ENTHEC

WHITEPAPER

BRAND PROTECTION:

Phishing, fraud and scam campaigns on social networks

kartos

XTI watchbots

kartos
XTI watchbots

Table of contents

kartos®
XTI watchbots

INTRODUCTION

In the digital age, social media has become integral to our lives and businesses, providing opportunities to connect, share content, and engage with diverse communities, including customers.

However, this growing reliance has also increased phishing, fraud, and scam campaigns in these virtual environments. These criminal practices have evolved, including corporate identity theft to deceive users and customers and obtain confidential information or illicit enrichment.

In this document, we will explore the growing problem that phishing, fraud, and scam campaigns with corporate identity theft on social networks pose for organizations, providing data on the techniques used by cybercriminals, the consequences for organizations of this type of cybercrime, and offering prevention and protection strategies against these constantly evolving cyber threats.

WHAT ARE PHISHING, FRAUD, AND SCAMS, AND HOW HAVE THEY ADAPTED TO SOCIAL MEDIA?

Phishing is a method used by cybercriminals to obtain sensitive information, such as passwords or credit card details, by impersonating a legitimate entity.

In the context of social media, scammers use sophisticated techniques to send direct messages or posts that appear to be from a reputable company or institution. Cybercriminals have adapted these tactics to the social media environment, taking advantage of users' trust and familiarity with these platforms.

In addition to phishing, cybercriminals use social media to carry out fraud and scam campaigns. These illegal activities include selling counterfeit goods, deceptive promotions, fraudulent investment schemes, etc.

Cybercriminals use corporate identity theft to carry out these phishing, fraud, and scam campaigns on social networks. Scammers impersonate well-known brands or specific brands they are interested in, using logos, images, and messages similar to legitimate businesses.

kartos®
XTI watchbots

THE USURPATION OF CORPORATE IDENTITY IN SOCIAL NETWORKS: A CONSTANTLY EVOLVING THREAT

Corporate identity theft, also known as brand abuse, on social media, encompasses a variety of tactics ranging from fake profiles impersonating the brand to distributing malicious content under the brand's name. This can end up causing significant damage to the public's reputation and trust in the brand. In addition, it can open the door to potential fraud and scams, triggering serious financial consequences.

PROFILE SPOOFING

Cybercriminals use similar names and logos to create fake profiles that mimic the genuine brand. These profiles are often used to spread false information, promote fraudulent products, or even scam clients.

SOCIAL NETWORKS PHISHING

Cybercriminals use people's familiarity with certain brands to send phishing messages. These messages may contain malicious links or requests for sensitive information, deceiving unsuspecting users.

POSTING MALICIOUS CONTENT

Attackers share infected links or files under the brand's name, taking advantage of the trust followers have in it. The purpose is the spread of malware or exposure to harmful content.

CUSTOMER SERVICES IMPERSONATION

Cybercriminals create accounts that impersonate the brand's customer service, responding to legitimate inquiries and often directing users to fake or dangerous sites.

ANALYZING THE IMPACT: CUSTOMER TRUST AND BRAND REPUTATION

Brand abuse on social media encompasses a variety of ploys, from creating fake profiles to spreading malicious content under the umbrella of the affected brand. This rapidly evolving practice has become so complex that it requires an equally sophisticated response from organizations, as it has very serious consequences:

- **Erosion of Customer Trust:** Brand abuse directly impacts customer trust. When users are exposed to fake profiles or malicious content under the name of a legitimate brand, it triggers a crisis of trust. Confusion and skepticism take hold of followers and customers, decreasing engagement and sales.
- **Brand Reputation at Risk:** A brand's reputation is one of its most valuable assets. Brand abuse or usurpation of corporate identity on social networks can irreparably damage this reputation. Malicious activities, such as spreading false information or promoting fraudulent products under a brand name, trigger negative reputational effects.
- **Financial and Legal Impact:** Beyond reputational and trust effects, trademark abuse can have significant financial and legal implications. Brands may incur direct losses due to declining sales and costs associated with reputation crisis management. In severe cases, trademark abuse can lead to litigation and regulatory penalties.

THE LIMITS OF EDUCATION AND AWARENESS

Educating and raising awareness among users and customers about this type of cybercrime so that they acquire skills to avoid deception is the main part of the strategies that organizations usually adopt in the fight against corporate identity theft.

However, protecting a brand requires a holistic approach in today's digital environment. While audience education and awareness are cornerstones, they cannot be the only line of defense. Brand abuse on social media ranges from creating fake profiles to distributing malicious content under the identity of a legitimate brand. This phenomenon has become increasingly sophisticated and dangerous, calling for a proactive identification and removal response that goes beyond the boundaries of user and customer education and awareness.

