ZEROFOX® | Whitepaper

InfoSec Guide: Impersonations and Brand Abuse in Financial Services

An analysis of tactics and steps for security teams to dismantle impersonation-based intrusions.

December 2020

zerofox.com

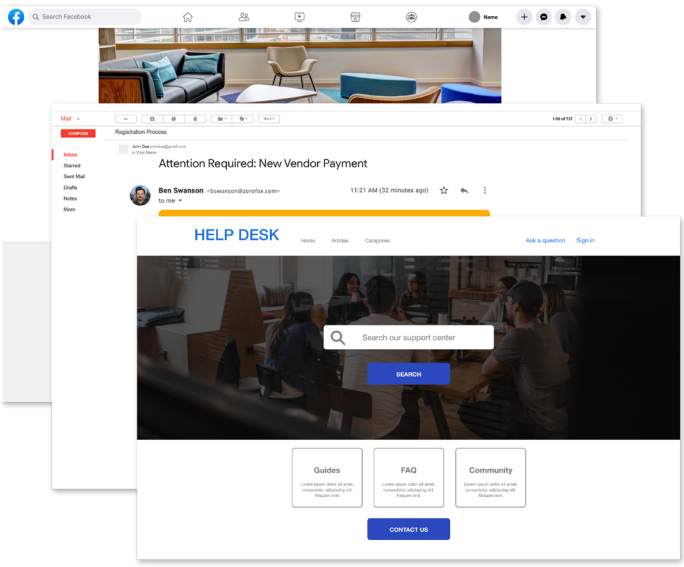
Introduction

As organizations, executives and everyday individuals shift to digital-first interactions, cyberhackers have found opportunity. By masking as a trusted brand or public figure, actors are able to gain access to eager customers and followers and exploit inherent trust. The frequency, location, and sophistication of these impersonations make it difficult for security teams to tackle alone. Brand abuse is more than a marketing problem — it's a security challenge that threatens the entire organization and all its stakeholders.

The ability to reach customers through websites, social accounts, mobile apps and online customer support portals is critical for organizations to survive in a digital-first world. The online presence maintained by organizations often serves as the first point of contact with consumers. For the financial services industry this includes everything from marketing promotions to mobile banking, loan applications, money transfers, account access and customer service. As financial business has shifted online, hackers have found new opportunities. By mimicking a financial institution's name, logo, website and even their people, hackers are able to trick consumers, employees and third parties into divulging information, providing network access, and sending funds through a variety of impersonation tactics. Impersonations can occur across a multitude of digital platforms, including fake profiles on social media, look-a-like domains, business email compromise and fraudulent mobile applications. This report details the persistent and emerging impersonation tactics hackers use to specifically target the financial services industry.

The Categories of Impersonation

Impersonations can take many forms, and hackers often leverage several platforms to conduct broad scale campaigns. In recent years, ZeroFOX has observed a trend towards more sophisticated campaigns that rely on a combination of look-a-like domains, fake accounts on social media, fraudulent mobile apps and fake customer support services. As impersonation tactics become increasingly complex, this has opened the door for specialization and created new opportunities for services such as phishing kits, which we'll discuss later in this report. While the impersonation ecosystem is robust, criminals often specialize; with some focused on creating impersonations of digital assets, others focused on impersonations of people and yet others on leveraging these accounts and capabilities to conduct the malicious activity. It is the combination of these tactics that has created the unique and persistent problem that now faces the financial services industry. With interwoven impersonations across the digital threat landscape, it can be difficult for security teams to know where to focus their efforts.



Impersonations of Digital Assets

The first category of impersonations are those that rely on an already established brand's online presence. This includes your website, any domains, mobile apps and even company-run social media accounts. These digital assets often serve as the face of your organization to the general public and are easy targets for copycats. Hackers also have equal access to your customers and prospects, making security particularly challenging. Within this category, we'll discuss three assets that are frequently targeted: domains, mobile apps, and corporate social media.

