OUTSEER

An RSA Company

Top 5 Brand Impersonation Attacks

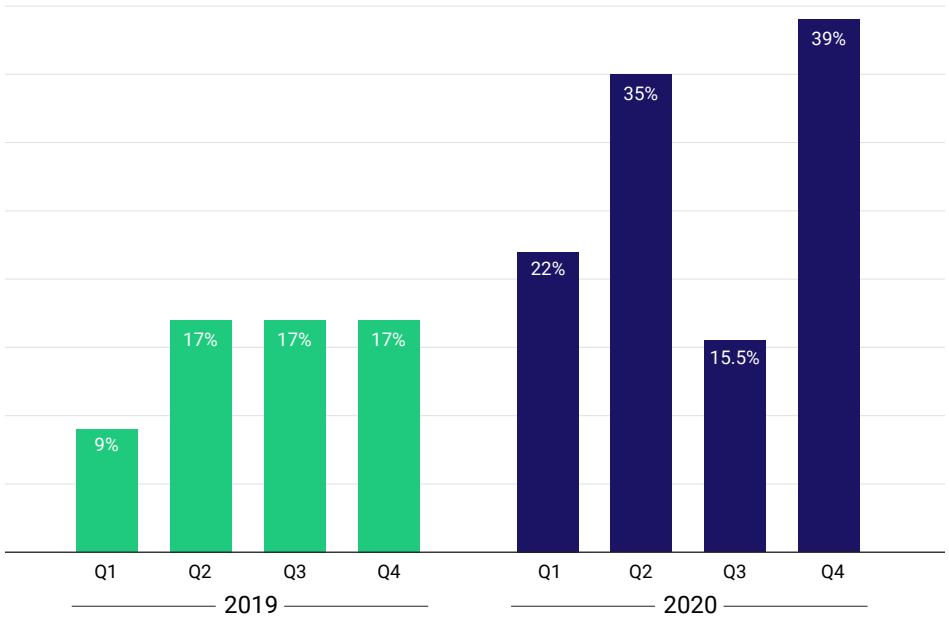
Protecting Your Customers and Your Organization from Phishing and Malware Sites, Rogue Mobile Apps, Fraudulent Social Media Pages & More

Brandjacking:
How Fraudsters Exploit Your Brand

Your organization's most valuable asset is your brand. But today, a growing number of businesses face mounting financial and reputational risks from cybercriminals who impersonate their brands.

