proofpoint.

ARE YOU MONITORING & PROTECTING YOUR COMPANY’S DIGITAL FOOTPRINT?

WHAT IS A CORPORATE DIGITAL FOOTPRINT?

Since the dawn of the digital age, organizations have embraced new opportunities to engage with customers across digital channels. First, consumers saw the birth of corporate websites and email marketing. Companies then followed with branded social media accounts and mobile apps. They also empowered employees and independent advisors to engage in social selling.

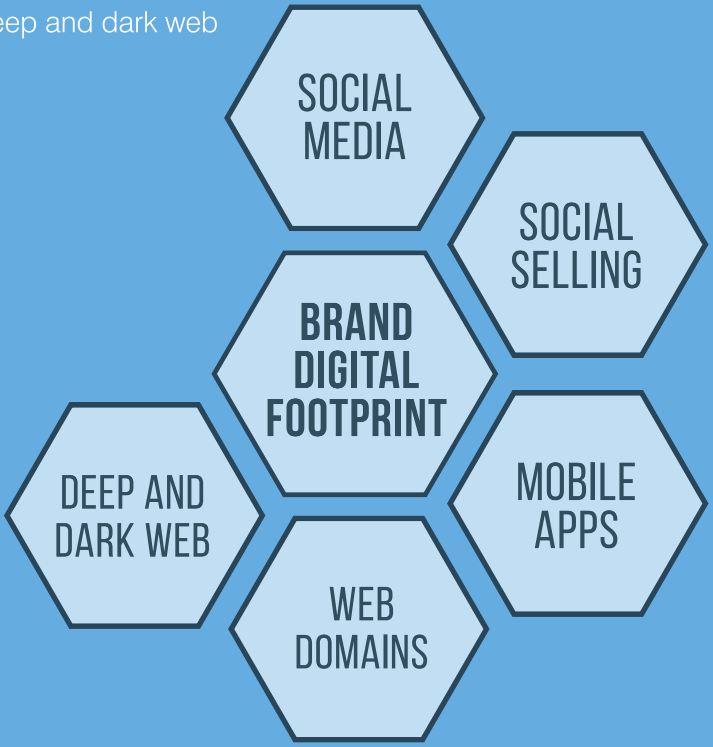
Your digital presence is critical to providing a cohesive customer experience. It also exposes your company to digital risk. Digital risks are especially dangerous and hard to combat. That's because they target people on infrastructure that sits outside of your corporate environment.

There's another issue too. Whether or not you engage in a digital channel such as social media, cyber criminals can create fake accounts that appear to represent your brand. Even in the deep and dark web—where corporations have clearly opted out—bad actors can defraud your brand or plan attacks on your key personnel and physical assets.

THE TAKEAWAY:

You need to consistently monitor and secure your organization's digital footprint in all channels, even if you do not have an official brand presence in one. These include:

- Social media
- Employee social selling
- Web domains
- Mobile apps
- Deep and dark web



SOCIAL MEDIA

SOCIAL SELLING

BRAND DIGITAL FOOTPRINT

DEEP AND DARK WEB

MOBILE APPS

WEB DOMAINS

WHAT ARE THE DIGITAL RISKS?

Cyber criminals have modernized their techniques to exploit the gap between your digital engagement and the ineffective security controls. Digital attacks expose your company and the people who trust it to an array of security, brand, and compliance risks.

CYBER THREATS

- Malware
- Phishing
- Other cyber-attacks targeted at your fans and followers

EXECUTIVE THREATS

- Doxing (published contact info and other personal data so that people can easily harass the executive)
- Reputation risks
- Credential phishing
- Physical threats across digital spheres

DATA EXPOSURE

Attacks on your digital presence to gain access to:

- Your customers' credentials
- Your sensitive corporate data

DOMAIN PHISHING

Spoofed branded domains for credential phishing

BRAND IMPERSONATION

Digital presence that imitates your brand to:

- Sell knockoff versions of your products
- Steal intellectual property

LOCATION THREATS

Protests and physical threats against or near your corporate locations

DOMAIN BRAND PRESENCE

The internet has grown to more than 330 million unique domain names and three billion users.[1, 2] The vast size and popularity provides companies with one of the richest customer-engagement channels. It has made it equally attractive for threat actors to register domains that imitate your brand. They use these lookalike domains in coordinated web and email phishing schemes. These impostors can register hundreds of lookalike brand domains per day.