Impersonating Domains

An organization's website is often the first touch for customers, giving threat actors early opportunity. Malicious, spoofed domains offer hackers endless possibilities, including phishing, vishing, ad fraud and malware. Actors rely on look-a-like domains to phish employees, customers and related 3rd parties. For financial services in particular, malicious domains include fake bank login sites, loan forms and other spoofed sites that leverage the institution's logo and brand to trick users into divulging personal details. An actor can use a malicious domain to establish pre-attack infrastructure or to gain initial access to an organization. In every case, one thing remains constant: the actor is using your legitimate name to drive traffic to malicious activity.

Impersonating domains often involve one or more of the following techniques:

- Trademark infringement and plagiarism
- Code stealing from brand's legitimate website
- Page redirects to brand's legitimate website
- Typosquatting
- Subdomain spoofing
- Homoglyphs
- Link shorteners

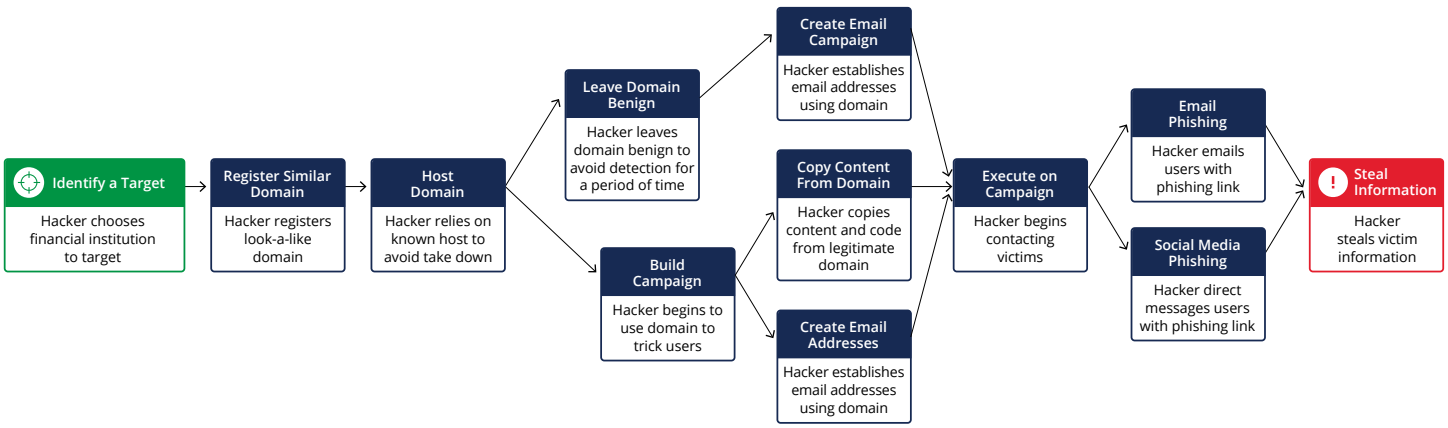
In all of these techniques, the actor relies on basic psychology to trick users, such as common misspellings, look-a-like characters and shortened text that the untrained eye may gloss over. The use of the brand's logo, trademarks and content exploits the inherent trust between brand and consumer.

How Impersonating Domains Are Used

Hackers leverage email, social media and other awareness tools to drive traffic back to the malicious site. Since there is no set time between when a domain is registered and weaponized, without continuous monitoring security teams will struggle to quickly identify and act on malicious domains. The quicker security teams can detect when a page goes from unarmed benign to weaponized and active, the higher likelihood of effectively addressing the problem. Particularly for large financial institutions with many domains and a broad web presence, manual searching and human response alone will not be enough.

Japanese phishing page impersonating Apple

Domain Impersonation Flow Chart



Actors rely on domains for web-based, email-based and multichannel campaigns. If the actor's goal is primarily email phishing, they may choose to leave the domain as a parked page to reduce the likelihood of detection and appearance of weaponization.

The Targets of Impersonating Domains

While both brands and executives can be the targets of impersonation, when it comes to domain impersonations, the target is usually at the institution level. Financial services are prime targets for domain-based impersonations because of the nature of the web-based services they provide. Online banking in particular offers hackers the opportunity to steal credentials and funds from banking customers. Loan applications and other standard forms used by financial institutions offer similar opportunities to steal PII. Regardless of the size of the financial institution, the services offered are typically the same, providing hackers a variety of targets. Protecting consumers against domain-based impersonations should be a top priority for security teams of every financial institution, big and small.

