- **Build policies for social media and what information should and should not be shared.** Social media is another domain to be monitored and protected. Having a corporate policy for the type of information that is shared on professional and nonprofessional social media sites (to the extent such restriction is required) is essential to stopping your employees from doing the cyber attackers' heavy lifting for them. The policy should be distributed as training material for key stakeholders.
- **Train employees on policies and how to use social media safely.** This includes what information to post publicly, what information to hide, and how attackers use personal information on social media to target an employee to breach the corporate network.
- **Work with marketing to identify key stakeholders and employees with privileged access to social media accounts.** It's important to limit this access as much as possible, especially for third parties such as consulting firms and digital marketing agencies.
- **Work with marketing and customer success to enforce access controls on corporate accounts and train corporate users.** Protect the usernames and passwords the same way you would for any critical infrastructure with two-factor authentication and identity access management (IAM). Social media security training should help new employees understand when to forward information to the security team. Perhaps more importantly, enforce strict policies around what happens when an employee leaves the company, especially if the employee has access to accounts.
- **Establish automated tools to identify inbound attacks and leaked data.** Social media protection tools allow security teams to gather data that's relevant to their organization and analyze it to detect a variety of cyber attacks, including spoofed accounts, sensitive data, phishing, and malware. Advanced algorithms are well-suited for

the task of analyzing vast numbers of posts to identify subtle differences, such as discrepancies between real and fake accounts, malicious and benign links, and scams and genuine promotions.

- **Work with the social networks to remediate cyber attacks and malicious accounts.** Anything in violation of a social network's Terms of Service, including cyber attacks and nefarious profiles, can be reported to the network for removal. A social media protection tool automates and facilitates this process.
- **Integrate social media data into the existing security infrastructure.** Social media is rich with relevant public metadata. Cross-referencing social media threats against an existing data stream provides valuable context and creates a value stream of new security data. Social media data can be useful for security information and event management (SIEM) system, an intrusion detection system (IDS), domain name system (DNS), log management system, identity access management (IAM) system, and more. How this data is used and contextualized can be highly customized based on the nature of the security infrastructure in place.

An organization's corporate assets can also be exposed to greater risk through social media. Criminals may threaten a particular store location or post dangerous content about events. Ingesting and analyzing this data in real-time are integral to robust situational awareness. Every second is crucial when an organization deals with advanced security threats, and social media represents the most current and accurate situational data anywhere online.

CORPORATE SECURITY CHECKLIST

Here are some actions corporate security teams can take to protect the company:

- **Work with marketing, information security, and executive teams to incorporate situational awareness into a social media protection program.** See Chapter 6 for a full dive on this process.
- **Audit company and executive social media usage.** Determine where and how executives put themselves at risk, as well as what social media engagement is productive, and thus worth encouraging. Corporate security teams should seek to empower executives

(continued)

(continued)

to use social media safely and effectively rather than block them entirely. For brand accounts, include individual store or franchise accounts while investigating what potentially risky data is exposed and how those accounts respond to inbound comments and posts. Identify who has access to which accounts.

- **Establish policies for different assets and different scenarios.** As executives or their families travel, attend conferences, and receive press coverage, the level and type of risks change. Corporate security teams need to be more vigilant when a CEO is delivering a keynote at a conference halfway around the world than when she is in her office. Establishing these policies helps streamline a corporate security team's responsibilities based on the situation.
- **Based on the nature of how social media is used by protected assets, monitor social media and owned accounts for risks.** Security teams can protect their critical assets by monitoring social media for threats or leaked sensitive data around a protected individual. Security teams can also monitor protected entities' accounts to identify compromising posts such as travel plans or outright compliance violations. This also involves establishing a rapid-response line of communication with the individual or whoever manages their accounts. All of these tasks can be achieved at scale by using a social media protection tool.
- **For physical assets, assume a more holistic approach to corporate security.** Monitor social media data for threats by ingesting relevant public social media data, a real-time repository to quickly identify threats, risks, natural disasters, or other issues as they arise.
- **Integrate social media data into the existing situational awareness infrastructure.** Social media data streamed in real-time can provide critical data for identifying and contextualizing risk.

IN THIS CHAPTER

- » Creating a social media protection program
- » Convening a social media protection task force
- » Assessing social media risks
- » Training employees on social media safety

Chapter 6
Ten Tips for Building a Social Media Protection Program

Because social media is relatively new, the department responsible for addressing security-, fraud-, and compliance-related issues is rarely determined. Though marketing, recruiting, sales, and customer success departments are the primary day-to-day users of social media, the legal, technical, and procedural expertise required to manage a targeted phishing attack or widespread financial crime demands that security and risk professionals take an active role.

In this chapter, we list ten helpful tips for building a social media protection program.

