The Untold Cost of Brand Impersonation

MEMCYCO

A guide for protecting your brand against impersonation attacks

Every interaction between an organization and its end users revolves around trust. Especially as interactions move online, 70%-80% of a brand's market value now comes from intangible assets such as goodwill . But as brands try to establish their reputation and connect with customers digitally, attackers capitalize on the trust they've built. In this ebook, we discuss the danger of brand impersonation and methods for protecting your brand from it––some of them may sound familiar, but we propose innovative ways to get past the limitations of traditional security tools.

On a global scale, brand impersonation (also known as brand abuse or brandjacking) is associated with almost half of all cyberattacks. Brand impersonation fraud exploded by 274% in Q3 2021 compared to the previous year's period.

With nearly one in seven cyberattacks now involving fake brand websites, how can we expect customers to want to interact with us online?

Brand's market value

Cyberattacks

50%

Brand impersonation

MEMCYCO

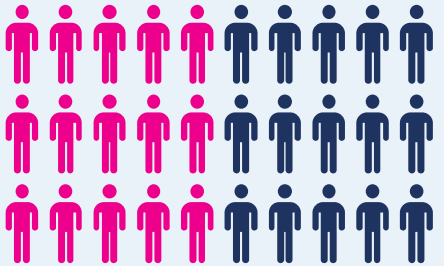
What Is Brand Impersonation?

Brand Impersonation is a cybercrime that sees attackers using a variety of tactics to mimic well-known brands. This is done to:

- trick victims into engaging with malicious platforms the attacker built to collect credentials
- steal sensitive data
- engage in fraud
- install malware

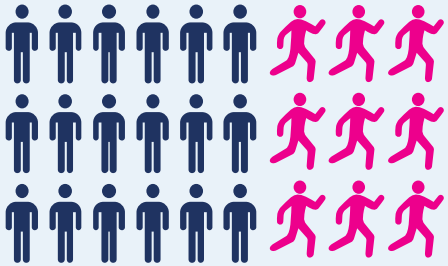
Studies show that 49% **of consumers purchase from a company because they trust it**, and attackers don't hold back from praying on that trust. But falling victim to a scam associated with your brand's name may erode that confidence: 44% **of customers have stopped transacting with a company due to a lack of trust resulting from brand impersonation.**