The two most important factors to consider when addressing impersonating domains are unpredictability and scale.

What to Do About Impersonating Domains

The two most important factors to consider when addressing impersonating domains are unpredictability and scale. As aforementioned, actors rely on both unarmed benign domains as well as actively weaponized domains to conduct impersonations. It is impossible to know if, or when, a hacker may switch a domain from benign to weaponized, and once they do, it may be too late to take action before the site can reach your customers. In order to address the unpredictable nature of these intrusions and gain early awareness to the threat, it's critical that security teams continuously monitor domain registrations for potential look-a-like domains and any other malicious activity. Identifying this activity at the initial registration phase thwarts hackers from even making the decision of whether or not to weaponize. Proactively registering domains with common misspellings, variations and homoglyphs prevents hackers from targeting your brand in the first place.

The vast extent of domain-based impersonations make them difficult to tackle manually. **In ZeroFOX's InfoSec Guide: Addressing the Rise in Phishing and Financial Fraud** published in May 2020, ZeroFOX observed almost twice the number of malicious domains compared to 2019 figures. Without automation, it can be difficult to find domains impersonating your brand, particularly if they aren't using a direct name match. The process of removing a malicious domain is arduous, and can even require legal involvement. As previously noted, hackers are sophisticated and trained to avoid detection, often relying on known hosts, which makes it more difficult for inexperienced security practitioners to effectively take them down. Relying on an external takedown service can help navigate the complex domain takedown process.

Spotlight on Phishing Kits

Phishing kits combine several impersonation techniques discussed in this report, including domain and social media threats. The targets of these kits are 3rd party relationships, the company's employees and its consumers. What makes phishing kits so difficult to detect is that oftentimes the phishing pages themselves are unindexed, meaning that the pages can only be found through direct messaging of the link.

Phishing kits generally include the code of the phishing website, infrastructure, and even distribution tools like mass mailers for a single fee. Hackers often rely on compromised pages to quickly stand up look-a-like content based on a previous wordpress exploit, thereby creating a page that is a perfect representation of your website, such as a banking login page. This allows phishing kit operators to run scams without having to worry about managing infrastructure or needing to design their own scams. Phishing kits offer an end-to-end phishing attack contained in a neat and structured compressed file. This is especially effective for intrusions leveraging impersonations, since phishing relies heavily on the brand as a pretext for carrying out a campaign. This also expands the pool of would-be hackers by making phishing a commodity and accessible to people who do not have the technical ability or desire to stand up their own scams.

In addition, because phishing kits are designed for ease of use, they allow for scam operations to be stood up at a larger scale. Even if a domain is identified as malicious and taken down, it is simple for hackers to stand up the kit on a new domain, with very little downtime. Even the compromised pages can be purchased, making the skill required to operate this campaign start and end with the ability to use a cryptocurrency.

The largest financial institutions of the world have been previously affected by phishing kits. It is clear that financial institutions offer lucrative opportunities for hackers to profit due to the nature of financial transactions and inherent trust built between financial consumers and the institutions themselves. As more and more become available, the economy of phishing kits will fluctuate in pricing, but also make more backdoored or cracked kits available for free. Since phishing is one of the more prolific forms of impersonation, this increases the risk to organizations affected by phishing kits, because the barrier to entry is much lower.

Hackers often rely on compromised pages to quickly stand up look-a-like content based on a previous wordpress exploit, thereby creating a page that is a perfect representation of your website.