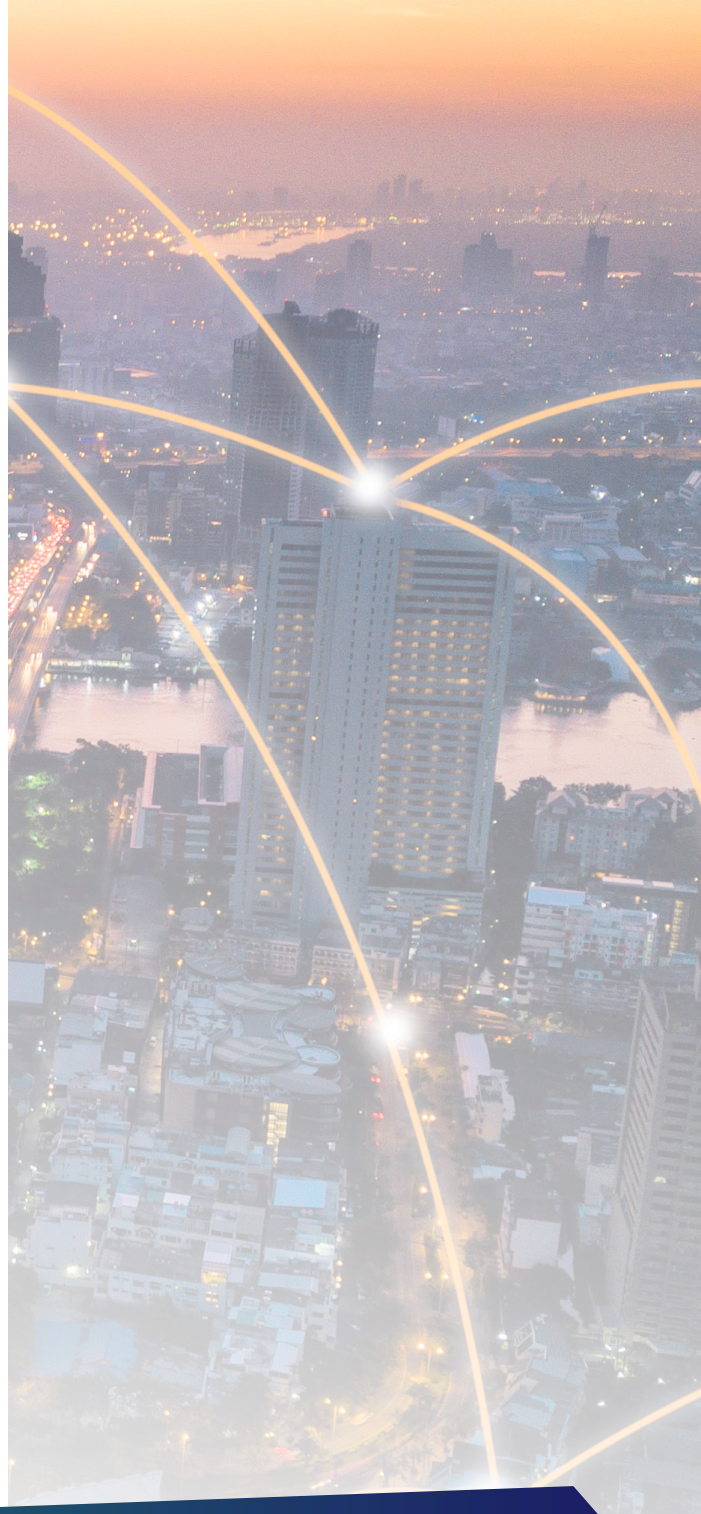
In these attacks, cybercriminals use phony websites, mobile apps, or social media pages, as well as bogus emails, voicemails, or text messages. All designed to look like the real deal. And all crafted to trick your employees and customers into authorizing money transfers or revealing login credentials or sensitive data. And it's happening at a rate Outseer has never previously seen.

Percentage of Brand Abuse Fraud Attacks[1]



Source: Outseer

NEXT The High Cost of Brand Impersonation



The High Cost of Brand Impersonation

According to the FBI, brand impersonation was a primary driver in more than half of all losses from cybercrime in 2020. The price tag: Nearly $2 billion in just the US alone. But beyond the immediate financial loss, these attacks can continue to cost you plenty.

Despite being one of the victims in these crimes, the blame will fall squarely on your brand. And as news and social media rants proliferate, it can cause lasting financial damage. Forrester notes that lost customer trust and even heightened customer suspicion can impact a company's revenue by 10% to 25% in a single year[2].

The cost of brand impersonation affects multiple functions across organizations, from marketing and security, to HR and risk management. The chart below shows each function's brand protection priorities.

Security Team

Decrease identity theft, account takeovers and fraud incidents

Identify stolen credentials, pcards or PII sold by criminals on the open, dark and deep web

Improve and focus fraud investigation prioritization to improve operational efficiencies and external threat detection rates

Risk, Compliance & Legal

Reduce risk and exposure of fraud losses and data privacy compliance violations

Assess exposure for M&A and third parties

Identify data leakage (corporate financials, trade secrets, PII and IP)

Human Resources

Monitor digital collaboration platforms and social media for inappropriate sharing of corporate information and compliance violations

Protect against executive impersonation and other threats targeting or impersonating VIPs

Marketing Team

Protect brand from digital impersonation, fake mobile apps, social media accounts and websites

Improve customer trust and experience

Reduce financial, competitive advantage and reputational loss associated with stolen IP and other data leakage

NEXT The Many Faces of Fraud

Cybercriminals have turned to digital brand impersonation for two reasons. For one thing, organizations lack the visibility and human resources to monitor these channels. For another, consumer adoption of digital channels has dramatically accelerated over the past year thanks to the COVID-19 pandemic.

