SAFEGUARD CYBER

CASE STUDY

Leading Cybersecurity Enterprise Protects Brand Value by Securing Social Accounts from Takeover and Combating Website and Profile Spoofing

Automated scanning of the surface and dark web enables company to prevent account takeovers and initiate 132 takedowns of fake domains and imposter social accounts per year– protecting brand reputation and industry credibility.

An attacker took over the company's official LinkedIn account, evading detection from the incumbent security provider, Proofpoint. **This takeover threatened both credibility and human capital.**

Via spoofed domains and social profiles, bad actors were also setting up fake customer support departments, and taking money from users. This spoofing further harmed credibility and **customer experience.**

With SafeGuard Cyber, the company can now **reliably defend against account takeovers.**

Through SafeGuard, the company is now alerted whenever a fake domain or profile is created, and can initiate takedowns.

Safeguarding a Hard-Won Reputation

By implementing **advanced digital risk protection** with the SafeGuard Cyber platform, a leading global cybersecurity company maintains 24/7 protection of its social channels, and automates the detection of spoofed domains and profiles for takedown. The company proactively monitors both the surface and dark web for:

- Bad actors seeking to initiate a takeover of company accounts on LinkedIn and other cloud channels.
- Domains posing as the company's support department. These imposters have previously taken payment from unsuspecting consumers for non-existent technical help.

This proactive monitoring allows the company to discover and take action against digital risks in real time. The brand has the power to repel takedowns, and immediately initiate takedowns of spook domains and profiles, minimizing the risk of reputational damage.

"We assumed that GoDaddy, LinkedIn, and Twitter all take security as seriously as we do. But that's not the case. The big players don't have this covered. **With SafeGuard Cyber, we have achieved true digital risk protection.** Now, we can sleep well at night."

- Head of Digital Media

The Challenge: Takeovers & Impostors

A leading cybersecurity company with over $2.5-billion in annual revenue and 7,000+ employees suffered multiple attacks on its brand:

1. Account Takeover

An attacker took over the company's official LinkedIn account, evading detection from the incumbent provider, Proofpoint. This takeover threatened both the company's credibility and its human capital, as human resources had recently digitized the entire hiring process.

2. Domain Spoofing and Social Media Imposters

On both the surface and dark web, bad actors were creating fake domains, and fake profiles on LinkedIn and Twitter. These impostors were offering fraudulent customer support. Unwitting internet users were paying hundreds of dollars for non-existent technical help. The company's real support department caught wind of these scams from aggrieved users.

Using Proofpoint, the company was not being alerted with the speed and precision necessary to repel resist attempts at account takeover. Additionally, IT teams were stuck manually searching for spoofed profiles and domains. This was time-consuming and ineffective. When an imposter was found, IT had to work with web hosting companies and social media platforms to attempt takedowns. This was a slow and convoluted process. During the delays, brand reputation continued to suffer.

"Truth is, I don't want to think about security. I want to think about how I can generate 1,000 downloads of a whitepaper that might get us a million dollars in sales! **The amazing thing about SafeGuard is that the tool is quickly set up, it works correctly, and then you just leave it alone.** It works its magic, and we can all get on with our lives."

- Head of Digital Media

The Impact: Brand Damage & Revenue Loss

As a leading cybersecurity enterprise, these attacks presented a real threat to brand reputation, with a potential impact on revenue. The company branded themselves as savvy and capable cybersecurity experts. However, as the company's Head of Digital Media recalls, "The perception was 'Hey, you guys can't even secure yourself on LinkedIn. How are you going to protect me?'"

Even though online victims were targeted by imposters, when they suffered an attack, they directed their anger at the company itself. "It was a really bad experience for the brand. We had unhappy customers who always blamed us, no matter what." The company worried that bad actors using their name for nefarious purposes might soon hurt their NPS. This could have a tangible impact on revenue.

Digital Risk Protection Drives Efficiency, Helping Teams Focus on Business Growth

Using the SafeGuard platform, the company has gained "visibility like we'd never had before." IT teams saved time and money, and let the SafeGuard platform do the work for them. With SafeGuard, the company now:

- Automatically detects and defends against account takeover attacks.
- Automates the detection of potential spoofed domains and profiles.
- Receives a notification whenever an impostor comes into existence – whether on the surface or dark web.
- Centralizes their view of these digital risks within a single dashboard.
- Rapidly initiates takedowns of spoofed accounts and domains.
- Prioritizes threats so that they always deal with the worst threats first.
- Automates the record-keeping of all actions taken, with a view to future audits.

Best of all, this digital risk protection happens without drawing on any additional resources.

Get our full **Digital Risk Guide** here.

SEE WHAT'S POSSIBLE WHEN YOUR DIGITAL CHANNELS ARE SAFE

Start a 30-day trial

SAFEGUARD CYBER

Americas
410A East Main St.
Charlottesville, VA
22902 USA

sales@safeguardcyber.com

1-800-974-3515 U.S. & Canada