mimecast®

The State of Brand Protection 2021

A new front opens up in the war for brand safety

Executive Summary: 2020 Transforms the Brand Protection Landscape

Marketers aim to use the right message to reach the right customer at the right time. That's exactly what cybercriminals do, too — except they're stealing *your* brand to sell *their* "product."

In 2020, cybercriminals exploited the world's fear and uncertainty about COVID-19 to dramatically escalate email phishing campaigns and other malicious attacks that impersonate brands in order to trade on those brands' customer trust. Based on Mimecast's threat intelligence monitoring:

- The number of brand impersonation emails per month detected en route to Mimecast customers **rose 44% in 2020 over 2019 to an average of nearly 27 million.***
- Companies on the *BrandZ™ Top 100 Most Valuable Global Brands 2020* list experienced a **381% spike in brand impersonation attacks during the two months of May and June 2020 over January-February** (before the pandemic hit).
- New domains suspected of brand impersonation also spiked, up **366% in May-June 2020**.
- And the unfortunate result: Monthly unwitting clicks on dangerous links soared **84.5% over the course of the year**.

Corroborating these findings, 76% of *Mimecast State of Email Security 2021 (SOES 2021)* respondents reported that, during 2020, they had identified or been made aware of at least one web or email spoofing attack using their domains or lookalike domains; 25% said they identified more than 10. And that's only what they knew about. In the customer interviews for this report, we heard multiple stories about how surprised marketers and cybersecurity professionals were when they began proactively monitoring for impersonation and discovered just how much their brands were really being exploited.

The challenge, as Deloitte points out in its *2020 Global Marketing Trends* report, is this: Companies that fail to safeguard customer trust in digital environments will likely face existential threats to customer loyalty and the market value of their brands.[1]

Key Findings.

Every clickthrough from a faked email to a spoofed web page can steal away a marketer's lead.

.01 All brands are at risk.

Big or small, B2C or B2B, if your brand has an online presence, it's at risk. Retail scams, business email compromise, supply chain impersonation, and money mule recruitment campaigns are just a few of the types of brand exploitation attacks interviewees reported. Technology and finance companies were the most impersonated brands in our analysis of the top 100 most valuable brands, followed by telecoms, shipping, retail, entertainment, and transportation companies.

.02 Brands don't realize the extent of the problem.

Marketers, stakeholders, and even cybersecurity experts often don't realize the full extent to which their brand is being exploited until they begin proactively monitoring for it — which is still rare. Two small banks, one in the U.S. and another in the UK, told us of their surprise over averaging 10 to 15 brand impersonation "takedowns" per month once they became proactive.

.03 Brands are losing trust — and leads — to cybercriminals.

As harmful as lost trust can be to a brand's reputation (Frost & Sullivan research shows 48% of survey respondents stopped using an online service when it had a data breach[2]), marketers may feel lost leads are a far more tangible pain point. Every clickthrough from a faked email to a spoofed web page can steal away a marketer's lead.

.04 Marketers and security teams must work together.

Traditionally siloed, these business departments must tag-team in order to achieve brand safety. Cybersecurity professionals can't always tell legitimate uses of the brand from the bad actors, and marketers can't get visibility into the extent of the problem without their IT security partners. One IT professional told us about launching a brand impersonation monitoring program just to open marketers' eyes to the problem and build a collaborative bridge between their team and his.

.05 Fast attack takedown is vital — but hard to achieve.

Companies can have spoofed web domains taken down but doing so can be challenging. Even with an in-house brand protection strategy, manual takedowns can be costly and time consuming — if you can get them taken down at all.

.06 Brand monitoring/protection services are a must.

Services that provide monitoring to identify brand impersonation, including the Domain-based Message Authentication, Reporting and Conformance (DMARC) email protocol, are a must for online brand safety. First, they shed light on the severity of the issue, which differs for every brand. Then brand protection services can help brands mitigate the problem and more rapidly take down brand impersonation websites than most organizations can do on their own.