consumers purchase from a company



49%

Trust



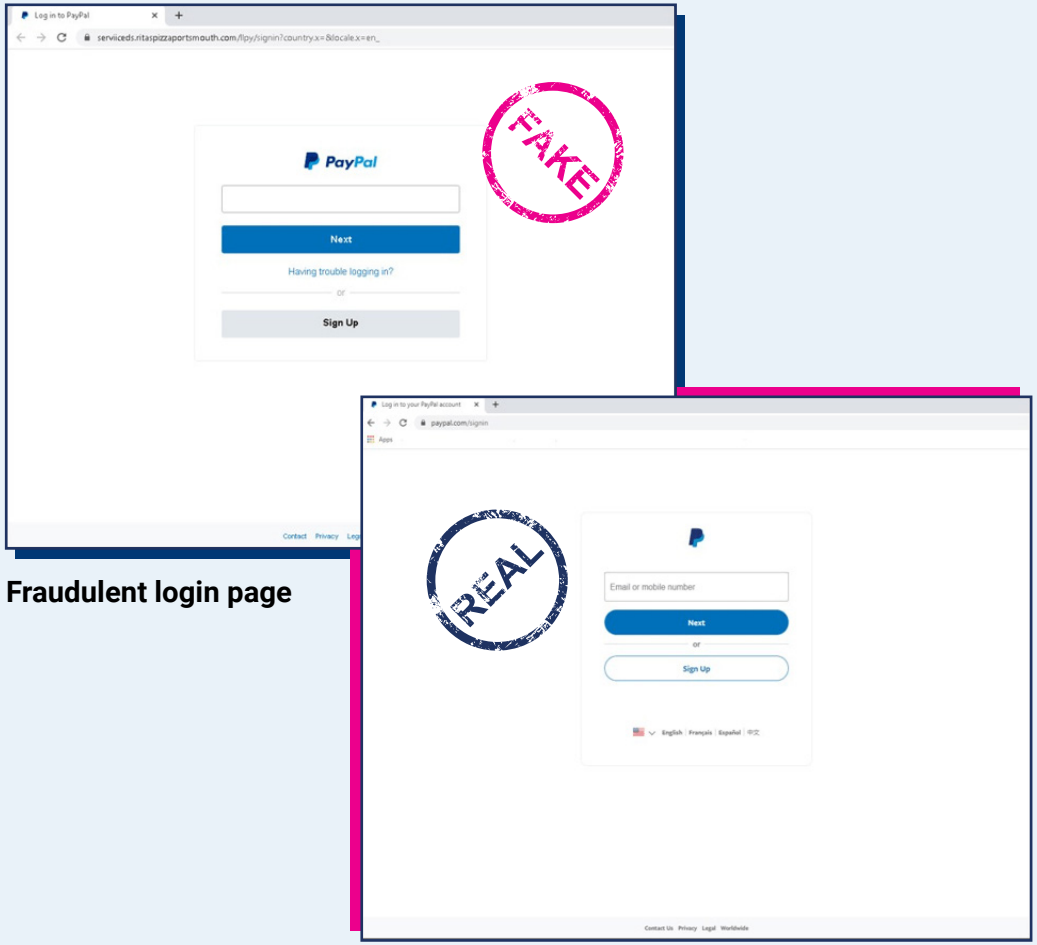
44%

stopped transacting with a company due to a lack of trust

MEMCYCO

How Does Brand Impersonation Look?

To impersonate an organization or one of its employees, attackers spoof a company's email domain or website that may look almost identical to the original ones, lending legitimacy to fake communications with its customers. Spoofed websites and email communications copy a brand's genuine colors, images, and code to trick victims into believing it is legitimate and push them for urgent action to get users to click on manipulated links. In many cases, users don't know they are being scammed even after clicking on malicious links because the customer journey is fake from start to finish. This is known as brand hijacking or brandjacking, in short.



Fraudulent login page

Real login page

MEMCYCO

Another broad category of brand impersonation attacks is service impersonation. To execute it, the scammer imitates a well-known organization or commonly-used business application and targets specific individuals, say, an employee inside another company, who is used as an entry point for account takeovers. This is often used to steal sensitive corporate information.

Other methods of brand impersonation can look like this:

- Fake social media accounts that send victims to malicious websites
- Fake job advertisements that impersonate legitimate companies on job sites
- Search ad phishing, which is when spoofed versions of legitimate domains appear in search engine results
- Vishing, or voice phishing, is when malefactors use phone calls or voicemails to pose as institutions, such as your bank, to get you to share personal and financial details.
- Smishing, short for SMS phishing, is similar to vishing, but the attack is conducted via text messages to convince you to open malicious links.

How Fraudsters Exploit Your Brand

Most fraud attacks rely on two techniques to exploit victims: There's the "lure," which is how attackers get in touch with the victim to trick them into engagement, and there's the attack platform, where victims are lured into so an action can take place to the benefit of the attacker.

The lure may take many shapes, from an email or social media post to a fake mobile app or SMS. The attack platform is often an impersonation platform where fraudsters convince victims to perform actions so they can steal credentials and data and commit fraud. These platforms must look very convincing. To that end, attackers may spoof or clone them (the most accessible approach for the attacker) or build them from scratch (attempting as much as possible to create pages similar to the brand's authentic website). Fraudsters may put these fake sites up on a registered domain or insert the website into someone else's domain–whatever it takes to get victims to engage with them without the means to discern the authentic from the fake. What's more: attackers will go through the trouble of registering their domain to make their fake websites seem credible, which means scans for suspicious domains won't catch them.