Corporate Social Media Impersonations

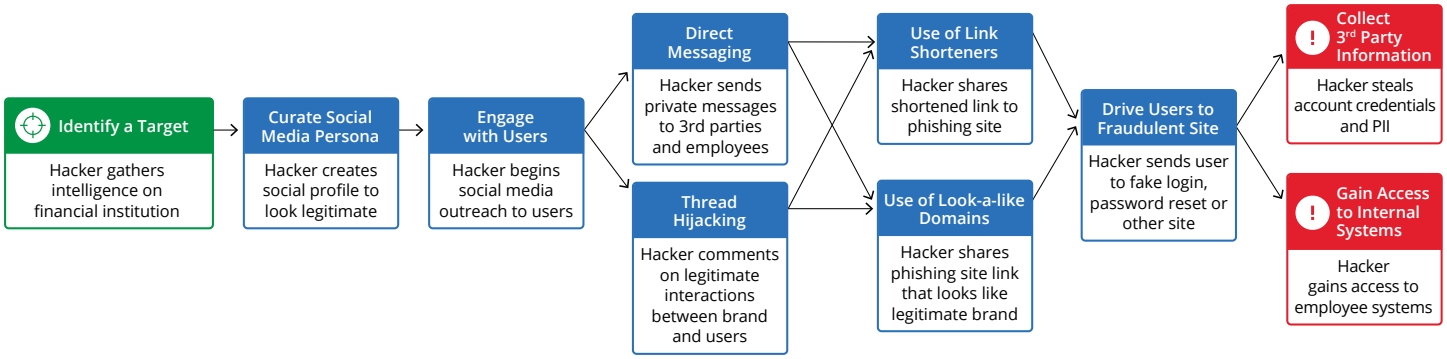
Perhaps the most widely known impersonation technique is the fake social media profile. Affecting everyday people and businesses alike, fake accounts on social media provide lucrative opportunities for hackers because they are quick and free to set up and immediately provide an audience - the legitimate network of the real account. While security teams may not traditionally think of social media accounts as "assets" they provide real value in engaging with customers and building awareness and therefore require protection like all other digital assets. Note that in this section we're speaking of corporate social media impersonations specifically - that is, fake accounts pretending to be your financial institution. There are other social media impersonations that target individuals that we'll discuss later in this report as well.

How Corporate Social Media Impersonations Are Used

An actor creates accounts on platforms where they know customers or employees of an organization visit and expect to engage with the institution. Actors leverage a combination of publicly available and leaked/compromised data to build a compelling and legitimate profile. Typically, this intelligence is curated from corporate websites, blog posts, social media websites and press releases. Once a persona is created, actors may spend time curating the profile by filling out additional fields, creating an organic network of peers, and even posting in a similar tone of voice to seem legitimate. When the actor is ready, the personas are used to interact with company employees to stage an attack, perform fraud on behalf of the threat actor, or be used to passively collect intelligence related to the target company or victim.

One of the main methods used by hackers to leverage corporate social media impersonations is thread hijacking. By impersonating the customer support function of the organization, the fake account will engage with the social media user in an attempt to drive them to a fraudulent page or phish their credentials. Using link shorteners or look-a-like domains, the attacker is able to drive the user to a fake banking login page, for instance. Because the profile itself and the associated link look legitimate, there are no real visual cues for the victim before the attack takes place. Thread hijacking often involves a combination of social media and domain impersonations, making this a powerful use case for the threat actor and a sizable challenge for defenders.

Corporate Social Media Impersonation Flow Chart



The Targets of Corporate Social Media Impersonations

Actors that impersonate financial institutions on social media have two targets: the brand itself and its consumers. Particularly for the financial services industry, consumers rely on social media for customer support such as help logging into accounts, transferring funds and accessing services. Social media is also a useful tool for financial institutions to promote offers such as sign on bonuses and savings to customers. Hackers recognize the lucrative opportunity that social media offers and the low barrier of entry to conduct these types of attacks and seek to capitalize on that opportunity.

Hackers often target consumers simply because they are the easiest and weakest link to fraudulent activity. This is true not only of social media impersonations but scams and other phishing tactics as well. There is a smaller subset of threat actors that target the financial institution themselves, typically targeting individual employees first to take unauthorized actions of divulged secrets. The tactics and intentions for these types of targets are essentially the same as impersonations targeting consumers, with the intent of stealing credentials and gaining access to the financial institution at large to carry out further malicious activity.