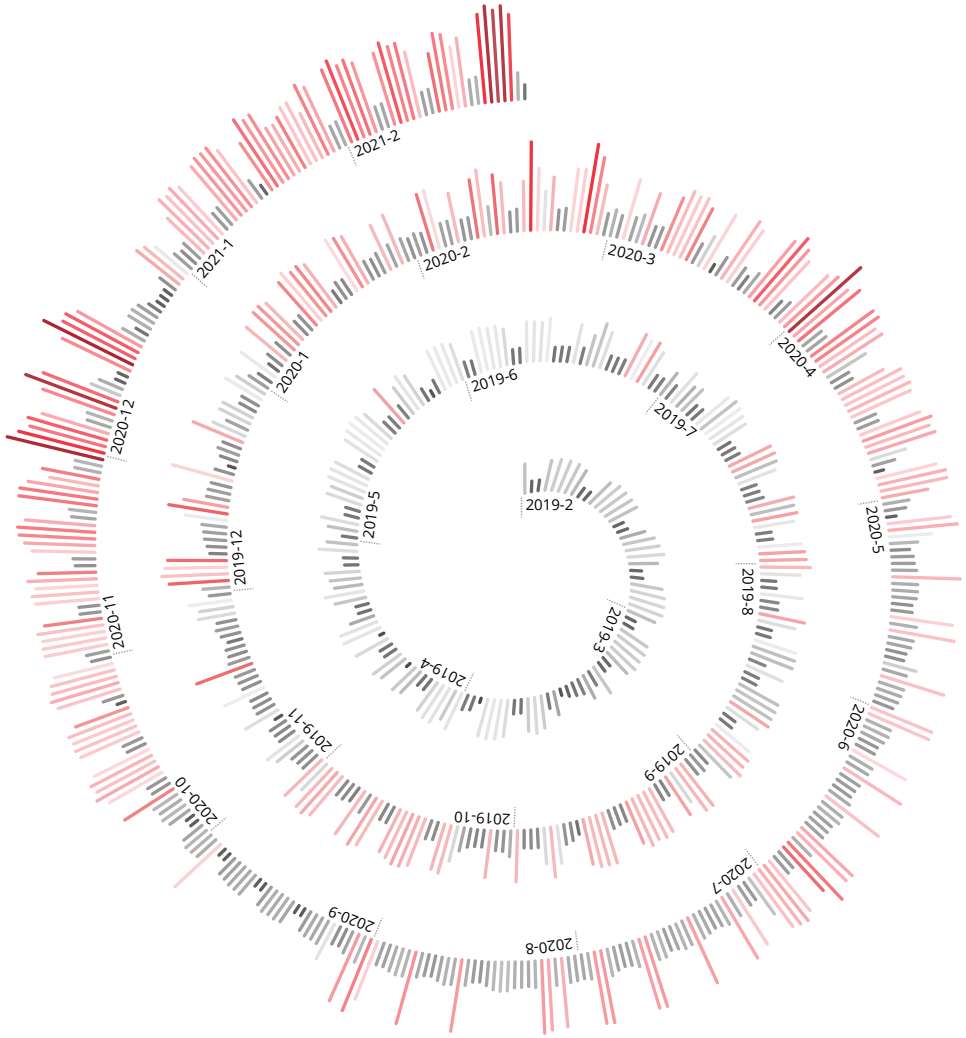
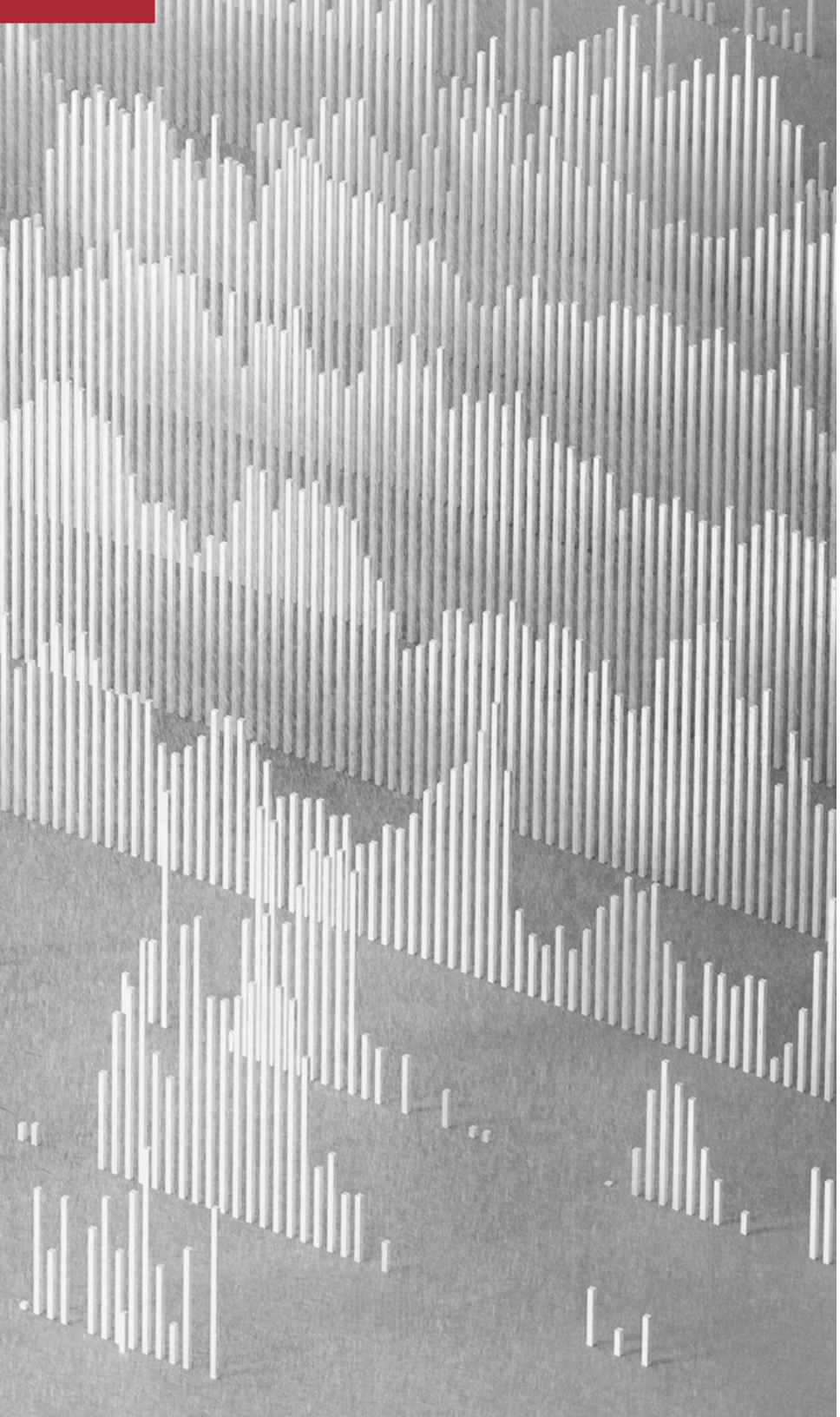


Figure 1: Daily Email Impersonations from Mimecast data, Feb. 2019-Feb. 2021

In this spiral graph of daily email brand impersonation attacks, grey and light grey lines denote days of light brand impersonations and red and dark red indicate heavy attack days. Note the increases in brand impersonation attack intensity in April and then November-December of 2020, and again in February 2021.



Report Methodology

The data in this report is derived from analysis of more than a billion emails per day monitored by Mimecast on behalf of its 40,000+ global customer organizations and compiled by the Mimecast Threat Intelligence Center.

In addition, from November 2020 through February 2021, report authors interviewed 10 cybersecurity professionals in organizations that used brand protection, DMARC services or both. The majority — but not all — were Mimecast customers.

Because there are millions of business organizations in the world, the actual number of global email phishing, brand impersonation, suspicious website domains and unsafe URL clicks will be many times the numbers described in this report. But the trends experienced by Mimecast customers likely reflect those in the world at large, and therefore should be considered illustrative.

State of Attack: Brands Don't See the Whole Problem

Brands today make heavy use of digital marketing technology to better engage with customers and prospects — largely through email. And for good reason:

Estimates of the return on investment (ROI) for email marketing are in the range of

$42 *for every* **$1** *spent.*[3]

But email has an inherent security flaw: Until recently, anyone could send email from your brand's domains — and 40% of consumers don't hesitate to click on links in emails from their favorite brands, according to new European brand trust research coming from Mimecast later this year.

40% **of consumers don't hesitate to click on links in emails from their favorite brands**

Anyone still can spoof a brand's domain in email unless the brand's security team puts relatively recent email authentication protocols in place, most notably DMARC. So, cybercriminals consistently impersonate brand likenesses and domains on the web to launch:

- B2C phishing attacks that aim to defraud customers or steal their credentials.
- Business email compromise attacks that use your CEO's and brand's likeness to trick employees into engaging with malicious content, potentially resulting in data breaches.
- B2B supply chain impersonation attacks that use your brand to communicate with vendors and suppliers, often with the intent of intercepting payments.

Brand impersonation online is all but invisible until you proactively look for it.

In **Mimecast's SOES 2021 report**, nearly half of respondents (47%) saw an increase in the volume of spoofed emails that misused their organization's brand during the past year, and 42% saw an increase in spoofed web domains that impersonated their brand. Many others may not be paying close enough attention to the problem. After all, while brand impersonation "in real life" is tangible — counterfeit goods, trademarks and copyrights are obvious to brand marketers — brand impersonation online is all but invisible until you proactively look for it.

