FORTRA

PLAYBOOK (PhishLabs)

Navigating Social Media Threats

A Digital Risk Protection Playbook

www.phishlabs.com

In 2021, the average business experienced a two-fold increase in social media attacks. Social media has dramatically changed how individuals and enterprises communicate, and as a result, it is rapidly becoming the landscape of choice for threat actors. Roughly a decade ago, this evolving landscape was dominated by platform giants Facebook and Twitter. Today, they are among the thousands of different social sites used to engage online. More than 4.62 billion people[1] use social media, and security teams need to be aware of the risks these channels pose to their organizations.

In this playbook, we discuss the social media threat landscape size and types, industries that are impacted by these threats, how to turn social media data into intelligence, and mitigation solutions. To successfully protect against threats on social media, security teams should apply the following best practices:

1. Understand the different threat types and identify which apply to your organization
2. Create defined criteria to curate intelligence
3. Develop relationships that will lead to effective mitigation

Threat Landscape

Social media is becoming a top online channel for threat actors. Two driving forces behind increased abuse are the ease of account creation and the trust users put in social media. In the last 12 months, 424 million new users subscribed to a social platform. Of those, countless were reported as fake. That means when a user interacts with a post, clicks on a link, or fills out a form, odds are they are unknowingly interacting with a bot.

Social media giants have tried to remove bots and suspicious activity from their platforms. Twitter, for example, purged 70 million accounts in 2018. In Q3 of last year, Facebook removed 1.8 billion. Despite this and similar efforts, scams on social media caused $770 million in estimated losses in 2021 alone.[2]

In order to proactively protect against and remove threats on social media, security teams must be able to identify the attacks on platforms relevant to their organization and understand each specific threat type.

[1] Hootsuite
[2] Federal Trade Commission

Types Of Social Media Abuse

There are a variety of methods cybercriminals use to target organizations on social media. Some of the most prevalent threats are highlighted below.

Financial Scams

Financial scams occur when threat actors request monetary compensation from their victim. These are the most frequently observed threat types on social media in conjunction with impersonation. There are various types of financial scams, and they affect more than one industry.

Types of Financial Scams include:

Deposit Fraud

Victims are manipulated to deposit fake checks into their accounts and send the threat actor a portion of the money. A victim can become complicit in this type of scam by sending a check to the threat actor for deposit, then reporting it stolen. After the threat actor removes and distributes the cash from the account, the bank refunds the falsely stolen cash to the account holder.

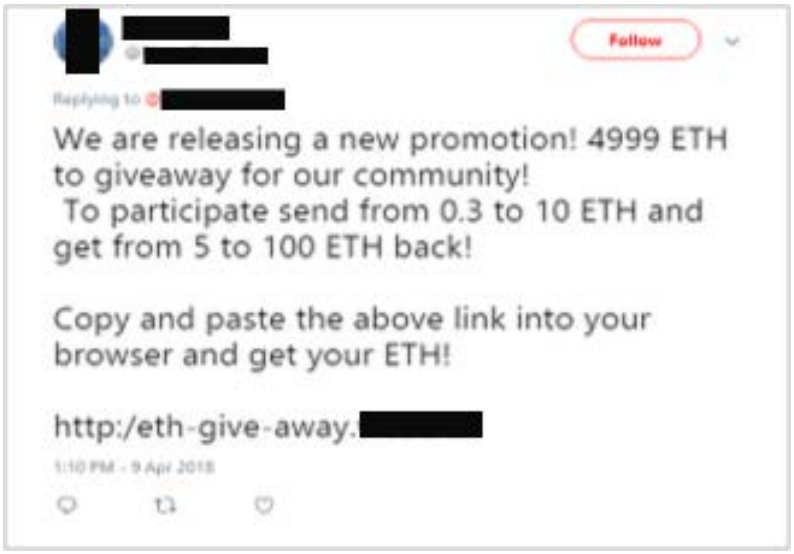
Counterfeit Ad Campaigns

Paid ads using stolen trademarks, images, and logos impersonate legitimate brands and lure victims to counterfeit stores on the open web. These ads are associated with fake business pages on social media, appear authentic, and feature heavily discounted products. If a victim clicks on an ad, they are directed to a fake website selling unauthorized goods.