What to Do About Corporate Social Media Impersonations

The first step to addressing corporate social media impersonations is to recognize them as a security challenge, not just a marketing problem. While social media often falls to marketing, it's critical to recognize that these accounts are digital assets similar to your websites and therefore must be protected. Security teams should maintain documentation of the organization's full social media presence, including account credentials and who has access to those credentials. Similarly to identifying domain impersonations, continuous monitoring of social networks will enable your security team to quickly take action on early signs of fake accounts before they are weaponized.

Ultimately, it's important to think about moving beyond your security perimeter and focus on assets that give you visibility and remediation capability into digital platforms such as social media. This will allow you to understand the scope of the threats at play and prevent harm rather than just reacting to it. Conducting vulnerability assessments and social media pen tests will allow your security team to be prepared in the event that a social media-based intrusion occurs in the future. These assessments and tests should be done in conjunction with your marketing department, and perhaps even your legal department. By proactively reducing your vulnerabilities on this front, you'll make it harder for a threat actor to access the initial data required to make a convincing impersonation in the first place. By setting a proactive security strategy and strict access controls, hackers will likely move on to easier targets.

While social media often falls to marketing, it's critical to recognize that these accounts are digital assets similar to your websites and therefore must be protected.

How the Pandemic Has Changed Social Media Threats

On October 21, 2020, the **Federal Trade Commission (FTC) posted a data spotlight blog** about scams on social media. In the piece, the FTC data demonstrates a positive correlation between scam reporting and pandemic activity. The Consumer Sentinel Network is a cyber investigative tool made available to US government agencies to gain access to many reports made by consumers to the FTC related to scams, fraud, identity theft, and any crime involving improper business practices and schemes. Investigators can use this tool to measure loss and quantify the impact scam activity has on American citizens.

In 2019, reports of loss from fraud originating on social media reached $134 million. Within the first 6 months of 2020, this reported number rocketed to $117 million. When comparing the FTC report to ZeroFOX data, we've seen a positive correlation between the increase in reported scams to the FTC and an increase in scams found across all of our data sources.

Across industries in the ZeroFOX ecosystem, we've seen a 519% year over year increase in security incidents specifically related to scams. A further breakdown of customer cohort scams include:

- **423% increase** in Financial Services (scammers/money mulers targeting banking customers)
- **1579% increase** in Retail scams
- **226% increase** in Consumer Goods scams

And specific scam types:

- **295% increase** in HR scams, which could align with scammers looking to capitalize on work from home opportunities and lay-off/furloughs due to the pandemic
- **164% increase** in crypto giveaway scams, where an account is taken over or an impersonator profile is created to look like an influencer to peddle the scam
- **609% increase** in money flipping scams
- **100% increase** in impersonating profiles that have someone who claims to work for a company in HR, but does not

Related remediation activity has grown significantly as well. Across all industries, ZeroFOX has seen a 94% YoY increase in scam takedowns submitted and then subsequently removed. ZeroFOX assesses that scammers will likely continue to use the pandemic as an opportunity to take advantage of desperate consumers. Emotional and economic distress can leave victims vulnerable to these scams, especially ones designed to alleviate stress and reduce the impact of the pandemic. ZeroFOX also assesses that the scam types will remain constant and we will not see many new scams, mostly due to the years of experience and resources available for tried and tested scams. The old adage "don't fix what isn't broke" applies to bad actors as well.

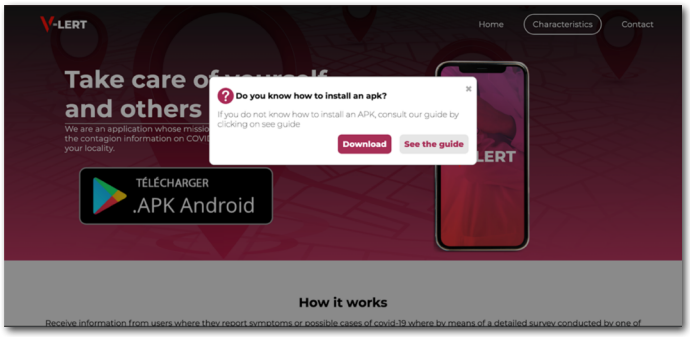
Fraudulent Mobile Apps

As many more financial institutions shift to digital-first interactions with consumers, mobile banking apps have become evermore prevalent as a consumer tool and hacker target. Mobile banking adoption has steadily increased in the last five years. **Business Insider Intelligence's Mobile Banking Competitive Edge Study** in 2019 found that 89% of survey respondents said they use mobile banking as their preferred method of banking. As adoption rises, mobile apps have become a vector ripe for impersonation abuse, particularly within app stores that maintain little to no regulation. Fraudulent mobile apps offer lucrative opportunities for threat actors to collect information including credentials and financial information as well as to distribute malware on the device on which the app was downloaded.