Attackers may also exploit vulnerabilities in pre-existing websites to create brand impersonation attacks. The culprit will find and investigate a website that is vulnerable (say, a wordpress website) where to insert its own page. This way, by being infiltrated without the owner's knowledge, a seemingly trusted website can also be used to create a fake domain.

Below, we look in more detail at some examples of how these two techniques come to life:

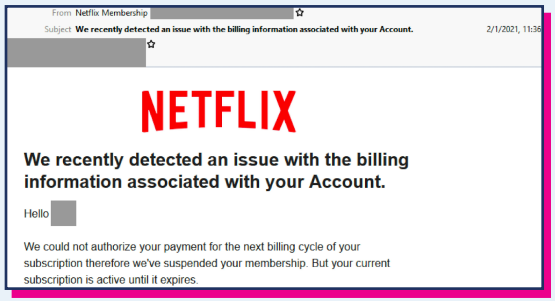
1. Social Media Platforms

Fraudsters use social media to make fake accounts impersonating your brand or employees to distribute malicious links. Hackers can also use social media to sell stolen credit card information, credentials, and other private information. It's essential to monitor social media platforms to ensure your company's data isn't being sold on a fraud forum.

2. Email

Cybercriminals impersonate brands through email to steal credentials or other sensitive information from victims, which they can use in future scams. By posing as a recognizable brand familiar to the recipient, attackers trick victims into clicking on a link to a fake URL or downloading an attachment that can lead to multiple adverse outcomes. These outcomes include personal data theft (such as name, address, and document numbers), credential theft (such as usernames and passwords), financial theft (such as stealing account numbers and credit card details), and malware or ransomware infection.

Generally speaking, attackers are playing a numbers game regarding brand impersonation via email: they may send generic emails to a wide range of individuals and hope that someone will fall for the bait.



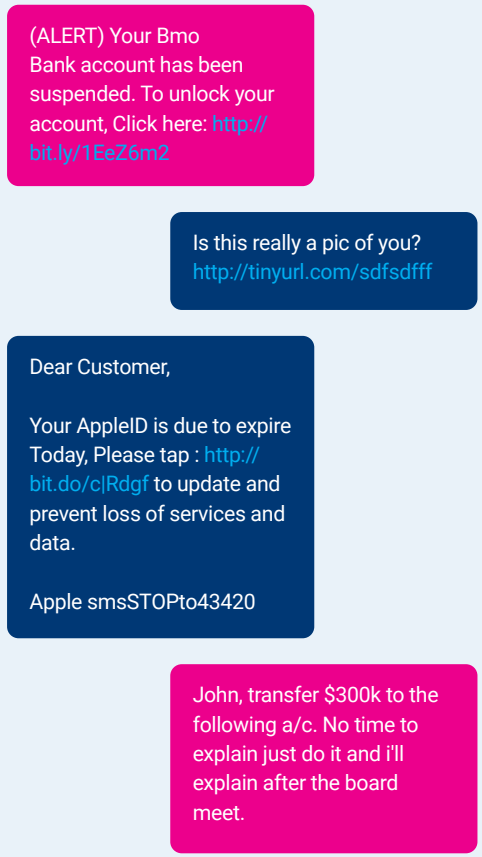
3. Text messages (SMS)

Also known as smishing (a term combining “SMS” and “phishing”), this variant of social engineering attack is carried out over mobile text messaging and relies on exploiting human trust rather than technical exploits. Victims are deceived into giving sensitive information to a disguised attacker, which they can use to commit fraud or other cybercrimes. Smishing occurs on many mobile text messaging platforms, including non-SMS channels like data-based mobile messaging apps.

These text messages often impersonate a business familiar to the victim or even the victim’s bank, asking for their personal or financial information, such as an account number. Providing the data is equivalent to handing over the keys to your bank balance. One way to protect yourself against these attacks is not to respond or engage with the text prompts, such as by clicking on links or downloading files (which is how attackers install malware on the victim’s phone).