Money Flipping

The threat actor promises a substantial payment to the victim in return for small amounts of cash. Once the victim transfers payment, the scammer ceases communication and disappears along with the money. Below is a money flipping example that impersonates a cryptocurrency trading platform.

Image 1: Money Flipping Scam



Card Cracking

Similar to deposit fraud, a victim reports a credit card stolen and gives the threat actor their bank account or card information. The threat actor then withdraws funds and divides the cash.

Tech Support

Threat actors request monetary compensation or access to the victim's computer to fix a supposed issue. Contact is made under the pretense of solving a particular problem and impersonation is used to add legitimacy.

Image 2: Tech Support Scam

Fake Employment Opportunities

Threat actors impersonate fake companies regarding potential employment. During the bogus interview process, they request money for processing fees or personally identifiable information (PII) that can be used to financially harm the victim by other means.

Cyber Threats

Cyber threats on social media platforms consist of phishing and malware attacks. Phishing examples can range from links or pages containing phishing information, to something as simple as general tips to running a campaign.

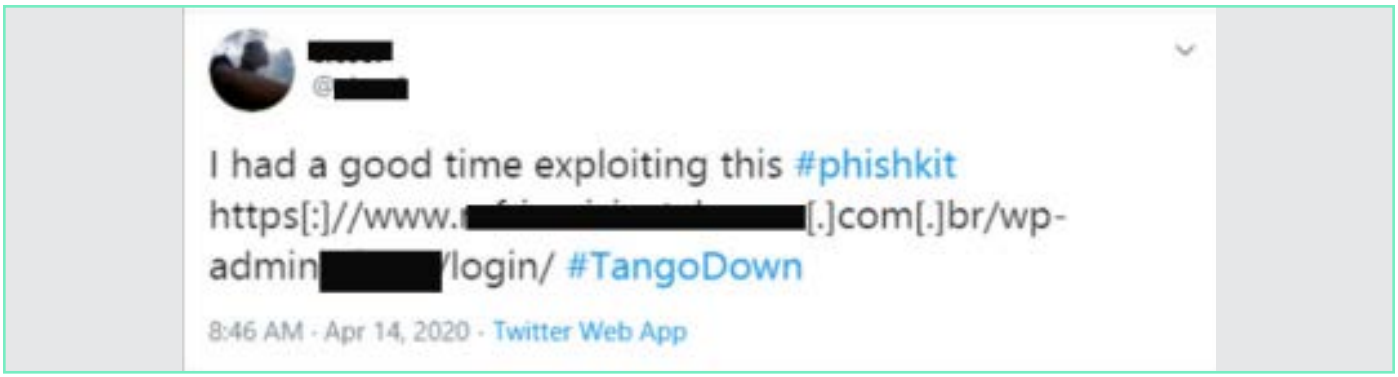


Image 3: Phishing Information

Malware can manifest as links in comments, posts, or direct messages. If installed, threat actors can gain access to the victim's computer and hold it, as well as account information, hostage.

Image 4: Malware

Data Leaks

There are four different types of sensitive data that are leaked on social media:

- Customer and employee PII
- Credentials such as usernames and passwords
- Sensitive documents including contracts and company projects
- Source code, which gives the threat actor access to internal software

Image 5: Leaked Source Code

In the majority of cases, leaked PII and credentials are financially motivated.

Reputation Risks

An organization's reputation can be damaged if they are the victim of any social media threat type listed above. In addition, threat actors can post defamatory comments or make unauthorized associations with a company to draw unwanted, negative attention.