How Fraudulent Mobile Apps Are Used

As mobile banking technology has improved, hackers have found a window of opportunity in banking malware on mobile devices. Hackers create apps with similar names, imagery and descriptions to legitimate mobile banking apps in order to trick unsuspecting users. These apps are typically offered on less regulated stores such as Google Play and third party stores.

Android devices have been a top target for mobile app malware because users can install applications without Google Play Store verification, and in many cases are able to circumvent Google Play Store controls. Other third-party app stores tend to be regional-specific and cater to different languages beyond major western languages offering potential for several impersonations of the same banking app. The targets of these apps tend to be users that either cannot access the official app store or don't speak the primary language of the targeted financial institution's customer base.



Sample malicious APK and Android mobile app

What to Do About Fraudulent Mobile Apps

The first step to addressing fraudulent mobile apps is to make sure that your own legitimate apps are clearly distinguishable and easy for customers to find. Placing app download links on websites, on social media, in email signatures and other places where consumers may engage with the financial institution helps ensure they access the correct app. Monitoring third-party app stores is critical to quickly identifying fakes. This can be difficult to do manually, as there are hundreds of regional app stores that are broadly unregulated. Utilizing a continuous monitoring tool will save security teams valuable time and resources.

Android devices have been a top target for mobile app malware because users can install applications without Google Play Store verification, and in many cases are able to circumvent Google Play Store controls

Impersonations of Your People

The other major category is impersonations of people. These impersonations are typically found on social media, but can also be leveraged through fraudulent email addresses (business email compromise) or chatbots on fraudulent websites. Within this section, we'll discuss two top targets: executives and customer service agents, including customer support, IT services and other customer-facing roles.

Executive Impersonations

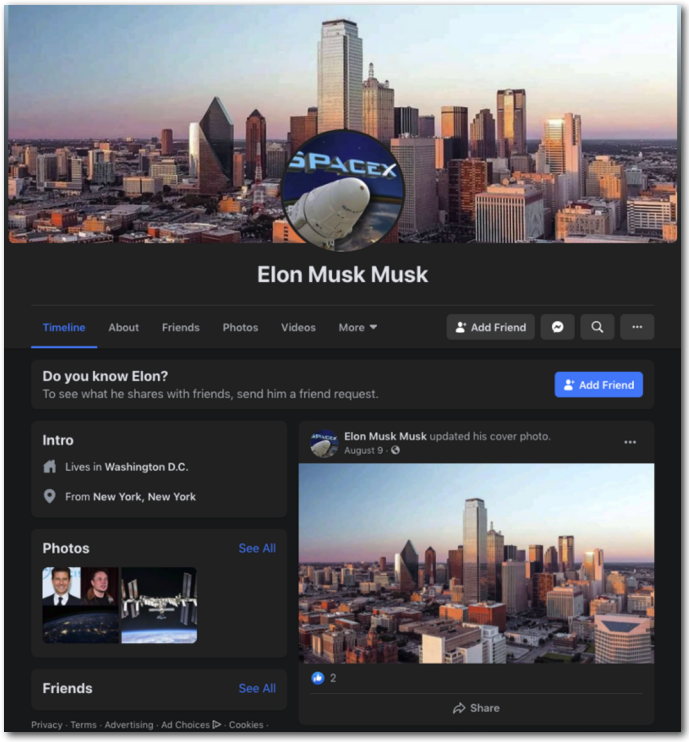
As with corporate social media impersonations, hackers create fraudulent social media accounts tied to high-profile individuals within a financial institution in order to target employees and consumers alike. Once created, these profiles can be used to phish, steal information and gain access to internal systems.