Email phishing, though, is only part of the equation. Cyberattackers can use any digital touchpoint to exploit the brand-stakeholder relationship and conduct fraud, drop malware, harvest credentials or plant the seeds for data breaches and ransomware attacks. Beyond email, this includes web domains, social media, mobile apps and more — in fact, 55% of consumers have landed on a spoofed website from search and 52% from social media in Northern Europe alone. Attackers even use encryption to fool victims into thinking they're accessing a "secure" webpage.

By the fourth quarter of 2020, about 84% of email phishing attacks clicked through to malicious websites that were "protected" by the HTTPS encryption protocol, up from only 10% in the first quarter of 2017, according to the Anti-Phishing Working Group (APWG), an international consortium of more than 1,700 companies.[4]

47%

saw an increase in the volume of spoofed emails that misused their organization's brand

42%

saw an increase in spoofed web domains that impersonated their brand

55%

have landed on a spoofed website from search

52%

have landed on a spoofed website from social media in Northern Europe alone

The Many Ways Cybercriminals Exploit Your Brand

Link Manipulation

What it is

Cybercriminals register domains with names very similar to legitimate brand web pages. These manipulated links can direct users to fake websites that host malicious content.

What it can look like

Typosquatting, which relies on the likelihood a user makes a typo or similar error when entering a URL into their web browser ("miemcast.com" instead of "mimecast.com")

Internationalized Domain Names (IDNs), which use international characters in place of English characters, such as the Latin character "ɱ" instead of "m."

Top level domain (TLD) abuse, which takes a legitimate domain name and uses the wrong TLD, such as ".ca" or ".jp" instead of ".com".

Website Spoofing

What it is

Cybercriminals build spoofed websites that look like legitimate brand sites. Users are usually directed via manipulated links.

What it can look like

Phony websites with colors, images, and coding directly copied from a real brand's website. These fake sites can look surprisingly real and easily trick unsuspecting users into accidentally downloading malware or entering their personal credentials into a login portal.

Supply Chain Impersonation

What it is

Cybercriminals pretend to be a legitimate brand and inject themselves into the supply chain process, usually via email.

What it can look like

Bad actors generally try to intercept real payments to vendors, or trick accounts payable employees into making duplicate or fake payments. An email appearing to come from a genuine vendor might urgently request payment for an “unpaid invoice”, with wire transfer information that directs funds into a criminal bank account.

Fake Job Ads

What it is

Cybercriminals post fake job posting posing as a legitimate company, either on job sites or search engine ads. They might also reach out directly to unsuspecting consumers.

What it can look like

In many **job offer scams**, the bad actor will post a job offer and require the victim to pay a sum in order to ”get hired” for a non-existent position.

In **money mule recruitment campaigns**, citizens might receive job offers, such as a basic payment processing position in which the unsuspecting person unknowingly launders money for fraudsters. The victim may not know they’re taking part in a money laundering scheme because the fraudsters are paying them a seemingly legitimate salary.

Social Media Impersonation

What it is

Cybercriminals create fake social media accounts using real brand names, making posts and commenting on messages to seem legitimate.

What it can look like

Posts or comments might include malicious links that direct unsuspecting victims to malicious websites.

In other cases, impersonators may simply aim to embarrass a brand or tarnish its reputation.

Business Email Compromise

What it is

Cybercriminals use email spoofing tactics to send emails that appear to come from legitimate employees or business executives.

What it can look like

An email that appears to come from someone in a leadership position asking the recipient to click a link that leads to a spoofed website, or to download an attachment that drops malware.

Other times, an “executive” might ask the recipient to change wire transfer information for an otherwise legitimate payment, allowing the criminal to receive the funds instead.

Search Ad Phishing

What it is

Cybercriminals make their malicious webpages appear in search engine results, usually by spoofing a brand’s domain.

What it can look like

What appears to be a legitimate search advertisement for a retail brand offers users free or discounted goods. Instead, the link might take users to a cloned webpage that drops malware, harvests credentials, or tricks the user into making a fraudulent purchase.

Vishing & SMShing

What it is

Cybercriminals send out voice or text messages pretending to be a brand.

What it can look like

An employee might get a voicemail from someone pretending to be the CEO and asking to transfer funds into a certain bank account.

A consumer might receive a text message with a link to ”tracking information” from a well-known shipping company, but the link directs the user to a malicious webpage.

Further, brand exploitation can affect businesses of all sizes, in any industry. Online banking, for example, was among the most trusted industries in the European brand trust research, but it is paradoxically also one of the most targeted industries for brand impersonation and phishing attacks. For example, a CISO at a small UK bank told us he found — and took down — about 14 fraudulent websites a month for the past year. A similarly small regional U.S. bank reported averaging 10 or 11 fraudulent websites imitating the bank's brand every month. SaaS, webmail, social media, ecommerce, retail, logistics, shipping, and telecom companies are all also at high risk.[5]

According to data from the APWG, criminal phishing activity doubled in 2020.[6] Analysis of Mimecast's own Threat Intelligence data (Figure 2) gives that growth more context and shows how cyberattackers strike opportunistically — like marketers, waiting for the right moment and message. The steep growth from year-end 2019 through the late spring 2020 peak concentrated around the early months of the COVID-19 pandemic, when fear, uncertainty and doubt introduced new layers of vulnerability. Bad actors appeared to take a breather for a while before attacking with renewed vigor in the runup to the U.S. presidential election in November (the second peak). The falloff after the election peak, however, was much shorter as both January and February 2021 have topped that peak.

Overall, throughout the period covered by Figure 2, email brand impersonations detected by Mimecast rose to 39.2 million in February 2021 from 14.5 million in February 2019, which is a 170% increase — or 2.7 times higher. The monthly average for 2020 was 26.95 million, a 44% rise over 18.73 million in 2019.

