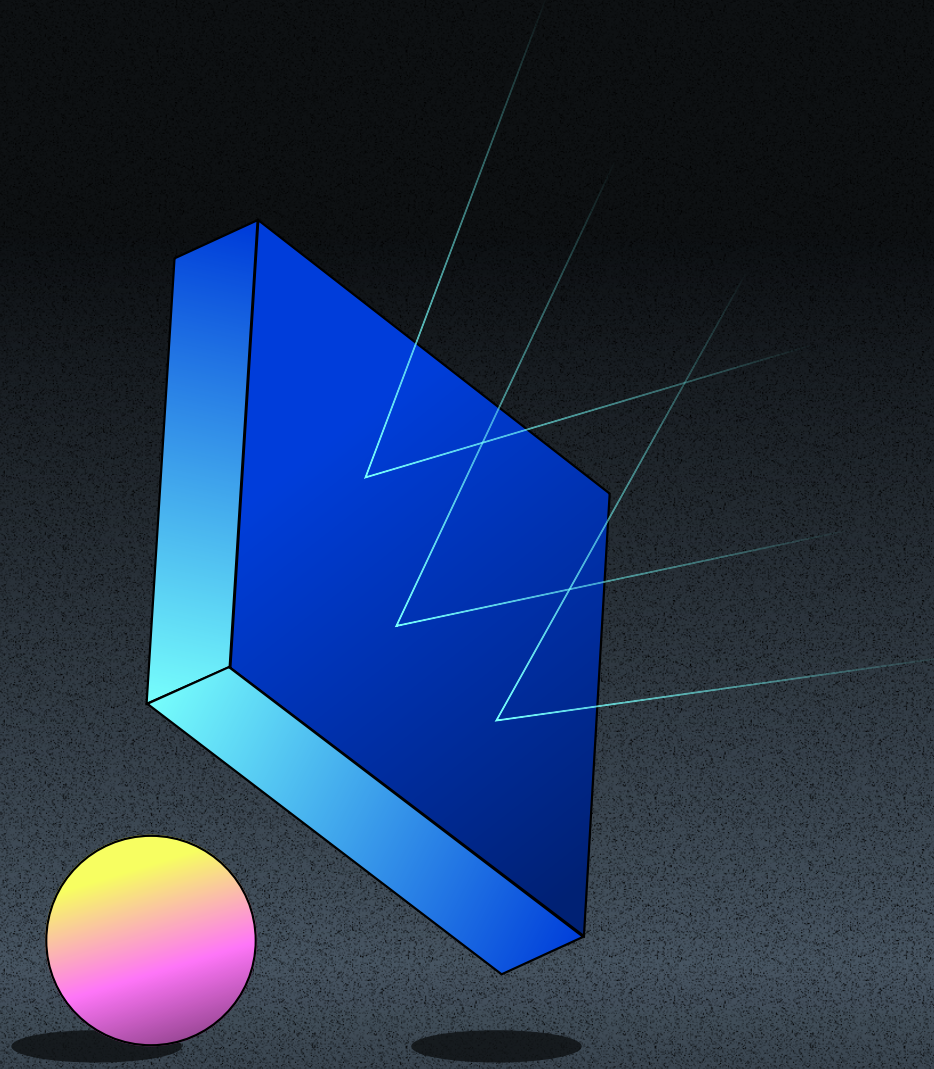
Doppel

The Executive Protection Guide

Doppel's Digital Protection Handbook for High Profile Employees and VIPs



Introduction

The more connectivity becomes embedded in every aspect of business and personal life, the more exposed executives and VIPs have become to cybercriminals. High-profile individuals, from corporate leaders to celebrities, face a growing number of digital threats that go beyond traditional cybersecurity concerns, into social media and telecommunications.

To address these challenges, the concept of digital executive protection has evolved, offering specialized strategies to safeguard the online presence and personal data of executives and industry leaders.

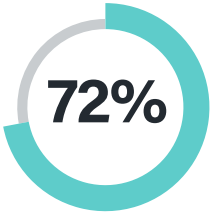
In this guide, we'll provide a comprehensive guide to digital protection strategies for executives and VIPs, exploring the threats they face, the consequences of these risks, and effective measures to ensure their security.