In Q2 2020 **U.S. retail e-commerce sales grew 31.8%** from Q1 2020 and **44.5%** from Q2 2019.[3]

of US consumers say COVID-19 influenced their decision to try a **new digital banking app or website**.[4]

Imposter Syndrome: Top 5 Ways Fraudsters Use & Abuse Your Brand

When you don't protect your brand and digital brand assets from fraud and cybercrime attacks, you put revenue and customer trust at risk. You also endanger the significant investments your company has made to build its brand over time and develop assets like your website and mobile apps.

On the following pages, you'll learn how cybercriminals are impersonating your brand in the digital world, and why. You'll also find a variety of recommendations for protecting your brand and your bottom line from these attacks.

These are the steps Outseer takes every day to keep hundreds of the highest profile banks, retailers, healthcare providers and other organizations safe from brand abuse and other forms of fraud and cybercrime. They can work for you, too.

NEXT Cybercriminals Are Posing As Your Top Execs

Cybercriminals Are Posing As Your Top Execs

Just ask Elon Musk. In just the last few years, the Tesla founder has had his Twitter account both hacked and impersonated. In both instances, bogus tweets encouraged Twitter users to deposit bitcoin in a fraudulent account.[5] But while the hack was shut down fast, the phony account netted the perpetrators $150,000 in bitcoin.[6]

The problem: This is just one of countless examples of cybercriminals impersonating top executives. And increasingly, they're widening their nets to target a wider range of companies, not just those with celebrity CEOs. If you don't think it can happen to you, cybercriminals are happy to prove you wrong.

And Twitter's not the only channel they're using—far from it. The most insidious form of impersonation today is business email compromise (BEC). This is where cybercriminals impersonate senior executives in phishing emails to employees, customers, or business partners and suppliers. These emails do enormous damage to corporate brands and to executives' personal reputations. And they often pave the way to costly data breaches and regulatory fines.

Since 2016, the FBI's Internet Crime Complaint Center reported

185 thousand+
incidents of business email compromise

$28 billion
or more in actual losses.

The best way to make a case for digital brand protection may be to show your executives how they're being targeted for attacks.