Rising Monthly Email Impersonations

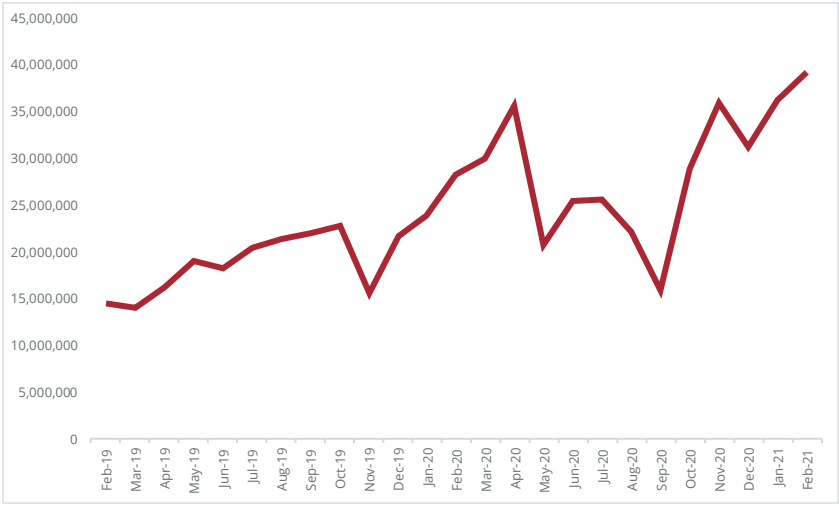


Figure 2: Rising Monthly Email Impersonations, 2/2019 – 2/2021

Cyberattackers strike opportunistically — like marketers, waiting for the right moment and message

Meanwhile, Figure 3 shows that the number of suspicious domains with live content impersonating brands that use Mimecast's Brand Exploit Protect service spiked 366% in May-June 2020 over January-February 2020 — 4.7 times the number in the first two months of the year, before the COVID-19 pandemic effect was felt. And while the number of new suspicious domains fell from that mid-2020 peak, they have remained at a "new normal" higher level: the last two months of 2020 saw 73% more suspicious domain registrations than the first two months of the year.

Figure 4 shows the unfortunate result. Rising brand impersonation attacks at moments when large portions of the world's population were most psychologically vulnerable led to a dramatic rise in user clicks on unsafe URLs delivered via email; in fact looking at Threat Intelligence Center data for Mimecast customers, unsafe clicks doubled (+99.8%) from January to May 2020. Again, there is a respite from May to September 2020 and then renewed growth so that January 2021 saw 8.1 million unsafe clicks, 84.5% higher than January 2020.

As one interviewee puts it, "the threat is ever-present yet seems to come and go." Said another: "In one month, we saw about 300,000 abusive emails were sent out pretending to be our brand. Some pretended to be part of our procurement process to either defraud us or someone else in our procurement chain. We've even had members of the public say they've been offered a job with our company, but it turns out the fake job offers are money mules, part of criminal money laundering campaigns."

Suspicious Domain Registrations, 2020

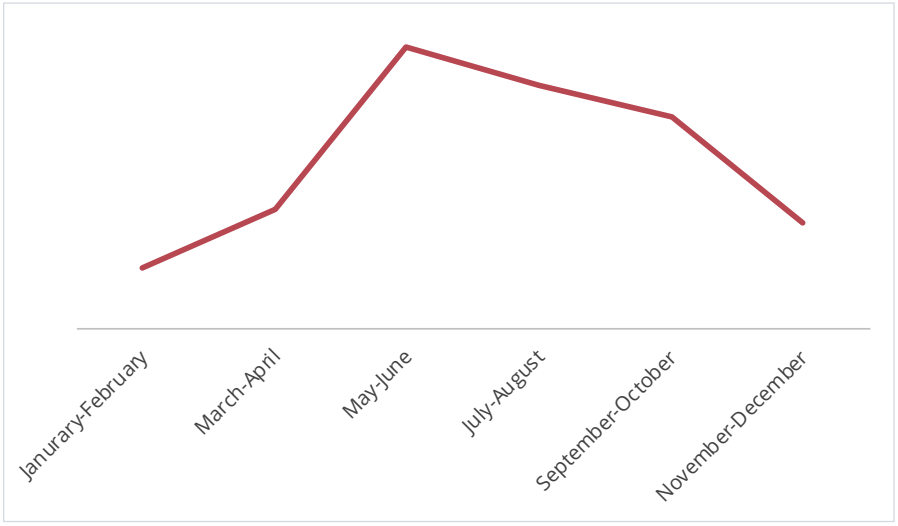


Figure 3: Suspicious Domain Registrations, 2020

Monthly Clicks on Unsafe URLs

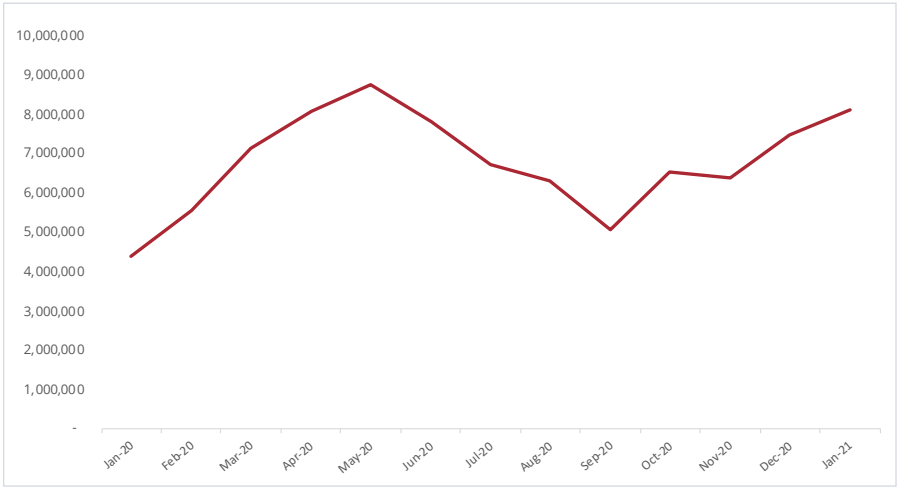


Figure 4: Monthly Clicks on Unsafe URLs, 1/20 – 1/21

The Bigger Your Brand, the Harder They Phish

While even relatively small companies can be victims of brand impersonation — especially if they have a website with a customer login — the larger the brand, the more potential value cybercriminals can siphon away. That's why it's critical to monitor brand impersonation attacks against the 100 companies on the *BrandZ™ Top 100 Most Valuable Global Brands 2020* list.

Since 2006, Kantar Group, the London-based data analytics and brand consulting company, has been calculating which 100 brands make the largest dollar-value contribution to the total value of their parent companies; it publishes the top 100 rankings annually. For 2020, Kantar determined that the aggregate value of those 100 brands — starting with Amazon and Apple at numbers one and two and ending with Pepsi and Commonwealth Bank at 99 and 100 — had reached $5 trillion. And that number represents just the value of the brands, not the companies' total market capitalizations.