Protests, petitions, and boycotts also cause reputational damage, and risk physical harm to employees or customers. In order to successfully monitor for reputation risks, it is important to track any upcoming concerns or mentions related to your organization.

Brand, Employee, And VIP Impersonation

Threat actors use impersonation to maximize effectiveness of scams across social networks. Impersonating high-ranking executives, employees, and recognizable brands aids in malicious efforts by adding familiarity and credibility. Common scams that use impersonation include fake giveaways and contests.

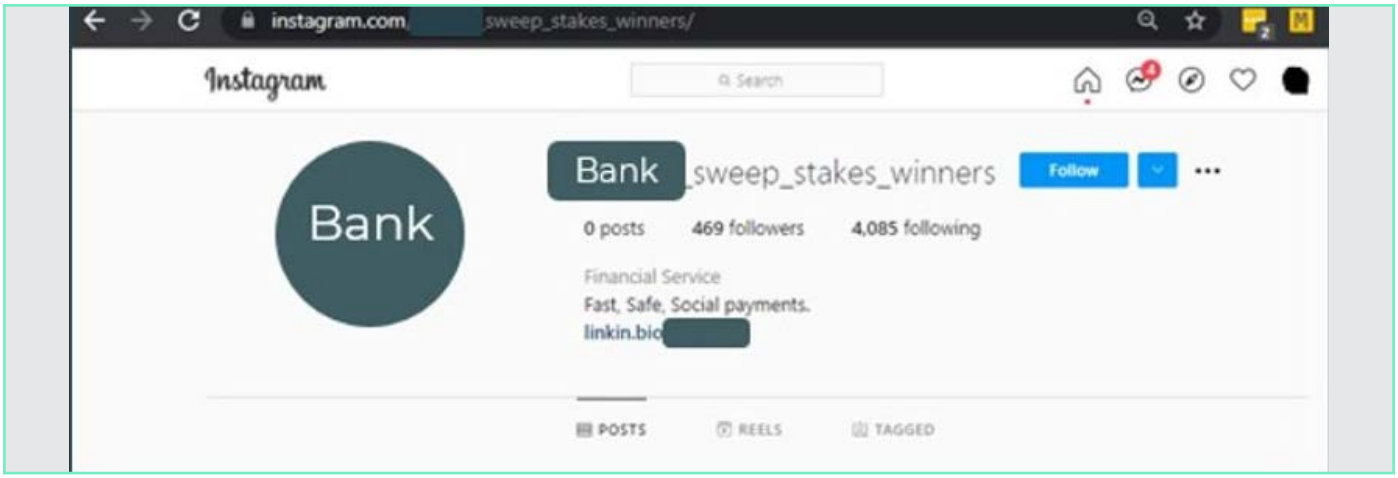


Image 6: Brand Impersonation

Industries Most Affected And How

No organization is immune to social media threats, although some face a higher risk of attack than others. The following are industries commonly targeted by threat actors.

Financial Institutions

Among the most common threat types for financial institutions are leaked PII, documents, credentials, and source code. A source code leak has the potential to lead to a data breach and publicize proprietary information. The reputational damage associated with these threat types can be severe and result in loss of brand trust as well as wavering investor confidence.

Phishing attacks and brand impersonation are also commonly seen as threats to financial institutions. A successful phishing campaign can ruin a customer's finances and, depending on the organization's response to the attack, negatively impact future business, customer trust and overall public reputation.

Media and Entertainment

Threat types to media organizations are more specific to the industry and include tech support scams, employment scams, and leaked PII. Victims of tech support or employment scams may have their credentials stolen, credit card numbers leaked, or their social security numbers compromised, all of which can lead to financial loss. Organizations have the potential to suffer massive indirect costs as a result of these scams due to customer distrust.

Healthcare

One of the threat types considered high risk for healthcare is tech support. These scams are particularly prevalent because they are easily created, modified, and mimicked. Tech support scams can result in stolen PII and credentials from patients and clients.