How Executive Impersonations Are Used

There are a number of ways executive impersonations are used as a door opener to an organization or to gain access to financial consumers. The most simple (and cheapest) method is by creating a social media profile based on the name, image and bio of an executive and immediately leveraging that profile for abuse. This requires reconnaissance prior to establishing the profile but requires no waiting time for weaponization. While hackers may find success with this simple method, profiles that have been created recently or lack engagement may be easily detected and removed.

A more sophisticated method that ZeroFOX has seen in recent years is called profile farming. Profile farming takes place prior to weaponization with specific actors specializing in profile farming. Profile farming involves actors creating new social media profiles that either have the same display name or a very similar name to the executive but also other modified information, such as a different profile picture or bio, to avoid detection. The actor then waits to weaponize these profiles in order to establish 'good behavior' or a level of credibility on the social network. Once they switch over the profile photo to match the executive, they'll begin leveraging the executive's name and notoriety to conduct fraud or money scams through direct messaging or posting links to scam-related activity, such as bitcoin scams as we've seen before, directly to their account. Profile farming has become much more common as social networks try to weed out inauthentic activity by identifying new or dormant accounts.

Hackers also look for other influential members of an organization to target employees with, such as HR professionals. In doing so, they are able to influence employees to share PII, sensitive information and even gain access to internal systems.



Impersonation profile on Facebook of the well-known CEO, Elon Musk

What to Do About Executive Impersonations

For impersonating accounts outside your direct control, timely awareness and response is key to mitigating damage. Early warning of impersonations, attempted account takeovers or of physical threats to executives, awareness of attack planning via dark web chatter, advertisement of breached data or stolen credentials, all provide real-time situational awareness based on indicators that allow organizations to take quick remediation actions. Actions can range from an account freeze to takedown of impersonating infrastructure, depending on severity. Doing so quickly, with efficiency and effectiveness, can prevent damages and encourage hackers to move to softer targets.

Other helpful actions executives and the security teams that protect them can take:

- Institute awareness training
- Continuously monitor for fake accounts and take immediate action to remove them before they can harm
- Routinely monitor public accounts (GitHub, for example) to avoid inadvertent sharing of credentials, IP or customer data
- Watch hacker forums (on dark web and elsewhere) for chatter on sale of passwords, credentials or planned attacks
- Harden owned account settings to lock down if PoC, image, ownership, or other aspects change

For impersonating accounts outside your direct control, timely awareness and response is key to mitigating damage.

Customer Support Impersonations

With more customer support services being provided online through chat portals, email and social media, customer service representatives have become top targets for impersonating infrastructure. Hackers leverage these profiles to target both consumers and employees, typically under the guise of an internal IT member.

How Customer Support Impersonations Are Used

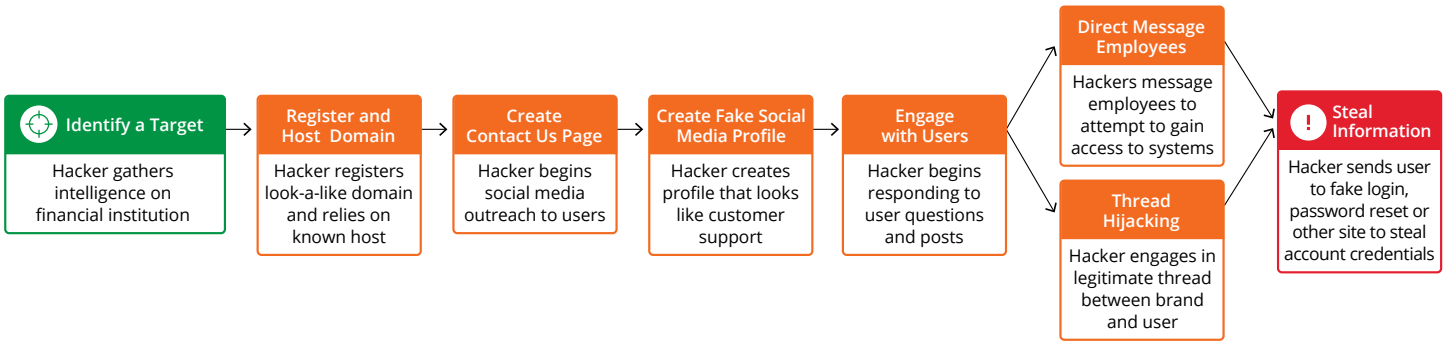
Hackers leverage online support channels to access consumers and employees alike. One prime example of this is the fake Contact Us page. By designing a look-a-like domain that matches a typical support form, hackers can gain access to your customers when they may be more susceptible to falling for a scam. Let's use an example we've previously discussed around thread hijacking on social media. Replying as the customer support rep with a fake profile, the attacker may provide a link to the customer, with the customer assuming that they are still chatting with the legitimate support rep. These types of attacks allow the actor to collect information from the consumer, be it account credentials or PII. Once revealed, they also negatively affect the reputation of the financial institution with its customer base.

