8 TIPS EVERY FINSERV INSTITUTION SHOULD KNOW TO MITIGATE SOCIAL MEDIA RISK

ZEROFOX®

THREATQUOTIENT™

More than three billion people around the world use social media each month, with 90 percent of those users accessing their chosen platforms via mobile devices.[1] While, historically, financial services (FinServ) institutions discouraged the use of social media, it has become a channel that can no longer be ignored.

FinServ organizations and their customers are migrating to social networks, collaboration tools and mobile networks to engage and support customers, recruit new employees and drive business development. Today, three out of four banking customers surveyed agree or strongly agree that social media is important to their banks, with Facebook, LinkedIn, Twitter, YouTube and Instagram being the most popular platforms.[2] However, few FinServ security teams incorporate these numerous threat vectors and data sources into their threat model. Taking advantage of the limited visibility and control these institutions possess to detect and remediate these risks, cybercriminals happily exploit these social and digital channels where vulnerable businesses and customers engage.

In this paper, we'll explore the most prevalent types of threats and scams targeting FinServ over social media and digital channels and provide a checklist to help security teams mitigate risk to their institution, brands, employees and customers.

ELIMINATING THE SOCIAL MEDIA BLIND SPOT

FinServ institutions are widely recognized as leaders in cybersecurity, employing layers of defense and highly skilled security experts to protect their organizations. But as the attack surface expands with the growing use of social media and external digital platforms, many FinServ security teams are blind to a new wave of digital threats outside the firewall.

To gain visibility, reduce risk and automate protection, leaders in the financial industry are expanding their threat models to include these threat vectors. They are embracing a data-driven approach that uses automation and machine learning to keep pace with these persistent and continuously evolving threats, automatically finding fraudulent accounts, spearphishing attacks, customer scams, exposed personally identifiable information (PII), account takeovers and more. They are aggregating this data into a central repository so that their threat intelligence teams can trace attacks back to malicious profiles, posts, comments or pages, as well as pivot between these different social media objects for context. Network security teams can block their users from accessing malicious social objects to help prevent attacks, and incident response teams can compare their organization's telemetry of incidents with known indicators of compromise to mitigate damage. Employee education is also a critical component of standard defenses. Raising awareness of these threats through regular training and instituting policies to improve social media security hygiene with respect to company and personal accounts goes a long way to preventing these attacks in the first place.

Analysis of prevalent social media risks shows the breadth and depth of these types of attacks. A deeper understanding of how bad actors are using social media and digital platforms for malicious purposes is extremely valuable as FinServ institutions strive to strengthen their defense-in-depth architectures and mitigate risk to their institutions, brands, employees and customers.

HOW THE LATEST SOCIAL MEDIA THREATS DAMAGE FINANCIAL SERVICES INSTITUTIONS

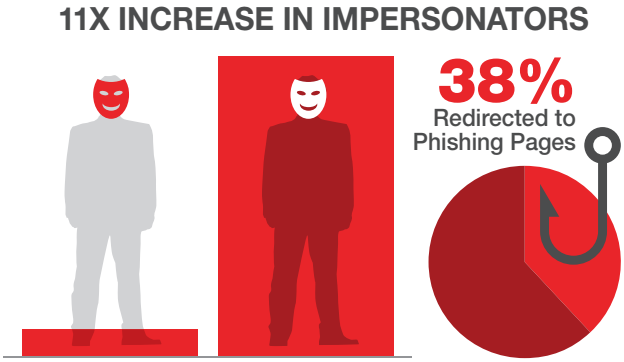
ZeroFOX's team of data scientists analyzes millions of social media posts every day using diverse data sources and a combination of automation, machine learning and expert analysis. Their research reveals that cybercriminals are using a variety of social media platforms to conduct customer attacks and scams, spoof accounts to impersonate brands and executives, spearphish employees, defraud customers, compromise and sell credentials online, leak sensitive corporate data and even orchestrate physical threats against executives and business locations. Following are the most prevalent social media threats to FinServ organizations.