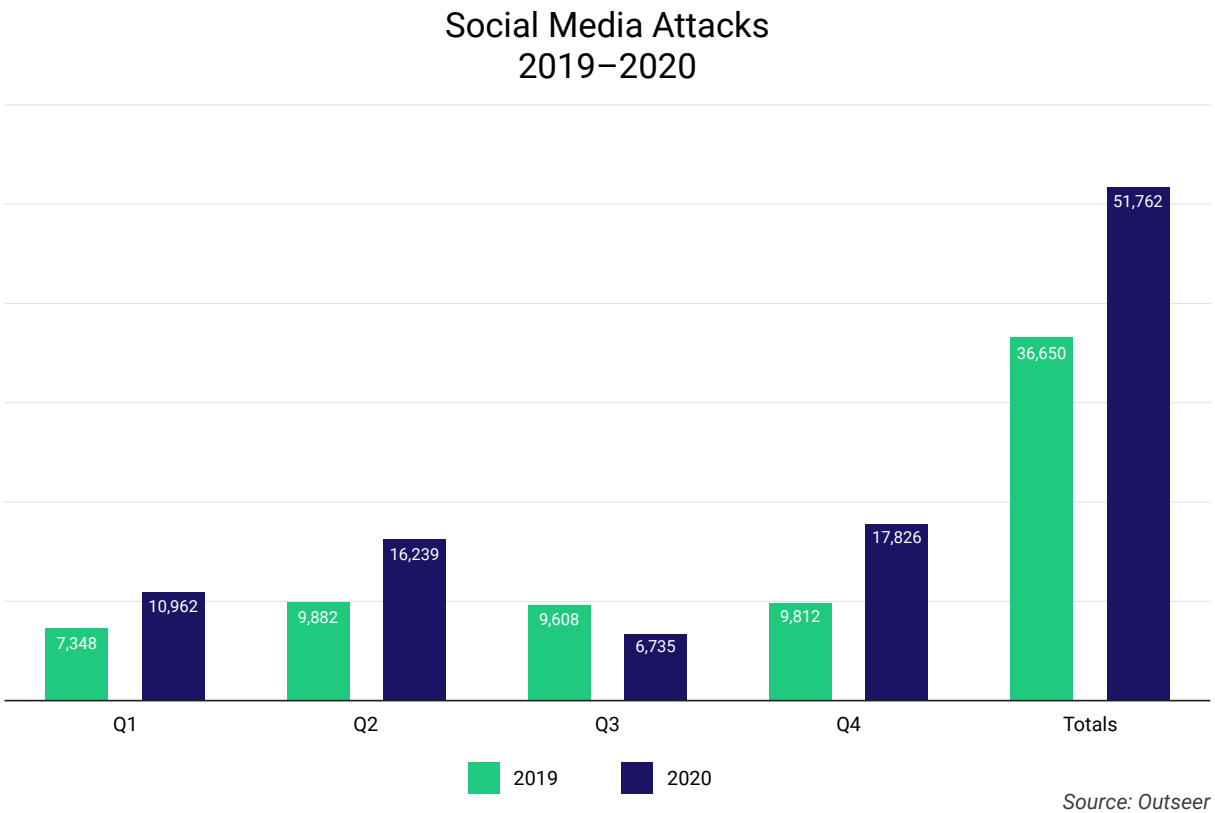
- Be on the lookout for business email compromise.
- Keep an eye on social media platforms for fake profiles of your executives.
- Monitor cybercrime forums for chatter targeting your executives for doxing, ransomware, and other forms of extortion.

NEXT More Reasons to Monitor Social Media

More Reasons to Monitor Social Media

Outseer has reported widely on the prevalence of cybercrime in social media. In addition to setting up accounts impersonating executives, cybercriminals also set up fake company profiles where they hide malicious links within bogus promotions.

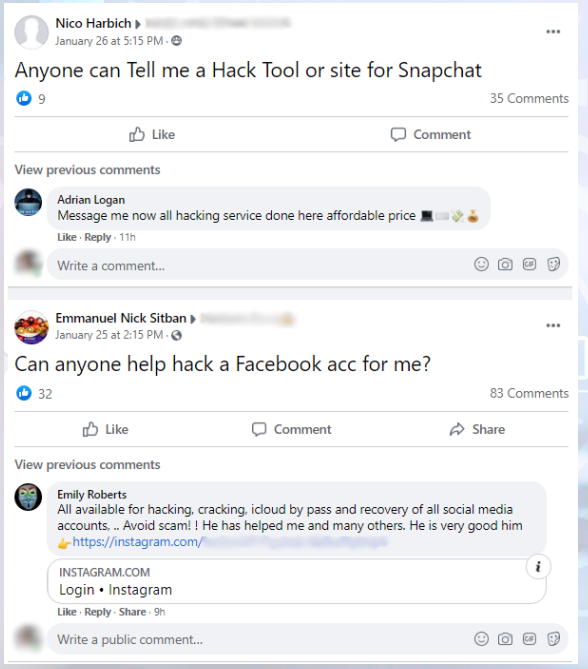
Fraudsters also use social media platforms to sell stolen credentials, payment card data, and more. So it's prudent to monitor social platforms to ensure your company's sensitive data isn't appearing on a fraud forum (and if it is, to get it removed pronto to prevent additional brand damage).



Source: Outseer

NEXT Watch Out for Rogue Mobile Apps

Monitor social media platforms for fake accounts using your company's brand, to ensure your company's data isn't appearing on fraud forums, and to make sure employees' posts aren't creating legal, reputational or compliance risks for your organization..