Even if a message conveys a sense of urgency, take your time to verify its authenticity by calling your bank or merchant directly. Legitimate institutions don’t request account updates or login information via text, and you can ascertain urgent notices on your online account or via an official phone helpline.

More effectively, brands can help customers verify their texts’ legitimacy by adopting Memcyco’s Proof of Source Authenticity (PoSA): a digital watermark on authorized websites that helps users identify whether the page they are visiting is authentic and safe.



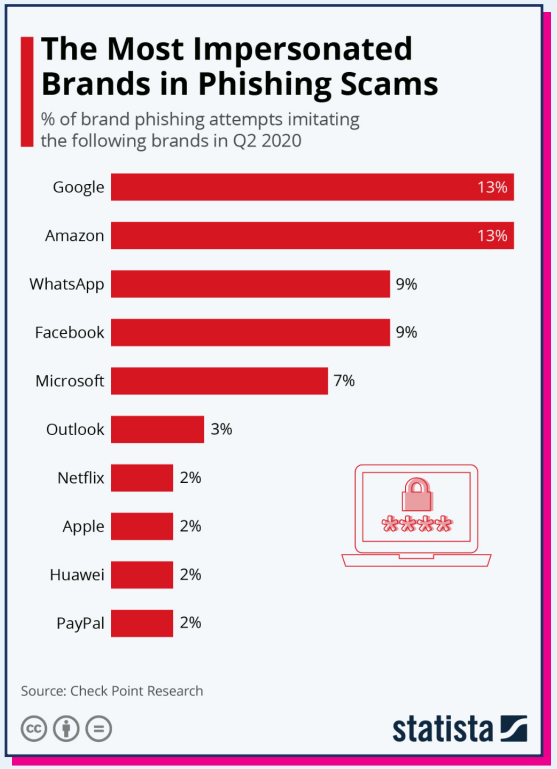
In addition, PoSA can embed a warning on cloned websites that pretend to be yours. This way, even if a user clicks on a malicious link in a smishing text message, PoSA will notify them that the page they see is fake and unsafe.

4. Impersonating Your Executives

Using platforms like Facebook, Twitter, and LinkedIn, hackers post as one or more of your executives and direct readers to malicious links. For example, when Elon Musk's Twitter account was hacked in 2021, hackers made posts encouraging followers to deposit bitcoin into an anonymous account. Despite the hack being shut down quickly, the hackers still made $150,000 worth of bitcoin.

5. Business Email Compromise (BEC)

BEC attacks refer to scammers impersonating senior executives while sending phishing emails to employees, customers, business partners, and suppliers. BEC attacks cause immense damage to the reputations of the brand and the executives being impersonated. In 2021, BEC attacks caused $2.4 billion in losses in the US alone. Additionally, these attacks often lead to fraudulent wire transfers and expensive data breaches that can lead to regulatory fines.



What Brand Impersonation Can Cost You

Brand impersonation costs not just the amount of money fraudulently transferred or stolen from victims, and the damage does not end once the attack ceases. The untold cost of these attacks can be seen in multiple areas, including:

Loss of Customer Trust

Brand impersonation attacks can leave customers unsure if your company can be trusted in the future, which means they are more likely to stop interacting with you digitally. And that goes for all customers, not just those who fell victim to a scam since these incidents are often made public and discussed in the customer community. In many cases your scammed customers, and other customers in their ecosystem, will stop engaging with you without you knowing about it or understanding why, since they did not contact you to complain, but rather felt unsafe to interact with you.

Reputational Damage

Even though your company is also a victim, customers are likely to blame you for their losses if they disclosed private information or had money stolen on a website that impersonates your own. The association between their terrible experience and your brand's name is hard to erase. And when social media rants and reviews abound, it could damage your company's reputation before you're even aware of the attack in question!

Lost customer trust and heightened customer suspicion can affect a company's revenue **by 10%-25%** in a single year.