The Rising Threat Landscape for Executives and VIPs

Executives and high-profile individuals face an increasingly dangerous digital threat landscape.

According to a study conducted by GetApp, 72% of senior executives at U.S. companies surveyed were the targets of cyberattacks, and over half (54%) of US companies reported having experienced at least one identity fraud incident affecting a senior executive over the last 18 months.

"With AI, protecting executives is top of mind for all of the CISOs and Boards of Directors we meet," said Doppel Co-Founder and CEO Kevin Tian. "Their names, images, and likenesses (NIL) are ripe for social engineering and impersonation campaigns."



OF CYBERATTACKS TARGETED C-SUITE
US Companies Surveyed

EXPERIENCED IDENTITY FRAUD
US Companies Surveyed, last 18 months

From the Doppel Vision Platform

Data YTD, as of Oct 2024, among EP customers.

Detections

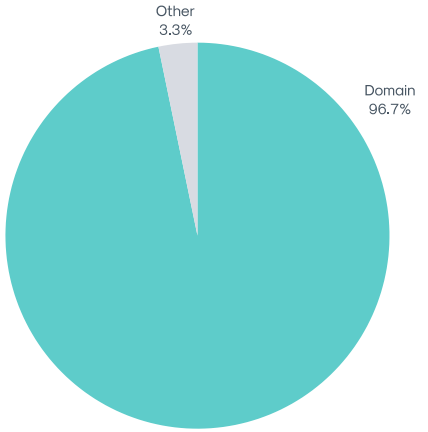
We've collected detection and takedown data from the Doppel platform and naturally found that our most mature detection module, domains, represented the majority of detections thus far this year.

TOTAL DETECTIONS

30,062,097

DOMAINS

96.7%



Detections other than Domains

With domains separated out, the mix of detections is split between TikTok, X (formerly Twitter), Zendesk, Instagram, and a slew of other public platforms.

TOTAL REMAINING

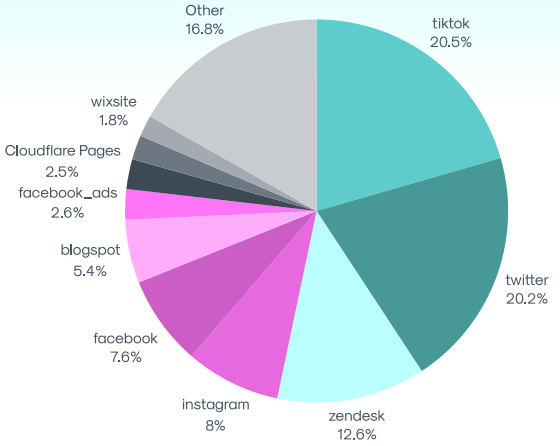
980,458

TIKTOK

20.5%

X (TWITTER)

20.2%



From the Doppel Vision Platform

Data YTD, as of Oct 2024, among EP customers.

From Detection to Takedown

Between Doppel's threat "detection" and "takedown" statuses, human expertise, in the form of both client review and Doppel review, takes place to determine a course of action. This review process leads to confirmation, reporting of the threat, and monitoring of the threat as it remains live before and up to takedown.

Steps leading to takedowns include:

- Detection
- Client Review
- Doppel Operations review
- Threat Reported to platform/provider
- Doppel Operations monitors for suspicious activity
- Doppel executes a takedown

Threats that are relevant, but no longer active prior to takedown, are archived but still on Doppel's radar, should they reemerge.

Takedowns

Takedowns were more evenly distributed across social media and domains. We also affected takedowns on hosting sites like Webflow and messaging apps like Telegram.

TOTAL TAKEDOWNS

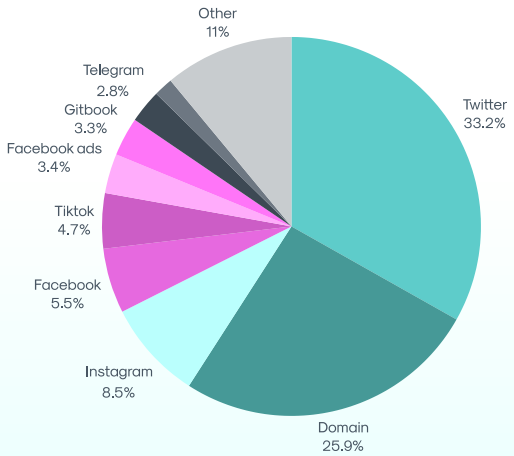
136,158

X (TWITTER)

33.2%

DOMAINS

20.2%



Executive Impersonation: The Opportunity for Cybercriminals

The appeal for cybercriminals is clear: these individuals have privileged access to sensitive corporate data, financial assets, and valuable networks.