Domains registered by someone other than the brand are on the rise. In 2016, for every brand-owned defensive registration (to preempt potential typosquatting), someone else registered 10 lookalikes. In 2017, suspicious registrations outnumbered brand-owned defensive registrations 20-to-1.[3]

In addition to mimicking your domain presence, bad actors piggyback on your brand's goodwill. Criminals use the lookalike domains to:

- Highjack your advertising traffic
- Deliver email phishing schemes
- Sell knockoff versions of your products
- Steal intellectual property

Chances are, you take precautions to protect your brand-owned domain presence. Monitoring your domain footprint for any suspicious or infringing domains is just as critical. Impostors can tarnish your brand and put your customers at risk.

[1] Verisign. "Domain Name Industry Brief." July 2018.

[2] Statistica. "Number of internet users worldwide." March 2017.

[3] Proofpoint. "Q3 2017 Quarterly Threat Report." October 2017.

MANAGE THE RISKS OF FRAUDULENT BRAND DOMAINS

PHISHING AND CYBERTHREATS

- Lookalike domains that are part of a web or social media phishing scheme
- Also used as the sender domain in email attacks and to lure your customers to sites that are infected with malware
- Designed to trick your customers into giving up their credentials or other sensitive information

LOST TRANSACTION DOLLARS

- Profit seekers spoof your domains to divert your traffic to generate ad revenue, sell knockoff versions of your products, or peddle competing products
- These ploys can lead to real revenue losses
- The Methbot scheme spoofed 6,000 U.S. domains and stole $5 million in fraudulent revenue per day[4]

CUSTOMER TURNOVER

- Infringing domains hurt your brand trust and customer experience
- When a bad actor spoofing your domain negatively impacts your customers, they could attribute the bad experience to your brand
- 73% of customers reconsider using a company if it fails to keep their data safe[5]

[4] Fortune. “The Russian Methbot Scam Is Just the Tip of the Ad Fraud Iceberg.” December 2016.

[5] Deloitte. “Cyber attacks leave a fifth of consumers out of pocket.” November 2015.

SOCIAL MEDIA BRAND PRESENCE

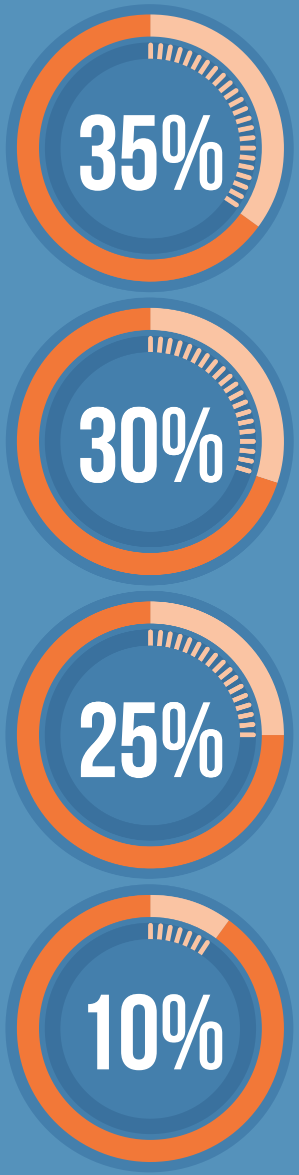
Social media is a great way to promote your products and interact with customers. Consumers turn to social media to engage with their favorite brands. In fact, 74% rely on social media to guide their purchases.[6] But with all this engagement, there are also risks from brand-related accounts you don't own. Fraudsters create lookalike brand accounts to scam your customers.

A Proofpoint study reported 19% of social media accounts associated with the 10 biggest brands are fraudulent. Social media phishing links grew 70%, and fake customer-support accounts used for phishing jumped 300% from Q1–Q2 in 2017.[7]

But impostors aren't the only issue. You also need to manage risks on your official brand-owned accounts. As your social presence and fan base grows, so does your exposure to offensive content, security threats, and compliance risks. And you must also consider your brand ambassadors' personal social media accounts. Your social selling program shouldn't hurt your brand or create compliance violations.

The Takeaway: Discovering and protecting your social footprint is vital to preserving your brand's reputation.

2017 MOST COMMON SOCIAL MEDIA SCAMS[8]



35% Free blockbuster movie streaming

30% Work from home and make easy money

25% Offers for free items to get a click

10% Brand fraud: fake coupons, free flights

[6] MarkMonitor. "Brand Abuse Lurking on Social Media." October 2015.

[7] Proofpoint. "Q2 2017 Quarterly Threat Report." August 2017.

[8] Proofpoint. "2018 Human Factor Report." April 2018.