The larger the brand, the more potential value cybercriminals can siphon away

Total number of attacks on top 100 brands

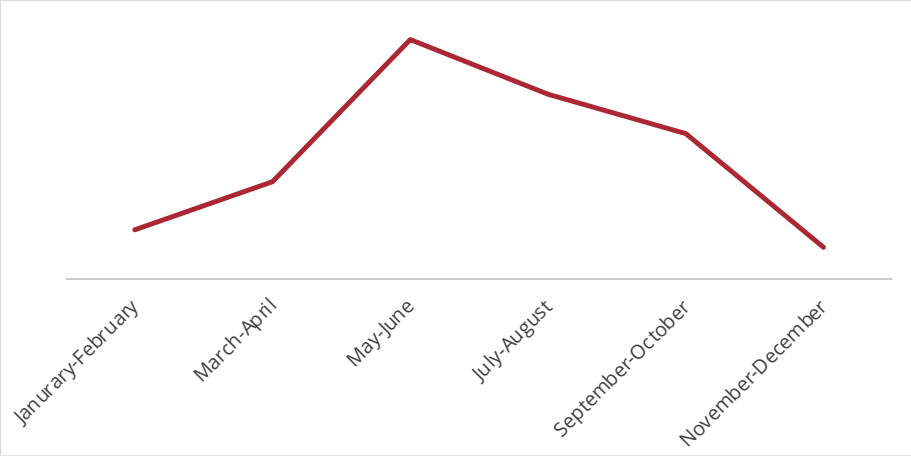


Figure 5: Attacks on Top 100 Most-Valuable Brands

Using Mimecast's Brand Exploit Protect (BEP) web-scanning tool, brand impersonation attacks against Kantar's top 100 brands rose and fell [Figure 5] in the same now-familiar 2020 trajectory: a 381% burst from the volume seen in January-February to the peak in May-June, followed by a gradual fall. In this case, however, there was no subsequent second rise.

20 most-impersonated of the top 100 global brands

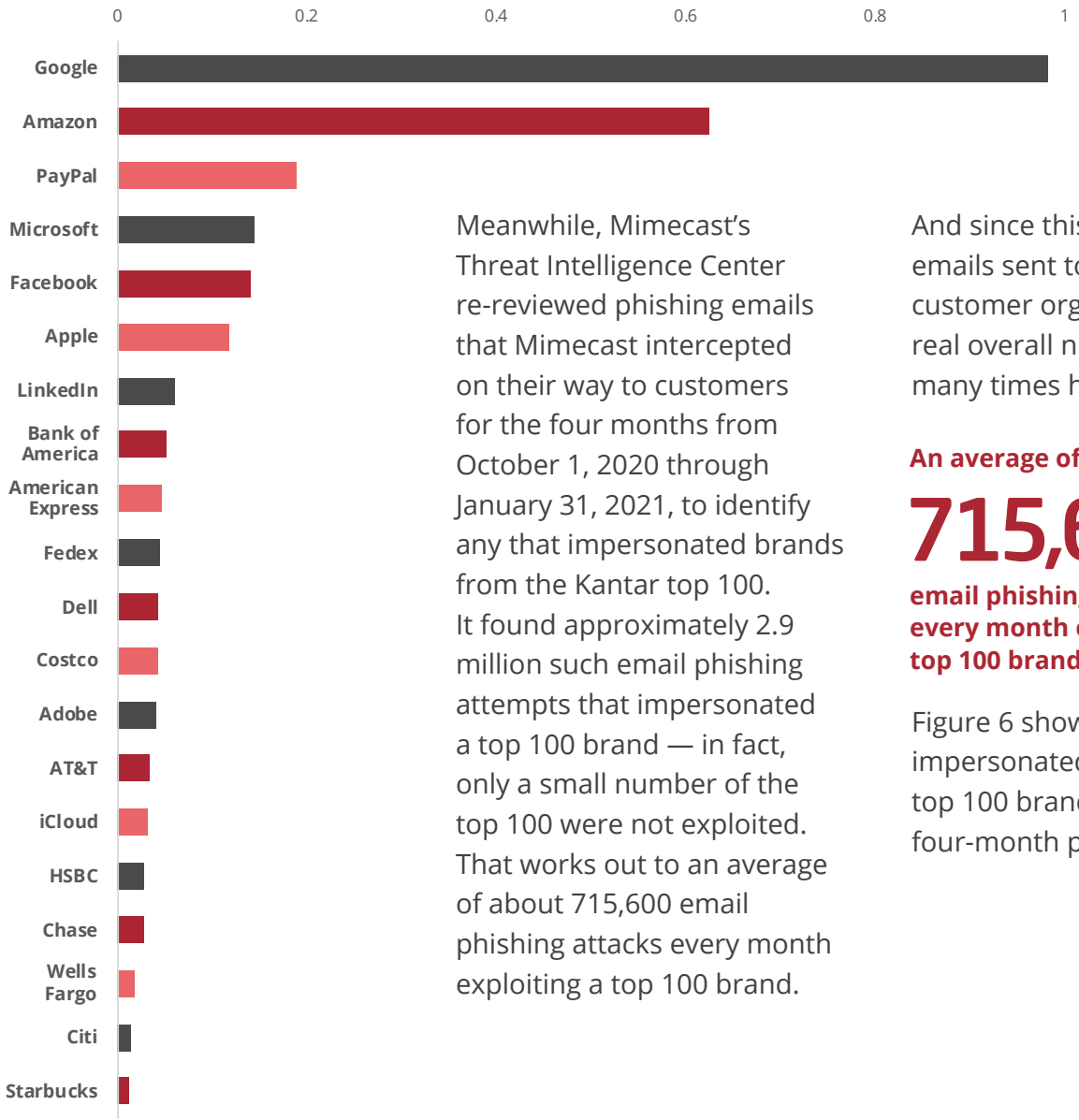


Figure 6: 20 most-impersonated of the top 100 brands during the four-month period, 10/1/20 – 1/31/21

Meanwhile, Mimecast's Threat Intelligence Center re-reviewed phishing emails that Mimecast intercepted on their way to customers for the four months from October 1, 2020 through January 31, 2021, to identify any that impersonated brands from the Kantar top 100. It found approximately 2.9 million such email phishing attempts that impersonated a top 100 brand — in fact, only a small number of the top 100 were not exploited. That works out to an average of about 715,600 email phishing attacks every month exploiting a top 100 brand.

And since this counts only emails sent to Mimecast customer organizations, the real overall number must be many times higher.