Leaked documents can also have a devastating impact on healthcare providers due to the sensitive nature of information they interact with. Threat actors can leak documents to scam, blackmail, or even harm a customer.

Leaked documents can create risk to corporate executives and offices as well, if protests ensue.

Retail

Retail organizations are facing an increased volume of attacks as social commerce fueled by the pandemic drives online purchasing activity. Impersonation and Counterfeit Ad Campaigns are the primary threat types targeting retail, with brands, employees, and VIPs at risk. These attacks are easy to set up using stolen intellectual property and are low cost to the threat actor. Impact can range from revenue loss through the decline of repeat and future sales, as well as significant brand damage.

Turning Social Media Into Intelligence

Security teams must have processes in place that ensure the delivery of accurate, highfidelity intelligence to streamline response times and reduce the lifespan of threat workloads. In order to thoroughly gather the data to do this, they must look for threats spanning all social media platforms that apply to their organization. To accelerate the gathering and accurate curation of intelligence, enterprises should leverage a combination of machine processing and human analysis.

There are four components to turning social media data into actionable intelligence:

- Classify the threat
- Determine its severity
- Eliminate false positives
- Add context

Because of the scope of data across social media, potential threats need to be classified by using relevant algorithms to find targeted references and filter false positives. An example of this is fuzzy matching or, a variation of defined criteria such as relevant keywords or brand activity.

Expert analysts must also apply business context to the threats to assess the risk they pose. Without this context, legitimate threats may be overlooked and benign activity may be misinterpreted as malicious.

In order to ensure alignment and accelerate mitigation, analysts need to not only be trained in the particulars of the organization and their audience, but also dialed into their priorities and specific needs, in addition to social media. Understanding the threat as it relates to a specific brand will ensure analysts can accurately determine relevancy and prioritize severity.

Finally, the resulting intelligence must be enriched with context and tuned in response to any changing business needs before being actioned.

Taking Down Social Media Threats

It is necessary for security teams to have multiple avenues for takedown in order to utilize the correct one for the issue at hand. There are various mitigation processes and takedown can be intricate and complicated. In order to takedown effectively, security teams need to establish direct relationships with social platforms that they can utilize in high-risk situations.

Networks and Criteria

Financial scams are most prevalent on giants like Twitter, Facebook, and Instagram. All three social media sites have individual reporting features found within the platforms and profiles. Both Twitter and Facebook allow security teams to submit direct reports on malicious activity.

Mitigation Criteria:

- Direct mentions of client in question with intent to commit financial fraud
- Posted login details
- Break in terms of service

Cyber threats are found on all major networks including YouTube and Paste Sites. Similar to financial scams, effective takedown avenues include direct reports to Facebook and Twitter as well as individual reporting and utilizing key relationships within the platforms. Platforms aren't simply looking at what content is on the post, and any information relating directly or indirectly to the cyber threat reported needs to be submitted as evidence in order to successfully mitigate.

Mitigation Criteria:

- Active links to malicious content that are abusive in nature
- Proof of past posted malicious content

Executive and Corporate Impersonation are utilized in many of the threat types seen on social media. These scams are found on all major platforms, with Instagram and LinkedIn being the primary abusers due to having the greatest reach to the targeted audience. There are many intricacies in filling out and submitting forms for impersonation, and reporting these types of threats includes direct contact with the platforms.

Mitigation Criteria:

- Proof that the profile is not a parody account
- Proof that the name and photo of the person impersonated is present on the post
- Legitimate profile of the victim is optimal

Conclusion

The vast number of social media channels and increasing user interaction gives threat actors a means of deploying threats rapidly on a global scale. More than half of the world's population is using some form of social media, and the malicious content they interact with on these platforms can manifest in many forms. By utilizing this playbook, security teams will learn how to identify the social media threat types associated with their industry, how to use social media as a means of gathering this intelligence, and proper mitigation techniques.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.