Leaders in digital trust are more likely to see revenue and EBIT growth of **at least 10 percent annually.**

Sales Losses

Search ad phishing attacks can cause a drop in sales: If customers search for your website and a spoofed version comes up, they may purchase from them instead. In this case, not only have the funds gone astray but also the negative experience customers have can damage your brand even further, as we've seen in the previous point. What's more: these customers may never come back. And other customers who've heard about this incident may avoid coming back too. After all, if customers can't trust that your website is yours and that their data and payment information are safe with you, they won't feel comfortable purchasing from you.

A Decline in Marketing Leads

Aside from the potential of losing existing customers, impersonating attacks also make it difficult for brands to acquire new ones. That's because your marketing campaigns will be less effective as customers lose trust in web links and marketing materials. If they were victims of a data breach in the past, or you warn them of an attempted brand impersonation, they will be less likely to respond or engage with your marketing campaigns out of fear of being scammed. Consider that marketing campaigns rely on an immediate positive reaction (we're talking milliseconds) that drives a customer to purchase. If target customers start contemplating whether the campaign is genuine or a scam, businesses are at risk of losing them at the blink of an eye.

In addition to these concerns, brand impersonation is damaging from a cybersecurity perspective because hackers are often looking to commit personal data theft, credential theft, financial theft, or install malware on your network.

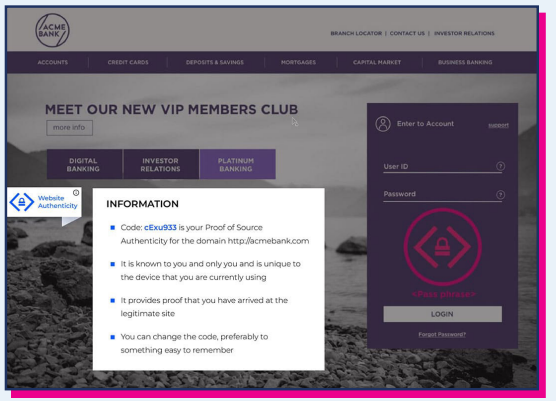
What You Can Do to Protect Your Brand from Fraudsters

Maintaining consistent communication with customers is vital to protect your company as it builds trust and shows them how your legitimate communications look. While these approaches can help, matching them with a proactive security measure will save you time, money, and stress. That's where we come in.

Building an Online Presence Without Fear

Memcyco's solution can help you get ahead of brand impersonation attacks with a Proof of Source Authenticity (PoSA). While many solutions allow companies to authenticate their users better, the customer side has been neglected. Brands rarely (if at all) make any effort to prove the authenticity of their websites to clients.

How can users verify companies' web presence? Currently, the only real effort to address this question of website authenticity is the website's certificate, shown as the little lock in the browser next to the URL. But it is almost invisible to the human eye and provides no proof that the user communicates with who they intended. For example, phishing websites hosted on Google Pages will appear safe to the end user as Google Pages have a valid website certificate.



PoSA provides visible, strong, and secure proof of website authenticity so that customers can verify the legitimacy and safety of the company web page they're visiting. This entails real-time monitoring that alerts your security team to potential attempts to use your brand for fake or unauthorized sites before reaching your end users. By preventing domain spoofing attacks, both your brand and customers are protected.

Memcyco's memorable and user-friendly PoSA watermark informs customers that the website or communications they see are authentic so they can feel confident interacting with your brand. Our solution applies a similar approach and has equal significance to watermarks on currency bills. There's a fundamental difference: our PoSA watermark can include a text code and visual elements unique to the specific user, much like a personal paraphrase, that they can set themselves.

The PoSA brand impersonation prevention suite is easy to install with just a single line of code on your website. It requires no end user-education, downloads, or installation. Moreover, PoSA features granular impact reports that help risk and fraud teams pinpoint potential victims of brand fraud and mitigate damages on brand and customer levels.

You've worked hard to build your brand. Now let Memcyco help protect what you've built so that you can focus on growth. Learn more and get started here.