Money-Flipping Scams
In these types of attacks, the scammer leverages a financial institution's brand and entices the victim to make a small up-front investment ($100-$500) with the promise of big financial gains and then walks away with the money. The attack begins over Instagram with a post that includes logos and hashtags with the bank's brand. Bad actors often follow the bank's followers to engage likely targets. Once they attract the victim, they typically migrate them off the platform, luring them to another site and out of public view or contact them directly via text message to reduce the risk of getting caught. Sharing photos of cash, drugs and luxury goods they could buy with their "investment," they use language that emphasizes urgency to act now or the offer will disappear.

Bad actors are using automation to create these accounts at an alarming rate.

Last year ZeroFOX analyzed over 2 million Instagram posts and found 4,500 unique scams authored by 1,400 unique scammer accounts. They found three times as many accounts being created versus being taken down, indicating the problem is growing in scale and that bad actors are using automation to create these accounts at an alarming rate. Eighty percent of these accounts were active for 45 days or longer, showing persistence and the ability to lure many victims. Since the study was first performed last year, the number of observed scams has soared to 340,000. These money-flipping scams cost FinServ institutions millions of dollars not just to reimburse their customers, but to keep them and overcome the damage to the brand and attract new business.

Spoofed Accounts and Impersonators
Instead of a specific post, a fake social media account impersonating a FinServ institution is often the unit of currency for these types of attacks. The cybercriminal looks at a FinServ institution's official company account, for example, on Facebook, Twitter or LinkedIn, analyzes images and descriptions that are used, and then copies the information with slight variations to create a new account. They gain followers' trust and then dupe them into sharing information that allows them to access their bank accounts and/or credit cards.

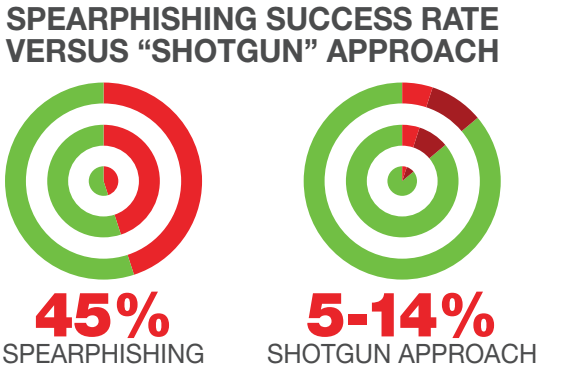


In a study conducted over a two-year period, ZeroFox found an 11x increase in impersonators.

In a study conducted over a two-year period, ZeroFox found an 11x increase in impersonators. A shorter, two-week study found that 38 percent of attacks redirected targets to phishing pages, often a copy of the FinServ institution's official website that would capture the target's login information when input. Some of these fraudsters even successfully leveraged paid social promotion to reach more people.

Social Spearphishing
In contrast to random phishing attacks, social spearphishing is highly targeted. For example, ZeroFox discovered a cybercriminal who had observed a customer of a bank asking for help with their account over Instagram and subsequently targeted them with a spoofed post offering assistance. Believing they were still interacting with their bank the customer shared their credentials which the criminal used to drain their accounts.

While the level of effort involved with spearphishing is very high, the success rate is as well. Spearphishing attacks achieve a 45 percent accuracy rate versus the



While the level of effort involved with spearphishing is very high, the success rate is as well.

"shotgun" approach of a typical phishing campaign that requires minimal effort but has an accuracy rate of only 5 to 14 percent. Other drivers of social media spearphishing, in addition to a high accuracy rate, include an abundance of personal data being exposed, a prevalence of shortened links that provide another layer of obfuscation for attackers, the undeserved culture of trust that permeates social media, and the use of automation and bots to simplify and accelerate execution of these campaigns.

Social Media Data Leakage and The Insider Threat
Data leakage by insiders can be inadvertent or intentional. In the case of inadvertent leaks, social media can entice users to expose sensitive information. Driven by the desire for retweets and more followers, individuals will expose PII like credit card and bank account data, as well as information such as travel plans and where they shop, bank and work. Individuals also use paste sites like Pastebin and unwittingly share information including corporate credentials, IP addresses and credit card data. Software developers may use GitHub to version control their code but, in the process, can share passwords and other valuable corporate data or systems details.