Assemble a Task Force

Marketing and information security teams generally lead the first task force meeting. They should educate stakeholders about the purpose of a social media protection program and explore its corresponding goals and responsibilities. Aim to deliver documented processes and policies.

Assess and Prioritize Risks

The frequency and severity of the risks you face varies depending on industry, size, and current social media presence. For a full risk profile of the company, work with a social media protection vendor to create an initial assessment.

Most social media protection task forces assess risk based on *frequency, likelihood, cost,* and *severity*. Account hijacking, for example, occurs at a low frequency but has an incredibly high severity and cost. Assigning some comparative qualifications for risk based on your organization's tolerance allows for prioritization of risk.

Assign Roles and Responsibilities

The objective during the initial meeting is to agree on roles and responsibilities. This entails identifying what risks exist for the brand and which are the most urgent.

It should be evident which stakeholder is tasked with identification and remediation. For example, the customer success team may be responsible for identifying customers leaking personally identifiable information (PII) or credit card information, but it may be up to fraud and legal to remediate.

Establish Processes and Policies

Documented processes and policies are a social media protection task force's core initial deliverables. Processes describe workflows for each risk, stakeholder engagement, remediation, and takedown, and review. Policies provide guidelines for key stakeholders and for active social media users to include executive social media usage frameworks, training programs, and regulatory guidelines.

Train Relevant Staff

Training staff on policies defined by the task force is a foundational component of a strong social media protection program. When you train employees on internal policies, include general education topics on social media protection, security, and privacy.

This is critical for marketing and support staff who actively engage with prospects or customers. Ensuring that your support staff engages appropriately can make the difference between return customers and a social media catastrophe. Establish a process, update it regularly, and develop an enforcement mechanism.

Monitor and Address Risk

The most involved stakeholders — generally information security, risk and fraud, marketing, and customer success — should use social media management, social listening, and social media protection tools to identify and manage threats.

The speed and efficiency of monitoring and damage control are critical because risks can spin out of control in minutes. Social media protection tools must be set up in alignment with the priorities laid out in the initial meeting and deployed to the correct stakeholders. Content in violation of a social network's Terms of Service can be automatically flagged for removal through a social media protection tool.

Monitor Trends

Monitor trends and update policies and processes as needed. Assign someone to stay abreast of social media topics, including emerging threats, changes in policies and regulations, and evolving attacker tactics. Deploy a tool that updates users with training and news.

Schedule Recurring Check-ins

Schedule regular check-ins for the task force to review trends, discuss wins and losses, and update goals based on feedback.

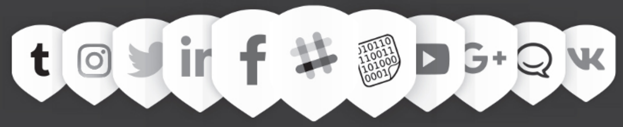
Report and Review

Establish a framework for metrics and reporting to be consistently circulated to stakeholders. Work with your social media management, social listening, and social media protection vendors to create analytics and reporting. These metrics, which guide the review process, should show forward and backward progress, as well as gaps in the program.

Complete the Ultimate Social Media Protection Checklist

The final tip is to complete our all-star social media protection checklist. Check off these items, and you'll be well along on the road to implementing a robust social media security program:

- Set up your organization's social media pages (even if you don't plan to be active), and keep them updated.
- Enable two-factor authentication for all your business social media accounts. Have the two-factor authentication linked to a corporate device that is locked down.
- Ensure that the corporate email accounts connected to your social media accounts follow the same user access guidelines of any other critical system.
- Leverage a social media management platform or leverage the native apps and limit personnel access.
- Change passwords to corporate social media accounts at least three times per year.
- Audit social media access and permissions quarterly.
- Create a corporate social media policy that aligns with your business needs and goals, including rules of engagement for employees on their personal accounts.
- Enable a technology with functionality to automatically lock down your accounts if they exhibit strange behavior.
- Train your social media business user personnel on social media security and privacy, at a minimum, annually.
- Do not share, retweet, or tag profiles you don't recognize.
- Programmatically monitor social networks for threats to your business.



Protect what matters most on social media

In this book, you'll learn about potential risks posed by social media to individuals and businesses alike. Every day, hackers use social media in harmful ways — ways that affect you! That's why having strategies to protect yourself and your organization before something bad happens is more important than ever. After reading our in-depth walkthroughs, you'll understand how anyone, from a casual user or a small business owner to an information security professional at a Fortune 100 organization, can build an effective social media protection program.

Inside…

- Explore social media's global growth
- Secure your individual, brand, and corporate social media accounts from attacks
- Protect customers from scams and fraud
- Defend your business from security risks
- Build a social media protection program
- Manage risk, fraud, and compliance

ZEROFOX®

for dummies®
A Wiley Brand

ISBN: 978-1-119-45961-3
Not for resale