MANAGE THE SOCIAL MEDIA RISKS

&#!* !@*** !#		#Phishing #HateText #Malware		
OFFENSIVE CONTENT	**ACCOUNT TAKEOVER**	**HASHTAG HIJACKING**	**COMPLIANCE RISKS**	**FRAUDULENT AND BRAND PROTEST ACCOUNTS**
Whether it's a "cyber punk" or an unhappy customer, abusive and offensive content on your company's social accounts diminishes your brand value and detracts customer engagement.	Companies have hundreds of social media accounts, dozens of admins with login privileges, and multiple authorized publishing applications. This complexity introduces risk for bad actors to take over your account and fill your feeds with harmful content.	Once you've invested in making a hashtag popular, anyone can use it so that their post lands on your social wall. Hijacking happens when someone uses your hashtag for a different purpose than you originally intended.	Regulated companies need to adhere to rules on managing social media accounts and communications. These also extend to your advisors who participate in your social selling programs.	Fraudsters set up accounts to masquerade as your brand and take advantage of your customers by distributing scams, counterfeit goods, phishing, and junk ads. Cyber criminals also create fake customer support accounts to phish credentials.

MOBILE APP BRAND PRESENCE

Today's mobile app ecosystem is large and dynamic. Users have 3.6 million apps to choose from in Google Play, the largest app store.[9] And hundreds of secondary third-party app stores offer millions more apps—legitimate or otherwise. Mobile apps are fertile ground for cyber criminals looking to impersonate your company and unleash attacks on the people who trust it. According to Marketing Science, 40% of mobile app inventory is fraudulent.

Keeping track of your mobile app presence and identifying fraudulent brand apps is important part of safeguarding your corporate digital footprint.

FRAUDULENT APPS

- Criminals create applications that imitate your brand—even if your company hasn't created an official mobile app.
- When unsuspecting customers install the app, it can steal their credentials, distribute malware, or access personal data stored on their device.

UNSANCTIONED APPS

- Managing your mobile app lifecycle can be hard. Apps can get published without going through your company's quality assurance and security review processes.
- Outdated versions of your app can remain on third-party stores after you release a newer version.

UNAUTHORIZED THIRD-PARTY HOSTING

- Hundreds of lesser known third-party app stores may host your brand's apps for download—without your knowledge or consent.
- These are popular stores for hackers to post modified versions of your app that deliver an attack payload.
- Unauthorized third-party hosting damages your brand reputation and customer engagement.

[9] AppBran. "Number of Android applications." February 2018.

DEEP AND DARK WEB RISKS

The deep and dark web emerged in recent years as the private place to engage on the internet. The websites are not indexed by search engines, and users need a Tor browser to access it. Given the "promise of anonymity" inherent in the dark web, it is a hot spot for posts and discussions that can pose huge security risks to your employees and office locations. In fact, 57% of the dark web sites designed for Tor facilitate criminal activity.[10]

MANAGE THE DARK WEB RISKS TO YOUR BRAND

EXECUTIVE RISKS				LOCATION RISKS		
DOXING	PHYSICAL THREATS	ACCOUNT COMPROMISE	REPUTATION RISKS	LONE WOLF ATTACKS	THREATENING LANGUAGE	PROTESTS
Bad actors can publish personal information about your executives to a wide audience. Your executives can then be threatened by anyone who wants to harass or harm them.	Cyberstalking, intimidation, and direct threats to your executives can deeply damage their sense of safety and wellbeing. From business and vacation travel to social media activity, there are many ways an executive can be tracked and eventually attacked.	Access to your executives' privileged credentials can lead to an orchestrated cyber-attack. Key executives' emails and passwords can be sold in the dark web. These actions can enable attackers to compromise accounts and exploit your company's confidential information.	People sometimes vent online about a company or flame its executives. This can be a one-time cyber jab. But often, threat actors turn up as antagonists who use profanity and hate speech to create a stir about a key executive and disrupt their day-to-day lives.	Organizations need to be aware of real-time threats and events in and around your key locations, such as your corporate headquarters and retail sites. Lone wolf attacks may be out of your company's control. But you can manage the risks when your company gets visibility into them and has a response plan in place	Organizations should monitor the digital universe for threatening language from suspicious and disgruntled people who are in and around your key locations. These issues can lead to critical events around populated areas, such as concerts, corporate-hosted events, holiday parades, sports arenas, and more.	Coordinated events where people are protesting or rioting near your business locations prevent successful day-to-day business and can impact employee safety.

[10] Daniel Moore, Thomas Rid. "Cryptopolitik and the Darknet." February 2016.