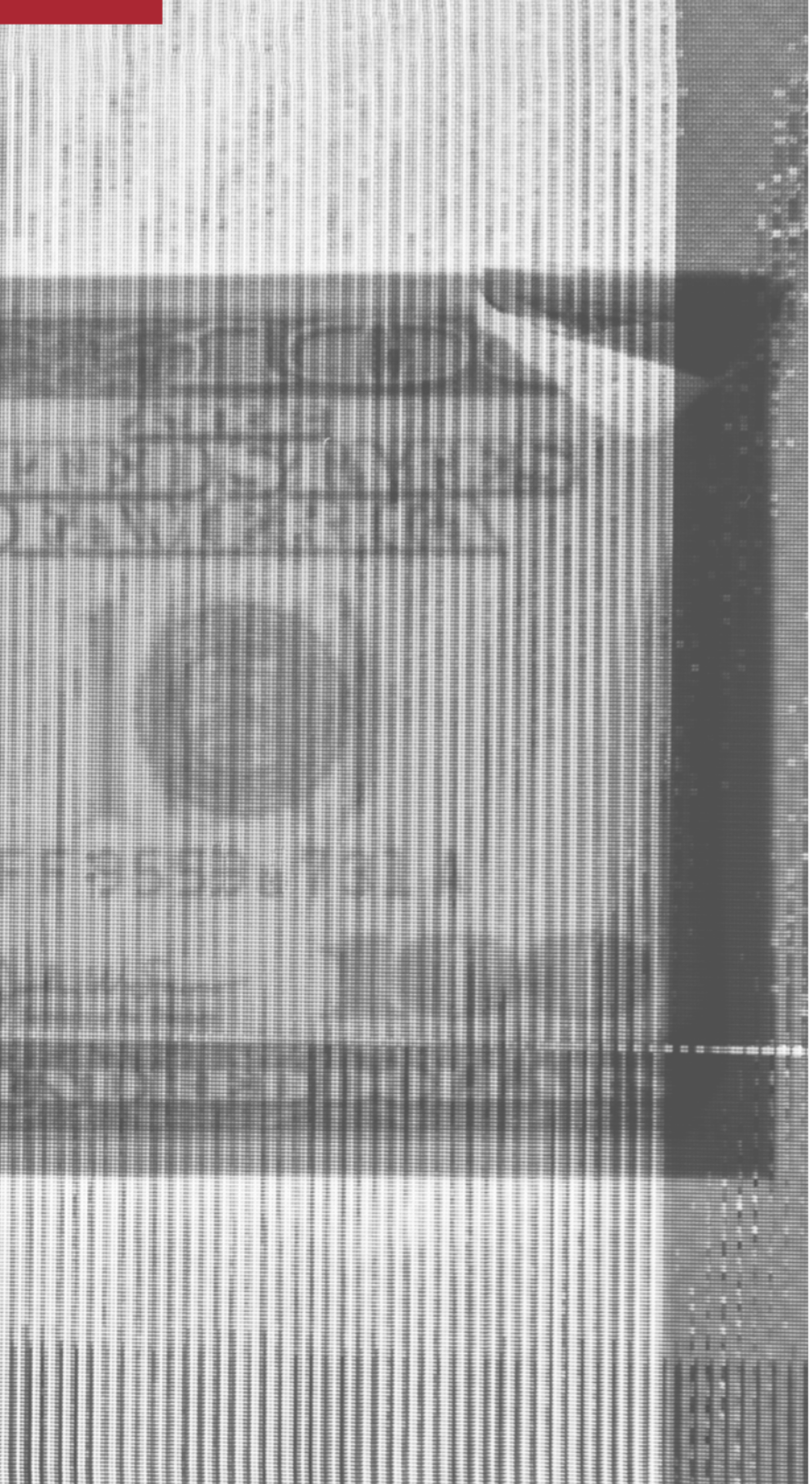
An average of

715,600

email phishing attacks every month exploited a top 100 brand

Figure 6 shows the 20 most-impersonated of the top 100 brands during the four-month period.

Of course, it's not just the biggest,most well-known companies that are susceptible to brand impersonation. Smaller organizations can also face the financial and reputational repercussions of brand exploitation. Worse, they're often less equipped to handle remediation than the larger, more well-known companies that fight to protect their brands on all fronts.



Understanding the financial and reputational repercussions

Brand impersonation is costly. According to the IC3 2019 *Internet Crime Report*, over $1.7 billion was lost in that year alone to impersonation via business email compromise and other phishing attacks.[7] And in the European brand trust research, 50% of consumers said they would stop spending money with their favorite brand, one they use regularly or one they're familiar with, if they fell victim to a phishing attack involving that brand. But brand impersonation is a complex, far-reaching issue with diverse outcomes. Every time a brand is exploited for a cyberattack, both the brand and its customers are at risk, each in a variety of ways.

Monetizing brand impersonation. Cybercriminals might exploit a brand to harvest customer credentials which they then sell on the black market or use to access the victim's personal email, work email or financial information. Ultimately, cybercriminals can then potentially takeover accounts, steal data, deploy malware or launch ransomware attacks. This means that not only are the recipients of impersonation attacks put in jeopardy, their organizations are, too. And all of these possible outcomes can stem from just one victim being tricked by one email impersonating a brand they know and trust.

$1.7 billion

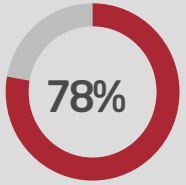
was lost in 2019 to impersonation via business email compromise and other phishing attacks

Legal fees and regulatory fines. Going a step further, an impersonated brand is likely to face clean-up costs and legal fees. In the infamous British Airways case, cybercriminals successfully diverted about 500,000 customers to a realistic but fraudulent website that gathered personal information like names, addresses, payment card details and login information. Although arguably itself a victim, the airline faced an initial General Data Protection Regulation (GDPR) fine of $230 million for not detecting and stopping the impersonation more quickly than it did (the fine was later lowered to $26 million).[8]

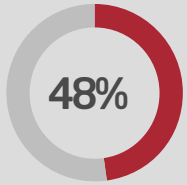
Reputational damage. Costly consequences of brand impersonation also include reputation loss and strained business relationships. Brand equity can be hard enough to build, and consumer trust is already declining thanks to the alarming rise in data breaches, according to Frost & Sullivan's *Global State of Online Digital Trust*. The report found the consumer digital trust index to be 61 out of 100, the equivalent of a failing grade.[9] What's more, 78% of consumers indicated that it's very important or crucial that their personal information be protected online, and 48% have stopped using an online service when it suffers a data breach. When customers are victims of brand impersonation attacks, they are likely to associate that unsettling experience with the brand — even though the brand itself was also a victim. This means they may be hesitant to click on links associated with the brand and avoid future legitimate email interactions, causing the brand's digital marketing ROI to fall. They might even lose an otherwise loyal lifetime customer.

As one Brand Exploit Protect customer told us: "Even if we aren't seeing any money loss from these brand exploitation attacks, our image is one of the main things we want to protect. We're taking the service on because we want to protect our image. If that helps the customer as well, then it's good for both of us."

The Frost & Sullivan report found the consumer digital trust index to be 61 out of 100, the equivalent of a failing grade.[9]



of consumers indicated that it's very important or crucial **that their personal information be protected online.**



have **stopped using an online service** when it suffers a data breach.