Another angle that actors use to access customers and employees alike is through social engineering. Finding a direct email address, such as that of someone in a leadership position or IT department, gives hackers direct access to their targets. Even reaching a single employee can enable initial intrusion into the company, allowing hackers to conduct broader scale attacks. In addition to traditional email phishing tactics, hackers rely on other tactics such as voicemail phishing, smishing and more.

What to Do About Customer Support Impersonations

As with other types of impersonations, it's important for security teams to understand the tools and processes used by customer service and IT teams to assess where they may be vulnerable. Any external customer support tools such as social media accounts or online portals should use consistent branding, be clearly documented and easily accessible to customers to help eliminate the likelihood of an impersonator getting there first. Maintaining a continual presence on social media channels also reduces opportunities for hackers to establish an online persona of your organization. In the event that you do identify a customer support impersonation, whether on social media, email or web, work directly with the network to have the account removed or rely on an external service provider to handle the tactic on your behalf. As with any security response, the quicker you can find these types of impersonations and get them taken down, the better.

Customer Support Impersonation Flow Chart



The Ultimate Impact of Impersonations

Financial institutions of all sizes find themselves the targets of malicious activity leveraging impersonation. There is a false assumption that smaller banks won't face the same sophistication or volume of activity that large banks will face, but this is simply not the case. In many cases, smaller or regional banks have a more difficult time avoiding impersonation campaigns because hackers believe they will have a higher success rate than they might with a few large bank targets. Hackers know that large banks have more resources to address this problem, so will often target smaller banks where the payoff is lower but the possibility for success may be higher. Impersonations are a security challenge that must be addressed no matter the size of the security department or the organization overall.

While security teams may assume that the immediate impact of an impersonation-based campaign isn't as high as the impact of a data breach or other infrastructure intrusion, impersonations often serve as the foundation for broader scale intrusions. Therefore, if you are able to take down an impersonation before it can be weaponized, you may be able to prevent significant intrusions, phishing and data breaches.

Threat actors will frequently use lessons learned from previous fraud, phishing and malware families to bypass most of the learning phase of building a criminal enterprise. Obtaining leaked source code for Android banking malware, obtaining pirated copies of phishing kits, or acquiring curated fake profiles help actors bootstrap their operations much quicker than starting from scratch. This yields flourishing economies in the cybercrime underground, where suppliers will focus on providing access to these resources and not perform the hacks themselves. This points to the ever-accelerating dynamic nature of the threat, and need for a continual, real-time approach to security protection.

Ultimately, impersonations serve as the tip of the spear for many intrusions. By addressing them head on, you'll be able to proactively protect your internal networks and your external perimeter created by digital assets.

ZEROFOX

To learn more about how to protect your public attack surface with ZeroFOX, visit zerofox.com.

About ZeroFOX

ZeroFOX, the global category leader in digital risk protection, safeguards modern organizations from dynamic security risks across social media, mobile application, surface, deep and dark web, email and domains, and digital collaboration platforms. With complete global coverage and an Intel-backed artificial intelligence-based analysis engine, the ZeroFOX Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, brand hijacking, executive and location threats and more. The patented ZeroFOX Platform technology processes and protects millions of posts, messages and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Instagram, Pastebin, YouTube, mobile app stores, domains, cloud-based email and more.