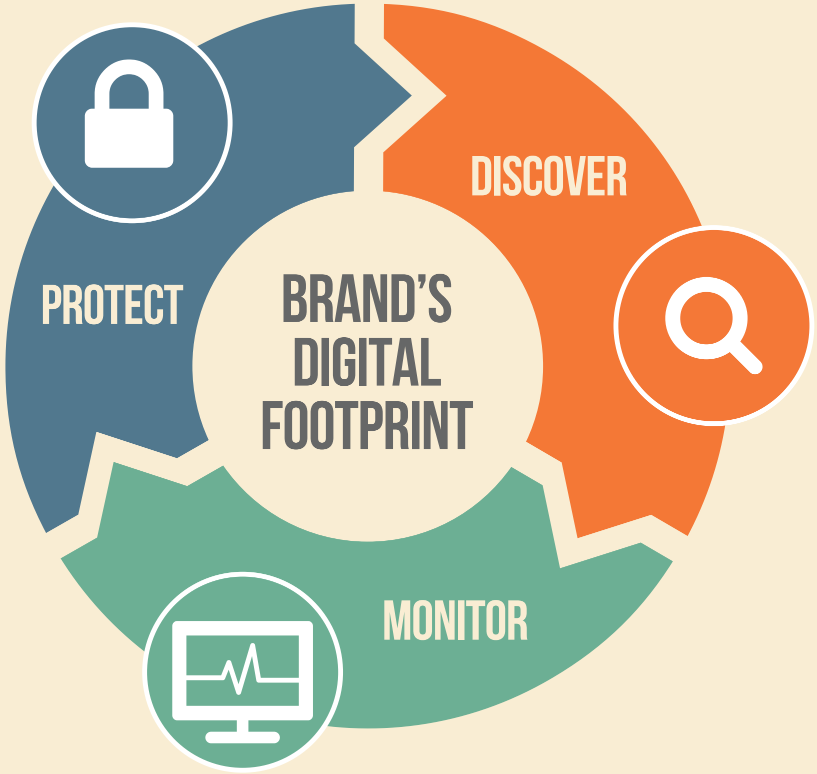
PROOFPOINT PROTECTS YOUR DIGITAL FOOTPRINT

Managing a brand's digital presence has traditionally been a manual, ad hoc effort. Processes are often reactive, and they may focus only on a specific channel.

Given the breadth and seriousness of digital risks to your brand and customers, monitoring and protecting your organization's digital footprint is critical across all of these channels:

- Social media
- Employee social selling
- Web domains
- Mobile apps
- Deep and dark web

3 STEPS TO MANAGING YOUR BRAND'S DIGITAL FOOTPRINT



DISCOVER

Scan digital channels to gain visibility of your brand's presence and assess risk.

MONITOR

Consistently monitor your brand's digital footprint to ensure it's free from digital risks.

PROTECT

Protect your footprint from brand fraud, attacks, malicious content, compliance violations, and other digital risks.

THE PROOFPOINT DIFFERENCE

Proofpoint Digital Risk Protection looks beyond your perimeter to deliver comprehensive security, brand, and compliance protection against digital risks. We provide real-time discovery, monitoring, and protection across social, mobile, domains, and the deep and dark web for risks to your brand.

It's the only solution that gives you a holistic defense for all your digital engagement channels.

SOCIAL MEDIA

- Discovers your brand's social presence with just a few clicks
- Automatically removes malicious content from your official brand accounts
- Detects account takeovers and locks down compromised accounts
- Monitors hashtags and brand terms for reputation and security threats to your organization
- Monitors digital content for threats to your executives, employees, and physical locations
- Controls connected applications
- Prevents phishing attacks on your followers

DOMAINS

- Provides visibility of suspicious domains, dormant domains, and your brand's defensive (typosquatting prevention) domains
- Quickly detects URLs that are part of active phishing campaigns
- Delivers automated alerts when new, risky domains are detected or their takedown status changes

MOBILE APPS

- Finds mobile apps associated with your brand
- Helps you detect and respond to risky mobile apps
- Scans official app stores and hundreds of secondary stores
- Gives you a complete list with just a few clicks

DEEP AND DARK WEB

- Analyzes more than 15 million deep, dark, and surface daily
- Detects threats to your brand, executives, and locations
- Provides detailed, real-time threat monitoring
- Increases cyber intelligence and peace of mind

LEARN MORE

To learn more about Proofpoint Digital Risk Protection solutions visit:

proofpoint.com/us/products/digital-risk-protection

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.