Falling Email ROI: Remember that incredible 42-to-1 email marketing ROI? It's not guaranteed, and the customer reaction Frost & Sullivan describes can lead directly to a decline in marketing leads, a rising cost-per-lead, or both. In addition, email spoofing can lead to email deliverability issues because internet service providers attempting to block brand impersonators are likely to also snare legitimate marketing organizations sending email on a brand's behalf. Meanwhile, web domain spoofing directs potential customers away from legitimate web pages. In just one example, cybercriminals can create imposter sites purporting to be a legitimate page that hosts ads.

Media buyers then unknowingly buy ads on the fake page thinking it's legitimate, allowing them to profit from the domains of reputable publishers. One test conducted by News UK found 2.9 billion ad bids per hour were made on fake sites posing as The Sun and The Times of London newspaper brands and estimated that marketers could be wasting up to $1,000,000 a month on domain-spoofed inventory.[10]

It is estimated that marketers could be wasting up to $1,000,000 a month on domain-spoofed inventory.[10]

2.9 billion

Ad bids per hour were made on fake sites posing as The Sun and The Times of London newspaper brands according to one test conducted by News UK

State of Defense: A Gap in Brand Safety

Despite the rapidly increasing virulence of brand impersonation cyberattacks and the growing list of potential consequences, many — if not most — small and midsize companies remain virtually oblivious to the danger threatening their brands. Ironically, brand marketers work closely with legal teams to guard their brands "in real life" and pay close attention to brand safety issues relating to advertising placement online but remain mostly unaware of how brand impersonation emails threaten brand safety. At the same time, some consumers remain unaware of the overall threat and are unsure what checks they should be carrying out to determine email and website legitimacy.

To combat brand impersonation, brand marketers must take stock of how cybercriminals are exploiting the numerous digital touchpoints marketers use to engage their customers.

As one interviewee aptly phrased it,

"If you have brand protection by way of trademark or copyright, you must consider online brand protection as part of the same strategy."

This is especially important, given that 75% of European consumers expect the brands they use regularly to ensure their website, email and communications services are safe to use, and that more than half consider it the brand's responsibility to protect itself from fake websites or emails.

The good news is that companies are growing more concerned about brand impersonation attacks. According to Mimecast's *SOES 2021*, 91% of respondents would be concerned if their organization experienced a fraudulent web domain or malicious website spoofing their domain, and 93% would be concerned about an email-based attack directly spoofing their email domains.

Though respondents are concerned, the volume of attacks is still increasing — throughout 2020, 73% of SOES respondents saw the same or an increasing volume of email spoofing that misused their brands, and 69% saw the same or an increasing volume of web domains that spoofed their brands.

From our customer interviews, there emerged a holistic five-part brand impersonation protection framework for brand marketers and cybersecurity professionals to implement together. We call it holistic because even though each part is useful in and of itself, all are interrelated and must be applied together to create highly effective online brand protection.

They are:

01.
Bridge the marketing and IT security siloes

02.
Use Proof of Concepts (PoCs) to extend brand protection awareness to all stakeholders

03.
Use third-party brand protection services

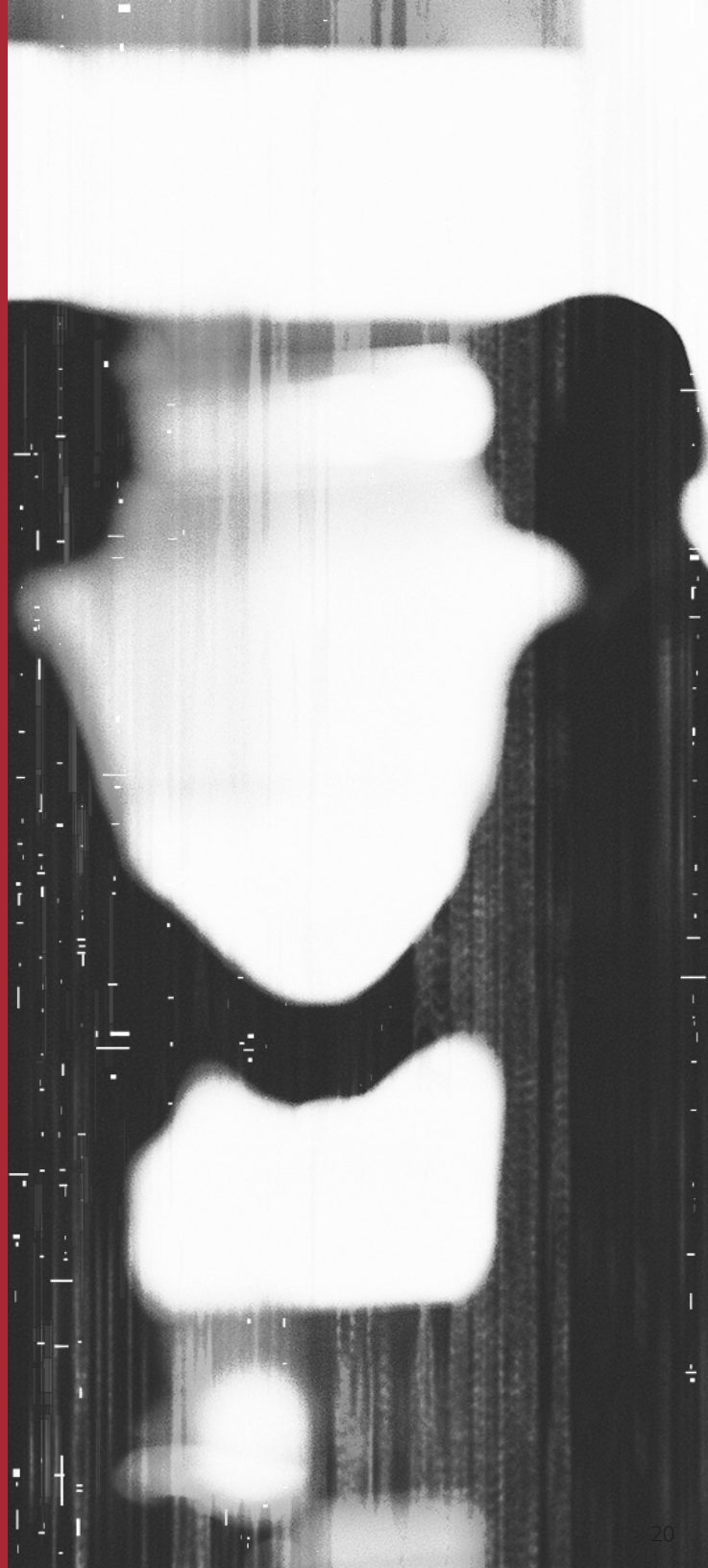
04.
Enforce DMARC

05.
Be transparent with customers

one.