SOPHISTICATION OF ATTACKS

Cybercriminals have perfected their techniques. They now employ highly complex social engineering, which means that even well-informed users and customers can fall into carefully designed traps.

FALSE SENSE OF SECURITY

Despite proper training, users and customers may develop a false sense of security, believing they are exempt from deception. This can lead to decreased surveillance and increased susceptibility to attacks.

NEW FORMS OF ATTACK

Attackers are constantly innovating. Introducing techniques such as AI-assisted spoofing presents an additional challenge for audience education and awareness.

IMPACT ON BRAND TRUST AND REAL ORGANIZATION COMMUNICATIONS

Education and awareness are vital tools in the fight against cyber threats. However, a one-sided approach can have unintended side consequences:

- Impact on Brand Trust due to the Brand's perception of vulnerability. This perception can decrease confidence in the brand's ability to protect its digital assets.
- Decrease in the follow-up and impact of real and important brand communication campaigns:

  - Confusion between cybersecurity and brand messages: Excessive cybersecurity education can overshadow genuine brand communications.

  - Loss of focus on the brand's mission: When cybersecurity education becomes dominant, the brand's mission and values can get lost in the noise. This can lead to a lack of cohesion and direction in the brand's communication strategy.

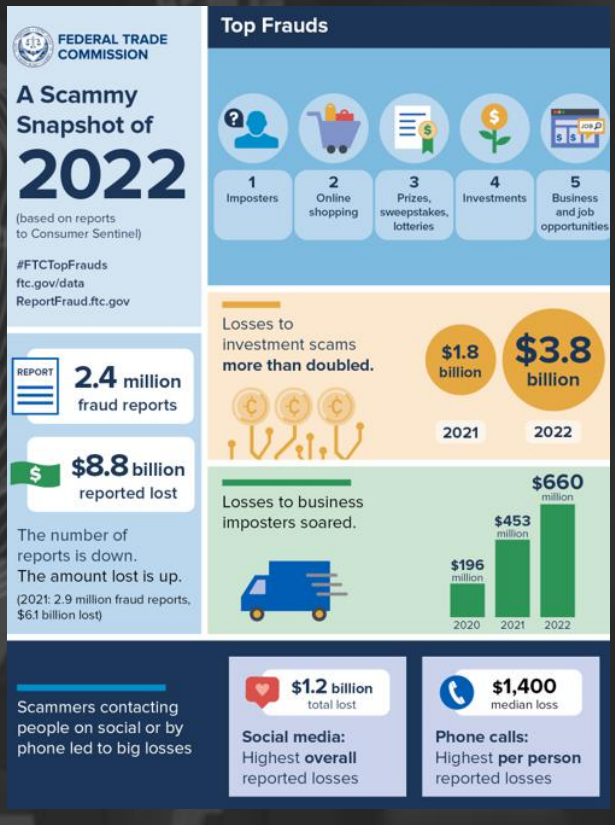
  - Distrust of any communication from the Brand that is not about Cybersecurity: Paradoxically, when education and awareness are the cornerstone of the strategy, the effect that it is trying to fight occurs: the erosion of trust in the Brand's communications that does not deal with Cybersecurity.

In practice, this means that the organization's commercial, advertising, recruitment, or loyalty campaigns are becoming less and less effective because the recipient finds it difficult to trust the content, while those that deal with Cybersecurity are the only ones in which they obtain full trust.

DATA:

According to data from the Federal Trade Commission (FTC), American consumers reported losing nearly $8.8 billion to fraud in 2022, an increase of more than 30% from the previous year.

Losses from fraud through social media platforms amounted to $1.2 billion in 2022.



Can a Brand feel calm when its strategy to combat the usurpation of its identity on social networks is based mainly on telling followers and customers to distrust any message its brand appears, no matter how credible it may be?

Is this a strategy truly aligned with the interests of the organization?

Isn't it a strategy that ends up having the effect it is trying to avoid?

CONSEQUENCES OF CORPORATE IDENTITY SPOOFING ON SOCIAL MEDIA

- **Financial Losses:** Corporate identity theft can lead to financial losses for businesses, both in lost sales and fines.
- **Reputational Damage:** Impersonation of corporate identity on social media damages an organization's reputation and its brand. Fraudsters may use the company's brand to spread false information or engage in unethical and even criminal behavior that negatively affects the organization's image.
- **Loss of Customer Trust**: After a phishing, fraud, or scam campaign with corporate identity theft on social networks, customers become distrustful of interacting with the organization if they believe it is not taking the appropriate measures to protect its Brand.
- **Legal Issues**: Corporate impersonation on social media can lead to legal problems for organizations when fraudsters use the Brand to engage in illegal activities, as the organization may initially be held liable and need to provide evidence to prove the impersonation.

