FORTRA®

Securing the C-Suite: Advanced Executive Protection

As executives expand their online presence — both personally and professionally — it becomes increasingly challenging for security teams to monitor and distinguish legitimate threats. Executives face a wide range of online and physical risks, and as their digital footprints grow, so does their attractiveness as high-value targets for threat actors.

The Implications of Executive Threats

At its core, executive protection is essential for maintaining business stability. Impersonation and other security threats can lead to reputational harm, fraud, misinformation, and harassment. These incidents often result in costly remediation efforts, financial losses, and long-term brand damage. Digital threats and physical threats are becoming increasingly apparent. As executives become prominent on social media, their exposure increases — amplifying threats and making protection critical.

Social Media Impersonation

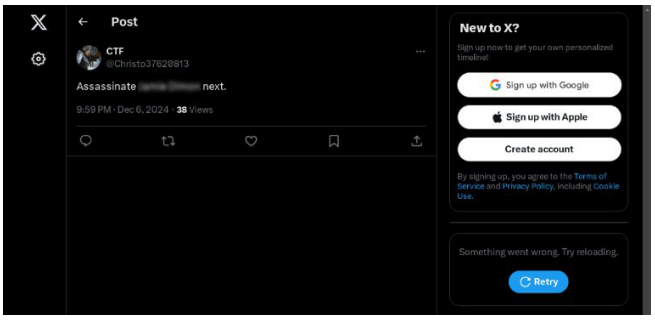
More than half of the world's population actively engages in social media. Scammers target this audience with a broad array of threats, including social media impersonation schemes, defamation, physical violence, and counterfeit ads. Threat actors are increasingly using social media to attack brands and their executives.

Domain Impersonation

A tactic used by threat actors where fake email addresses or domains are created based on valid organizations and their executives. These typo-squatted domains can be used to commit fraud, steal credentials with malware/phishing campaigns, trick users into sending money, and even to misrepresent your brand in a negative light.

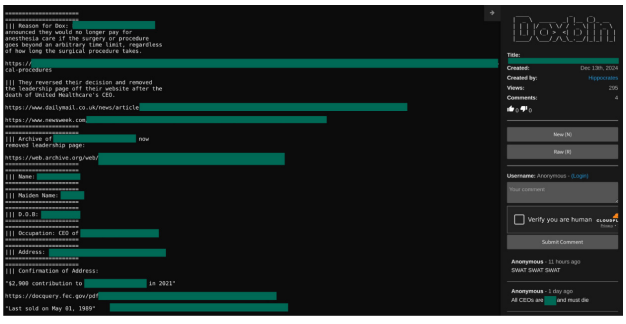
Compromised Credentials

According to Verizon's Data Breach Investigations Report, the use of stolen credentials remains the leading tactic employed by threat actors. Compromised credentials can wreak havoc on organizations, enabling data breaches, account takeovers, and significant reputational damage.



Physical Threats

A threat with the intent to cause physical harm may follow any of the previously mentioned threats. For example, posting threats on social media that incite violence against an executive or their family would constitute a threat of physical harm. When thinking of executive protection, the safety and physical well-being of executives must be a priority.



Doxing

Doxing is defined as the publishing of identifying information about an individual, and even their family, on the internet. For example, a threat actor can use address information to engage in activities such as violence, stalking, and targeted harassment.

Why Executive Targeting Works

The unique nature of an executive role along with human behavior and security gaps can create a perfect storm for threat actors. Easily accessible information on a prominent figure gives way to compromised credentials, impersonation tactics, and other threats. Threat actors can exploit the blend of visibility, trust, and convenience. In fact, Fortra research found that executive impersonation made up 51% of all social media impersonations last year.

The use of AI is rapidly gaining traction in the creation of fake social media accounts. Threat actors are leveraging AI to mimic imagery, speech, and even generate realistic responses to comments, making these accounts appear more legitimate. Some go further by populating fake profiles with convincing content to establish credibility, while others create private accounts and allow them to "age" over time to avoid detection and build perceived authenticity.

Unique Challenges of Executive Threats

Many organizations lack the capabilities to monitor dark web mentions, social media threats, and credential leaks that specifically target their high-profile individuals. And with a lack of resources, delays can increase the damage and physical harm caused by executive threats which can escalate into a public crisis. This can be especially true if the threat originates in an executive's personal digital environment.

While the digital footprints of executives are prime targets, the lines between personal and professional presence can blur. Using personal devices for work, the same password for multiple accounts, and even social media sharing methods can make detection difficult for security teams.