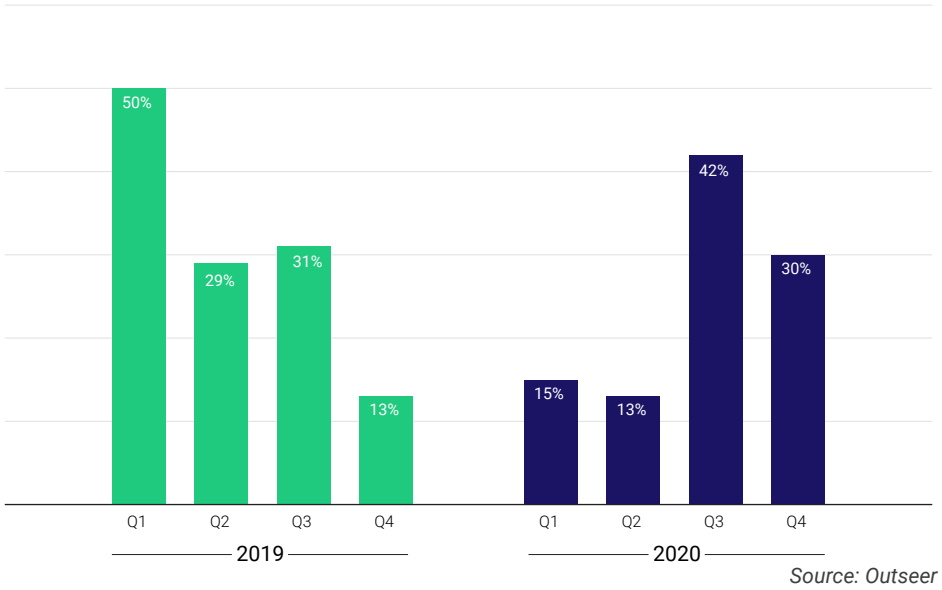
Watch Out for Rogue Mobile Apps

Rogue mobile apps are counterfeit apps designed to look like trusted brands' legitimate apps, and they're growing more prolific—and more dangerous—by the day.

When rogue mobile apps first began appearing on app stores in 2010, they were mainly designed to steal people's contacts or access their photos. Now many of these apps are designed to give attackers root-level access to an individual's mobile device so that they can compromise other, legitimate apps and gain access to the user's credentials and any payment card data stored on the device.

Rogue mobile apps represent the fastest-growing attack technique. During the third quarter of 2020, over 18 thousand cybercrime attacks originated via rogue mobile apps, representing 42% of all cybercrime attacks during the quarter, up from 13% the previous quarter, according to Outseer data.[7]

Rogue Mobile App Cyber Attacks



Source: Outseer

NEXT Get Ahead of Spoofed Websites

Monitor authorized and unauthorized app stores for software abusing your brand. Work with app stores to ensure your organization is part of the vetting process for apps leveraging your brand name.

In Q1 2019, Outseer detected

41,313

rogue mobile apps,

a 300% increase from Q4 2018.

In Q2 2019, the number of **rogue mobile apps uncovered** across popular app stores over the same time the prior year.