The rise in executive cybersecurity incidents is driven by several factors:

- Increased use of social media and digital platforms by executives for both personal and professional purposes.
- High visibility in media and public life, making executives attractive targets for exploitation and impersonation.
- AI-driven social impersonation accounts and deepfake media that make it easier to fool employees and customers.

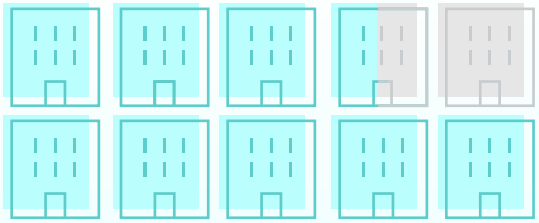
High-impact cyberattacks, such as executive impersonation or Business Email Compromise (BEC), can have catastrophic results. According to the UK National Cyber Security Centre, 84% of businesses were the victims of BEC attacks in 2023, costing businesses over $2.9 billion in losses, per the FBI IC3's Internet Crime Report 2023.

These targeted attacks are not just about financial gain—they often aim to damage reputations, disrupt operations, and exploit corporate vulnerabilities. As these attacks grow in sophistication, the need for robust, tailored protection strategies becomes paramount.

BEC Attacks, 2023

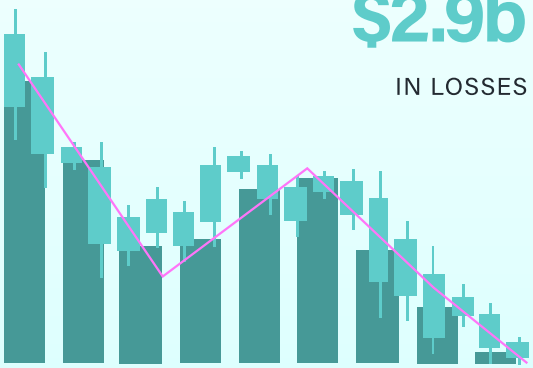
84%

OF BUSINESSES AFFECTED



$2.9b

IN LOSSES



What Digital Threats Are Targeting Executives and High-Profile Individuals Today?

Spear Phishing Attacks

Spear phishing is one of the most common methods used to target high-profile individuals. Unlike traditional phishing, which sends mass emails to a wide audience, spear phishing is highly targeted and personalized. Cybercriminals will often research executives' public profiles, social media accounts, and professional roles to craft messages that appear legitimate.

These messages trick executives into providing sensitive information or clicking malicious links, often leading to data breaches or financial theft.

Executive Impersonation

Impersonation attacks are increasingly prevalent. Cybercriminals assume the identity of an executive or VIP—often using stolen personal information or creating social media impersonation profiles. These fake accounts can be used to mislead business associates, defraud clients, or launch more intricate social engineering attacks.

Impersonation isn't limited to email; cybercriminals exploit social media platforms like LinkedIn, Twitter, and Instagram to build fraudulent personas that mimic the digital footprint of high-profile individuals. Such impersonations not only deceive contacts but also pose significant reputational risks.

Data Breaches

Executives and VIPs are often custodians of sensitive corporate data. Whether they're accessing company documents via mobile devices or maintaining contact with key stakeholders, this data is a valuable asset to cybercriminals. Data breaches targeting these individuals can result in the exposure of confidential business strategies, financial data, and even personal communications.

The consequences can extend beyond financial losses, potentially leading to long-term damage to both personal and organizational reputations.

The Impact of Executive and VIP Digital Threats

When cybercriminals successfully target high-profile individuals, the fallout can be devastating. The consequences are often felt across multiple dimensions, including financial, reputational, operational, and legal areas. Below are some of the most severe impacts that executives and VIPs face when subjected to digital threats.