HOW DOES CORPORATE IMPERSONATION ON SOCIAL MEDIA AFFECT CUSTOMER LOYALTY AND BRAND REPUTATION?

- **Loss of trust:** If customers believe the company is not taking the right steps to protect its brand, they are wary of interacting with it on social media.
- **Confusion**: Customers who can't distinguish between the organization's official and fake social media accounts may be confused by the company's messages and offers.
- **Negative brand image:** Corporate identity theft on social media damages an organization's image. If cybercriminals use the company's brand to spread false information or engage in unethical behavior, the organization's reputation is damaged.
- **Decreased engagement**: Corporate spoofing leads to decreased social media engagement. Customers who are unsure of the authenticity of your organization's social media accounts are less likely to engage with your organization.
- **Decreased loyalty**: Corporate impersonation leads to a progressive decrease in customer loyalty. Customers who feel the organization is not taking the right steps to protect its brand are less likely to remain loyal.

WHAT ARE SOME OF THE FINANCIAL RISKS ASSOCIATED WITH CORPORATE IMPERSONATION ON SOCIAL NETWORKS?

- **Loss of Revenue**: Corporate impersonation on social media can result in a loss of revenue for businesses due to lost sales to deceived or scammed customers.
- **Legal Fees**: Corporate identity spoofing can result in legal fees for organizations when cybercriminals use the corporate identity to engage in illegal activities, forcing the organization to take legal action to protect its brand.
- **Damage to Brand Equity**: Impersonation of corporate identity on social media damages a company's brand value. Cybercriminals use the brand to participate in phishing, fraud, scam campaigns or spread false information, damaging its image and reputation and decreasing its value.
- **Cost of Regaining Brand Trust:** The organization must invest in powerful communication campaigns to recover some of the lost brand trust after a successful corporate impersonation on social networks by cybercrime.

COMMON MISTAKES WHEN AVOIDING CORPORATE IMPERSONATION AND BRAND ABUSE ON SOCIAL MEDIA

- **Failure to monitor Social Networks:** Continuously monitoring social media for fraudulent use of your corporate identity allows fraudsters to use your brand with impunity to deceive customers.
- **Not having a proactive protection strategy:** When an organization does not have a proactive strategy in place to protect its brand on social networks, which prevents and neutralizes campaigns, it becomes vulnerable to being used for phishing attacks and other types of fraud.
- **Not being active on Social Networks:** Not having profiles on social networks or having them inactive means that the fake profiles created by cybercriminals can have greater credibility with customers and users.
- **Failure to protect the brand with advanced strategies and technologies:** The sophistication of cyberattacks makes it necessary to protect the organization that is up to the task and uses advanced strategies and technologies such as Artificial Intelligence and automation to provide the necessary responses.

ADVANCED DEFENSE STRATEGIES FOR BRAND PROTECTION

- **Cyber Intelligence Tools for Advanced Detection and Prevention:** Investment in state-of-the-art cyber intelligence and detection tools is essential. Artificial intelligence and machine learning-based solutions can identify fake profiles and malicious activity more effectively than traditional methods and track active or latent fraudulent social media campaigns to their complete elimination.
- **Behavior Analysis and Attack Patterns:** Understanding the behavior patterns of attackers is crucial. Constant monitoring and data analysis can reveal emerging trends and enable proactive responses.
- **Rapid Response and Recovery:** It is essential to have a well-defined response strategy to detect corporate identity theft in phishing, fraud, or scam campaigns on social networks. Rapid detection and responsiveness limit damage to the brand.
- **Collaboration with Social Networks Platforms:** It is crucial to have the ability to immediately report fake accounts or suspicious activity to social media platforms to speed up the response and removal of fraudulent profiles.

kartos®
XTI watchbots

BRAND THREATS CYBER INTELLIGENCE SOFTWARE SOLUTIONS HELP PREVENT

- **Counterfeit Products:** Detection of sites with counterfeit products and unauthorized sellers.
- **Online Scams:** Monitoring social networks, online marketplaces, and websites for phishing, fraud, and scam campaigns with fraudulent use of corporate identity.
- **Reputational Damage:** Monitoring social media for fraudulent activity causing reputational damage.
- **Trademark Infringement:** Monitoring domain registrations to detect fraudulent use and quickly remove fraudulent websites.
- **Unauthorized use of Brand Identity:** Using advanced image and logo recognition tools to find fake accounts that use corporate identity.
- **Unauthorized Use of Organization's Intellectual Property:** Monitoring social media to detect any misuse of intellectual property, using advanced algorithms to scan the internet and social media platforms.
- **Cyberattacks:** Detection and prevention of cyberattacks, including phishing attacks and malware.