GREW **191%**

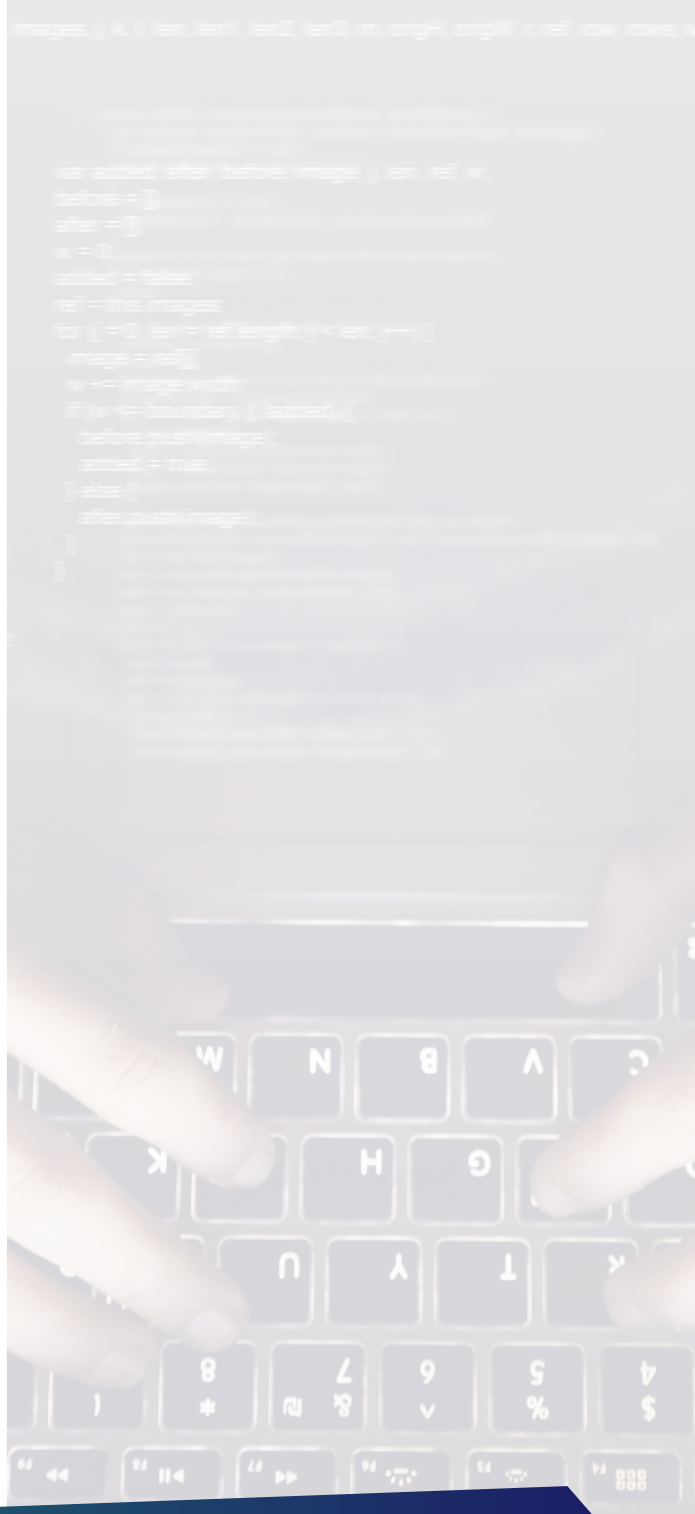
In Q4 2019, the number of **rogue mobile apps uncovered** across popular app stores over the same time the prior year.

GREW **175%**

Get Ahead of Spoofed Websites

Spoofed websites are one of the oldest cybercrime tricks in the book. But they remain one of the most effective. By exploiting consumer trust in legitimate brands, these sites fool users into forking over sensitive personal information or downloading malware. In 2020, Outseer FraudAction took down over 82 thousand spoofed websites.

To prevent spoofing, work with registrars or DNS providers to alert you to newly-registered domains similar to yours. Also watch out for websites that give out SSL certificates to subdomains resembling your brand's. It can be a sign cybercriminals may be planning to set up spoofed websites. Work with registrars or DNS providers to take down those domains and subdomains before they become malicious websites.



NEXT The Many Faces of Phishing

The Many Faces of Phishing

Phishing remains the most popular attack technique for cybercriminals. You'll want to monitor for all forms of phishing, including newer forms, such as smishing, vishing and reverse vishing.

Smishing, the use of SMS text messages to steal personal information, skyrocketed in 2020 with COVID-19 related scams. The Centers for Disease Control. The World Health Organization. The Internal Revenue Service. These and many other organizations were impersonated in text-messaging scams that preyed on economic and health anxieties and linked to malicious sites.

Vishing is also on the rise. In these schemes, urgent voicemail messages hoodwink consumers into calling a counterfeit phone number to pay a "past-due invoice." To do this, cybercriminals are increasingly using voice over internet protocol (VoIP) technology to spoof caller IDs and identities.