Financial Loss

Many digital attacks against executives result in direct financial damage. Whether through fraudulent wire transfers, identity theft, or the loss of proprietary data, these attacks can lead to significant monetary losses. Executives with access to sensitive financial systems or company funds are prime targets for such schemes.

Reputational Damage

An executive's reputation is one of their most valuable assets. A successful executive impersonation attack or data breach can severely tarnish an individual's personal brand. For executives, a damaged reputation not only impacts their career prospects but also the public's perception of the companies they lead. Rebuilding trust after such incidents can be a long and arduous process.

Operational Disruption

When digital threats disrupt business operations, the ramifications can be far-reaching. The leakage of sensitive company information or the compromise of executive accounts can halt business processes, trigger internal crises, and even lead to the temporary closure of essential services.

Legal and Compliance Risks

High-profile individuals are subject to a range of regulatory frameworks. A breach involving sensitive data can lead to serious legal consequences, including fines, penalties, and lawsuits. Compliance with data protection regulations like GDPR or CCPA is critical, and failure to protect personal data adequately can lead to significant legal liabilities.

> "With AI, protecting executives is top of mind for all of the CISOs and Boards of Directors we meet. Their names, images, and likenesses (NIL) are ripe for social engineering and impersonation campaigns."
>
> **Kevin Tian,** Dopple CEO & Co-Founder

Strategies for Comprehensive Executive and VIP Cybersecurity

Given the high stakes, it's essential to implement comprehensive cybersecurity measures to protect executives and VIPs. Below are six key strategies to enhance their digital security:

Implementing Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) adds an extra layer of protection by requiring users to verify their identity through multiple steps. By using a combination of passwords, biometrics, or authentication apps, MFA significantly reduces the risk of unauthorized access to executive accounts.

Conducting Regular Security Training

Regular security training is crucial for executives and their support teams. Educating high-profile individuals on the latest phishing techniques, impersonation tactics, and security best practices ensures they are better equipped to recognize and avoid digital threats.

Using Threat Detection and Response Tools

Advanced threat detection and response tools are critical in monitoring executive and VIP digital footprints in real-time. These tools actively scan for signs of impersonation, phishing attempts, and other suspicious activities. Solutions like Doppel's AI-driven social engineering defense platform can identify threats early and respond quickly to mitigate their impact.

Establishing Robust Security Policies

Comprehensive security policies tailored to executives and VIPs should be a priority. These policies should cover everything from secure communication protocols to personal device management, ensuring that all digital activities are closely monitored and controlled.

Protecting Personal and Professional Digital Footprints

Executives often maintain extensive digital footprints through personal and professional accounts. Regular audits of social media profiles, personal email accounts, and professional networks can help reduce the risk of social media impersonation and other attacks. Encrypting sensitive data and limiting its exposure online are also essential steps.

Developing Incident Response Plans

No cybersecurity strategy is complete without a robust incident response plan. In the event of a breach, having a clear protocol in place ensures a quick and effective response. This can help minimize damage and maintain trust with stakeholders during a crisis.

Executive and VIP Digital Protection Tools: What to Look For

When selecting digital protection tools for executives and VIPs, it's essential to focus on platforms that offer comprehensive coverage across multiple attack vectors, including traditional modes like email and domains, and emerging attack channels like paid ad fraud, SEO poisoning, and new social media and telecommunications apps.

Here are some key features to look for in a digital executive protection solution:

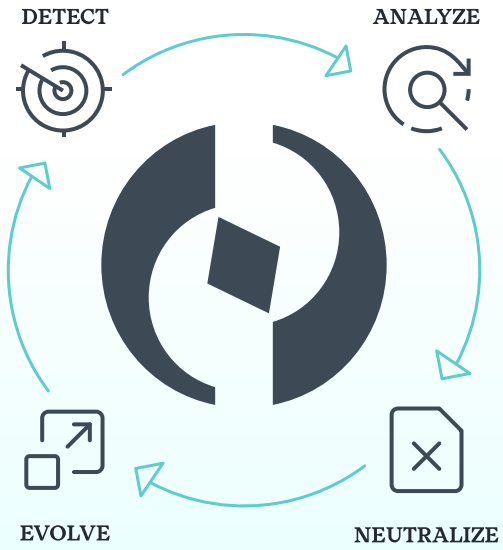
Real-time threat monitoring:
Solutions that offer continuous monitoring of personal and professional digital footprints, with alerts for suspicious activities.