KEY CAPABILITIES OF CYBER INTELLIGENCE TOOLS FOR SOCIAL MEDIA BRAND PROTECTION

- **Clear Web, Deep Web, Dark Web, and especially Social Networks Monitoring:** Software should provide automated monitoring and enforcement for legal and compliance teams, helping to ensure that the brand is properly represented on the web. This includes monitoring social network platforms, online marketplaces, and websites for counterfeit products or trademark infringement.
- **Monitoring and Removal of Domain and Subdomain Registrations:** The software should monitor domain registrations for any fraudulent use of the brand. Organization should also be able to remove fraudulent websites quickly.
- **Detection of Domains and Accounts similar to the Official Ones:** The Cyber Intelligence tool must be able to detect domains, subdomains, and accounts that are not the same but very similar to the official ones, either because they contain small and almost undetectable typographical errors, slight changes in the design or strange wording.
- **Monitoring, Alarms, and Reports with Accurate Data in Real-Time:** The software must automatically record data and issue alarms to detect brand abuse in real-time, as well as provide the necessary reports so that the organization can respond to complaints to the platforms and obtain the elimination of fraudulent profiles and campaigns.

kartos
XTI watchbots

BENEFITS OF USING CYBER INTELLIGENCE SOLUTIONS WITH BRAND PROTECTION ON SOCIAL NETWORKS

- Maintain brand integrity: Thanks to real-time detection of unauthorized or fraudulent use of the brand.
- Manage online reputation: Thanks to constantly monitoring social networks, online marketplaces, and websites in search of brand theft.
- Increase customer trust: By preventing the fraudulent use of corporate identity, companies increase customer trust and loyalty, demonstrating that they carry out a proactive protection strategy that does not shift responsibility to their customers or followers.
- Reduce potential revenue losses: Detecting and eliminating accounts opened for counterfeiting and fraud.
- Ensure a consistent and positive brand image: By detecting, reporting, and removing fraudulent websites and social media accounts.
- Detect impersonating websites and accounts: Allows organizations to take action to report the impersonation to social media platforms, request its removal, and destroy the threat.
- Detect phishing, fraud, and scam campaigns with corporate identity theft: Prevent customers and users from falling victim to these campaigns and reinforce their trust in the brand.
- Trace the source of the breach: Track and detect the source to take the necessary steps to eliminate the threat, including reporting online scams and monitoring social media for reputational damage.
- Accurate real-time monitoring, alarms, and reporting: Receive real-time data and analysis of corporate identity theft on social networks for phishing, fraud, or scam campaigns to deactivate them before they can reach customers and users and be successful.

kartos

XTI watchbots

AI layer that allows operation 100% automated without intervention in any part of the process.

Continuous operation 365x24x7, allowing you to detect new information leaks practically in real-time.

Strictly non-intrusive tool. The research is conducted on the Internet, the Deep Web, and the Dark Web and does not attack the IT perimeter of companies, so their operation and the information obtained strictly comply with the limits imposed by the legislation.

Maximum ease of use. No complex configuration is required. Simply enter the domain in the platform and it works autonomously without configuring search parameters or other criteria for locating information.

The only platform that analyzes conversations on social networks from the perspective of detecting threats and attacks beyond that relating to reputation and branding.

Automated, objective, and continuous monitoring of risks caused by third-parties belonging to the Company´s External Attack Surface.

EASM + DRPS + SRS

ON A SINGLE PLATFORM

Kartos XTI Watchbots is the Cyber Intelligence and Surveillance platform developed by Enthec to extend the security perimeter controlled by organizations. Conceived from a hacker strategy approach, Kartos is in a permanent R&D process to incorporate categories and capabilities advanced to the evolution of cyber attacks.

EXTERNAL ATTACK SURFACE MANAGEMENT

Detection of corporate assets and information about systems, cloud services and applications that are available and visible in the public domain to any cybercriminal.

DIGITAL RISK PROTECTION SERVICES

Detection of contextual information about possible attack agents, their tactics and processes to carry out malicious activities. Elimination of malicious activities on behalf of the organization.

SECURITY RATING SERVICES

Independent assessment of own and third-party risks, for a broad visualization of the cybersecurity maturity of any organization using an external approach. Expansion and weighting of the information provided by traditional third-party risk assessment methods.

Analysis of 9 Threat Categories

- Network
- DNS Health / Phishing
- Patch Management
- IP Reputation
- Web Security
- E-mail Security
- Leaked Documents
- Leaked Credentials
- Social Networks Intelligence

Learn more about our licenses.
Try the XTI Cyber-Intelligence for free. Start using Kartos.

hello@enthec.com

#AlwaysWatching

ENTHEC

@enthec

@enthecsolutions

@enthecsolutions

kartos
XTI watchbots