Creating an Advanced Executive Protection Plan

Having strong protection for executives can prevent security breaches, keep leaders safe from harm, and stop harmful disruptions of business. The following are steps your organization can take to elevate executive protection:

Prioritize solutions that quickly detect and validate threats targeting executives.

Fortra cuts through the noise to quickly identify real threats targeting executives. High fidelity, technology-driven results, and expert human analysis add critical context needed to identify and stop threats. This delivers complete visibility into malicious online activity that exposes corporate executives to serious risk including physical harm.

Implement social media monitoring tools that offer both threat detection and mitigation.

Strengthening social media protection by taking down threats before they cause damage can be difficult and time-consuming. Each platform enforces unique policies and procedures for removing content and suspending accounts. Effective social media brand protection also takes time to gather the intelligence needed to determine if a profile is malicious. For these reasons, many enterprises lack the time, expertise, and budget to mitigate threats.

With Fortra, once a social media threat is identified, we immediately act. We have strong business relationships, procedural knowledge, and experience needed to quickly stop these attacks. Fortra's brand protection mitigates and minimizes security threats.

Use dark web and credential monitoring to identify exposed employee and customer credentials.

With focused, direct monitoring of marketplaces and other dark web sites to identify references to stolen data and criminal activity associated with enterprises, Fortra Brand Protection delivers high-value intelligence and links key points of data to threat actor personas to continue surveillance and monitor for changes in activity. Whether it's stolen credentials, the exploitation of source code, monitoring threatening chatter, or the distribution of malware exploit kits, Fortra's dark web surveillance helps mitigate future attacks.

Fortra Threat Intelligence quickly responds and implements countermeasures to guard against fraud. Threat Intelligence delivers broad visibility into stolen employee and customer credentials revealed from dark web sites and harvested from third-party leaks, infostealers, botnets, and other forms of malware. Enhanced visibility allows you to quickly respond and implement countermeasures, such as alerting the proper authorities, forced password resets, and lockouts to guard against potential account takeovers, breaches, and malware attacks.

Dark Web Brand Monitoring
Dark sites, marketplaces and forums

Brand and Executive mentions, Stolen PII, card data, BINs, emails Phishing kits, Fraud tools Initial Access Brokers

Continuous targeted surveillance
Monitor for changes in activity

Compromised Credentials Monitoring
Infostealers, botnets and other malware

Actionable compromised logins
Emails, passwords, secret codes
Not parked behind paywalls

Implement proactive countermeasures
Forced password resets/account lockouts
Stop exfiltration of outbound transfers

Deploy advanced email security and phishing protection to defend against targeted attacks.

Fortra Email Security solutions stop deceptive impersonation attacks like BEC, targeted social engineering ploys, and spear phishing attempts. Through AI-based predictive technology and data science, Fortra solutions like Cloud Email Protection, DMARC Protection, Threat Intelligence Services, and Suspicious Email Analysis give you a comprehensive, proactive security plan.

Treat all identified threats with urgency and due diligence.

The moment a threat is identified, ...time is not on your side. Treating identified threats with urgency can help minimize remediation efforts, financial losses, brand damage, and harassment and harm to your executives and their families.

Invest in a robust security awareness training program for employees at all levels.

Even the most advanced cybersecurity technology can't fully protect your organization without informed, vigilant end users. Having engaging, interactive security awareness training can give people a clear understanding of what suspicious activity looks like and simple, accessible tools to report potential threats.

Fortra's award-winning security awareness training delivers targeted, engaging training with a practical, people-centric approach. Each learning module and phishing simulation template is designed to reduce risk and help create a strong human line of defense against cyberattacks.

Establish and regularly test an incident response plan specifically for executive-targeted threats.

A strong incident response plan for executive-targeted threats mitigates damage and minimizes potential harm to the organization and its executives. An organization should always be ready.

Securing the C-Suite Will Help Secure the Organization

As executives' digital presence continues to grow, so too does their vulnerability to a wide array of online and physical threats. Protecting these key individuals is vital to safeguarding both their personal well-being and the stability of the organization they lead. By prioritizing comprehensive security measures, such as advanced threat detection, social media monitoring, and credential protection, businesses can stay ahead of potential risks. Additionally, fostering a culture of security awareness and preparing for rapid response can significantly mitigate the impact of attacks. With the right tools and strategies in place, organizations can effectively defend their executives from both digital and physical threats, ensuring long-term safety and business continuity.

Fortra offers full visibility across the attack chain, disrupting attacks before they succeed.
With a vast array of solutions and capabilities, Fortra protects organizations and their executives better.

Learn More

FORTRA®

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.