Impersonation protection:
Tools that scan the web and social media for impersonation attempts and provide mechanisms for quickly taking down fraudulent accounts.

Phishing prevention:
Anti-phishing technologies that detect and block spear-phishing and impersonation attacks.

Data privacy and encryption:
Ensuring that sensitive data is securely encrypted and that only authorized individuals have access.

Incident response support:
Access to security experts and fast response teams to mitigate and resolve cyber incidents.



Platforms like **Doppel Vision** excel in offering these essential features, providing high-profile individuals with peace of mind that their digital lives are secure.

CASE STUDY

Doppel's **Executive Protection AI** Protects Sugar23's Team from Digital Impersonation Threats

Overview

Founded by Oscar Winner Michael Sugar, Sugar23 is an entertainment powerhouse, producing world-class TV, films, podcasts, books, and more. Managing an elite roster that includes leading actors, directors, writers, producers, and other influential figures, Sugar23 is at the forefront of blending Hollywood allure with brand power.

Always innovating, 2024 is a transformative time at Sugar23, as the brand works to integrate billion dollar consumer brands with its production pipeline, providing them with world-class creative and unprecedented opportunities for return-on-investment (ROI).

Problem

As Sugar23 continues to redefine the entertainment industry by bridging the gap between brands and Hollywood, it faces a growing challenge confronting the entire industry and its leading participants: An alarming rise in phishing, deepfakes, and digital impersonation threats. These threats target Sugar23's roster of executives, celebrities and thought leaders, seeking to exploit their high profiles and compromise their online presence. In line with its stature as an industry innovator and leader, Sugar23 has been at the forefront of seeking out leading-edge solutions to address this problem.

Results

Responding to the growing threat of impersonations and client deepfakes online, Doppel's AI-driven social engineering defense platform has been a game-changer for Sugar23. With vigilant, 24/7 detections and swift takedowns, Doppel has detected and taken down over 600 instances of impersonation for Sugar23's executives and partners across major social platforms like Instagram, Twitter, Facebook, and TikTok - with over 300 takedowns on Facebook alone. These impersonators were jeopardizing both the brand's reputation and the personal online security of its team.

Doppel's brand protection technology has been crucial in preserving Sugar23's unblemished digital reputation, allowing it to navigate the entertainment landscape with unwavering confidence and innovative spirit.

> "Doppel's proactive approach and rapid response have been integral in maintaining the integrity and security of our brand and our team's reputation(...). Their expertise in navigating the complex digital threats in today's entertainment world has been invaluable to Sugar23."
>
> **Evan Sils,** Sugar23 COO

Key Takeaways for Executive and VIP Digital Protection

Companies must face the reality that executives and VIPs are at an increased risk of targeted cyberattacks, from spear phishing and executive impersonation to data breaches. The consequences of these threats are severe, ranging from financial losses to long-term reputational damage.

To mitigate these risks, organizations must implement robust cybersecurity strategies, including the use of multi-factor authentication (MFA), regular security training, and advanced threat detection and response tools. Platforms like Doppel Vision offer critical features, from real-time monitoring to impersonation protection, ensuring that high-profile individuals can navigate the digital world securely.

By adopting a comprehensive approach to executive and VIP cybersecurity, digital protection professionals can safeguard their clients against evolving digital threats and ensure their ongoing success in a rapidly changing cyber environment.

For more information on how to protect executives and VIPs, and to explore the advanced capabilities of Doppel's social engineering defense platform, request a demo today!

Book your demo at
www.doppel.com/request-a-demo

Doppel

Defend what's real; **Disrupt what's not.**

Doppel is revolutionizing social engineering defense with our AI + human-powered platform. We don't just detect threats - we dismantle them. Phishing, BEC, impersonation, digital risks? Neutralized. Powered by Doppel Vision, our suite of tools — Brand Protection, Executive Protection, and Phishing Incident Response — adapts to every new threat in real time, securing your people, brand, and communications across channels.

Aa Aa

Aa Aa

Aa Aa

Aa Aa