In the case of intentional leaks, malicious insiders with access to login credentials or other valuable data use social media to deliver that information to competitors or nation state actors. They can disguise the information using a variety of tools such as encryption or steganography, where they embed text within an image. Those few lines of text may be the data itself or they may be instructions that point the recipient to a website or forum to retrieve the information.

A CHECKLIST FOR FINANCIAL INSTITUTIONS

Social media is a morass of information flooding the Internet with billions of posts per day that comprise text, images, hashtags and different types of syntax. It is as broad as it is deep and requires an equally broad and deep combination of defenses to identify and mitigate the risk it presents. This checklist that encompasses people, process and technology will go a long way to helping FinServ security teams better protect their institutions, brands, employees and customers.

8 TIPS
EVERY FINSERV INSTITUTION SHOULD KNOW TO MITIGATE SOCIAL MEDIA RISK

1. **IDENTIFY** the institution's social media and digital footprint, including accounts for the company, brands, locations, executives and key individuals.
2. **OBTAIN** "Verified Accounts" for company and brand accounts on social media. This provides assurance to customers that they are interacting with legitimate accounts and prevents impersonators from usurping a "Verified Account."
3. **ENABLE** two-factor authentication for social media accounts to deter hijacking, and include corporate and brand social media accounts in IT password policy requirements.
4. **MONITOR** for spoofed and impersonator accounts and, when malicious, arrange for takedown.
5. **IDENTIFY** scams, fraud, money-flipping and more by monitoring for corporate and brand social media pages.
6. **MONITOR** for signs of corporate and executive social media account hijacking. Early warning indicators are important to protecting the organization's brand.
7. **DEPLOY** employee training and policies on social media security hygiene.
8. **INCORPORATE** a social media and digital threat feed into a threat intelligence platform as part of an overall defense-in-depth approach. This allows teams to ingest, correlate and take action faster on attacks made against their institution via social media.

CONCLUSION

FinServ institutions and their customers use many different social networks to communicate and conduct business but are often blind to the risk bad actors present as they increasingly targeting these public, uncontrolled channels to commit financial fraud, damage brands and even pose physical threats. FinServ security teams need visibility into digital threats outside the firewall and actionable information to reduce risk and automate protection. Those that are most successful have a defense-in-depth architecture that includes intelligence on social and digital threats, context to understand what threats pose the greatest risk, and the ability to build on existing processes and workflows to block more threats and accelerate remediation.

1 Global Digital Report 2018, We are Social. https://digitalreport.wearesocial.com/

2 The State of Social Media in Banking, Results of an American Bankers Association Research Study, 2017. https://www.aba.com/Products/Endorsed/Documents/ABASocialMedia_Report.pdf

ZEROFOX®

ABOUT ZEROFOX

ZeroFOX, the social media & digital security category leader, protects modern organizations from dynamic security, brand and physical risks across social, mobile, web and collaboration platforms. Using diverse data sources and artificial intelligence-based analysis, ZeroFOX protects modern organizations from targeted phishing attacks, credential compromise, data exfiltration, brand hijacking, executive and location threats and more. The patented ZeroFOX SaaS platform processes and protects millions of posts, messages and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Twitter, Instagram, Pastebin, YouTube, mobile app stores, the deep & dark web, domains and more.

To find out more information about ZeroFOX, please visit: https://www.zerofox.com.

THREATQUOTIENT™

ABOUT THREATQUOTIENT

ThreatQuotient™ understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ™, and cybersecurity situation room solution, ThreatQ Investigations, empower security teams with the context, customization and prioritization needed to make better decisions, accelerate detection and response, and advance team collaboration. Leading global companies use ThreatQuotient solutions as the cornerstone of their security operations and threat management systems. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC.

For more information, visit https://threatquotient.com.