Then there's reverse vishing. This involves replacing legitimate phone numbers for businesses that appear in search results with numbers that go to scammers. Within just the first week of 2021, two very well-known consumer brands fell prey to reverse vishing. It's a sign that we're about to see a lot more of this form of impersonation.

Stay vigilant for all forms of phishing that either exploit your brand or target your customers, employees, and business partners.

NEXT Protect the Brand, Take Down the Bad Guys

Protect the Brand, Take Down Bad Guys

You've now seen five of the most popular attack techniques for perpetrating impersonation attacks. To mitigate the impact to your brand and bottom line, initiate a takedown as soon as you've verified it. Takedown involves the following:

DETECTION → QUALIFICATION → BLOCKING → TAKEDOWN → FORENSICS

1. Analyze the attack to identify all the authorities unwittingly caught up in it. This includes ISPs, web hosting providers, DNS providers, registrars, registrants, hijacked website owners, and more.

2. Contact these authorities to make them aware of the attack and to get them to cooperate in takedown. You may need to follow up with them until the takedown is complete. If you can communicate in their native language, you will develop stronger relationships and see faster response and resolution times.

3. Contact the local CERT or cyber police to make them aware of the attack and initiate legal action. Here again, speaking law enforcement's native language will be an asset.

4. Identify every resource involved in the attack, such as redirections, frames or drop points, so you can ensure these resources get dismantled as part of the takedown.

Initiate takedown as soon as you detect fraudulent activity to minimize financial and reputational harm.

NEXT Outseer FraudAction™ Can Help Protect Your Brand

Outseer FraudAction™ Can Help Protect Your Brand

Protect your brand and your customers 24/7 with our fraud intelligence and cyberattack takedown service. Outseer FraudAction keeps your business safe from fraudulent websites, mobile apps, and social media pages used in cyberattacks that target or impersonate your executives or your brand. Through data science, human expertise, and a wide ecosystem of more than 16,000 partners worldwide, we help recognize and shut down attacks before they can do damage.

Rapid Detection, Swift Takedown

By seeing what others can't, Outseer FraudAction protects thousands of brands, including many Fortune 500 companies, from impersonation and more. The results speak for themselves.

2 million+
Successful cyberattack shutdowns, across phishing and malware sites, rogue mobile apps, and executive or brand social media threats

68 million
URLs scanned daily, including newly-registered domains, in search of lookalike phishing and malware sites impersonating your brand

10,000+
Takedowns per month, across the web, social media platforms, and app stores—as well as thousands of pre-empted attacks achieved by monitoring registered SSL certificates

30 minutes
Average time to detect, investigate, and report cyberattacks for takedown

6 hours
Median takedown time for phishing and malware sites of under six hours

1 million+
Compromised credit card and login credentials recovered and reported each month

Source: Outseer FraudAction team

1. Outseer Quarterly Fraud Reports: Q1 2020, Q2 2020, Q3 2020
2. Tom Champion, "How to Build Customer Trust Faster," Forrester, June 12, 2017
3. U.S. Department of Commerce https://www2.census.gov/retail/releases/historical/ecomm/20q2.pdf
4. Lightico, Covid-19 Survey: Consumers Demand a New Digital Banking Normal, https://info.lightico.com/banking-covid-19-survey-may-pdf-page
5. BBC News, "Fake Elon Musk scam spreads after accounts hacked," November 5, 2018.
6. Coren, Michael J. "A verified Twitter account impersonating Elon Musk collected over $150,000" Quartz, November 5, 2018.
7. Outseer Quarterly Fraud Report: Volume 3, Issue 3, Q3 2020

About Outseer

Outseer empowers the digital economy to grow by authenticating billions of transactions annually. Our payment and account monitoring solutions increase revenue and reduce customer friction for card issuing banks, payment processors, and merchants worldwide.

Leveraging 20 billion annual transactions from 6,000 global institutions contributing to the Outseer Data Network, our identity-based science delivers the highest fraud detection rates and lowest customer intervention in the industry. See what others can't at outseer.com