Bridge the marketing and IT security siloes

Marketing and cybersecurity have been historically siloed, often due to conflicting motivations: Marketers aim to get customers in the door, cybersecurity professionals aim to keep unauthorized people out. But to best protect against brand impersonation, marketers and cybersecurity teams must begin a productive, constructive partnership. As one interviewee put it, “it’s cybersecurity’s job to ride sidesaddle with marketing.” He explained that while marketers build their brand, security teams should be riding alongside and shooting down fraudulent websites as they pop up so that they don’t get in the way of marketers’ leads. These types of obstructions to marketing include DMARC — if marketing teams have massive email campaigns or regular email communication partners, those emails must always be seen as legitimate. If a company’s DMARC policy isn’t appropriately set, key emails could end up in spam folders or rejected.

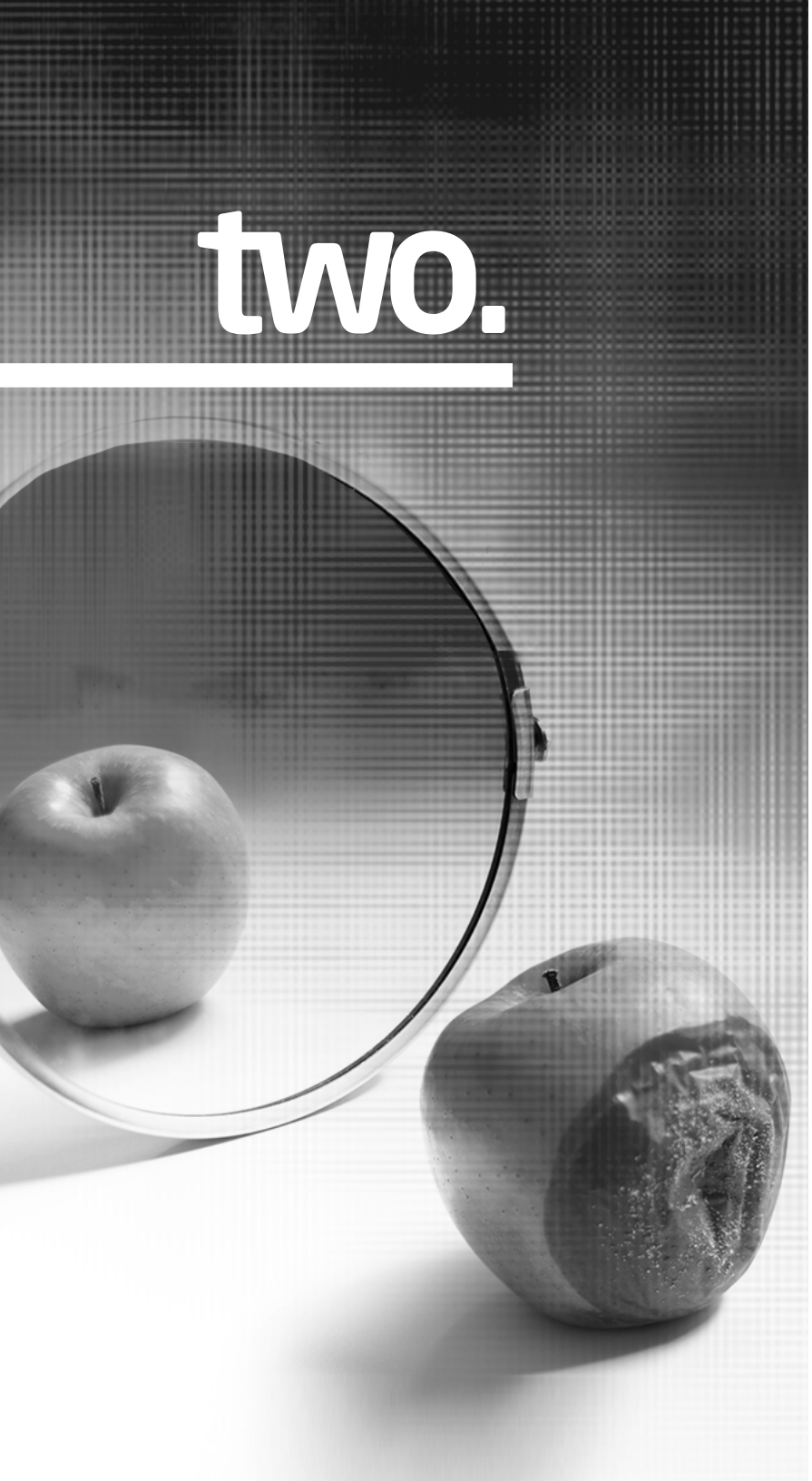


If a company's DMARC policy isn't appropriately set, key emails could end up in spam folders or rejected.

The interviewee mentioned earlier in this report who used brand impersonation monitoring to build a collaborative bridge between his team and the marketing department did so entirely within the company's IT security budget, since marketers were unaware that there might be a brand impersonation issue. He told us: "I only had a suspicion, but it turns out there's a lot more than we would have ever anticipated — we take down an average of about 10 or 11 fraudulent sites every month, usually within 48 hours of notification." His marketing counterparts became active partners once they saw the extent of brand impersonation attacks against their customers, helping the security team tell which emails were legitimate and which were from impersonators.

He added: "My guess is if I offered to shut down [our brand protection service] now, they'd say 'Wait a minute, why are you doing that? We need that!'"

"I made the case to my boss and to the marketing team. I said, 'you're spending upwards of two million dollars on your brand, but are you looking for the fraudulent websites, mobile apps and social media accounts that are polluting your brand?' They said 'no.' They had no idea that a lot of malicious actors were trying to impersonate the brand."



Use PoCs to extend brand protection awareness to all stakeholders

The same invisibility that allows marketers to remain blissfully unaware of online brand impersonation until they proactively look for it affects other stakeholders as well. The best practice for making sure your entire organization understands the need to invest in brand protection revealed by our interviews is to show them the problem through a proof of concept (PoC). Instead of attempting to explain DMARC in all its technical complexities, one interviewee set up a PoC of a DMARC tool that showed fraudsters were sending hundreds of thousands of emails abusing the brand. That, he said, illustrated brand exploitation in a way that was universally understood, and leadership began to take the issue very seriously. The interviewee who used the IT security team's budget to roll out a brand impersonation protection solution said that after providing C-suite executives with metrics like monthly takedowns over a six-month time frame, they quickly agreed to the business value of a brand exploit protection solution.

Going a step further, it's critical to educate your employees, suppliers and customers. Humans are the weakest link when it comes to protecting themselves and their organizations, but with the right skills, they can detect even the most subtle brand exploitation attacks. For example, on average, only 6.85% of the clicks on dangerous URLs made by Mimecast customer employees in all of 2020 (Figure 7) were made by people who had undergone cybersecurity awareness training; 93.15% of the clicks were made by people who did not have training.

Unsafe URL Click Volumes, Jan 2020-Jan 2021

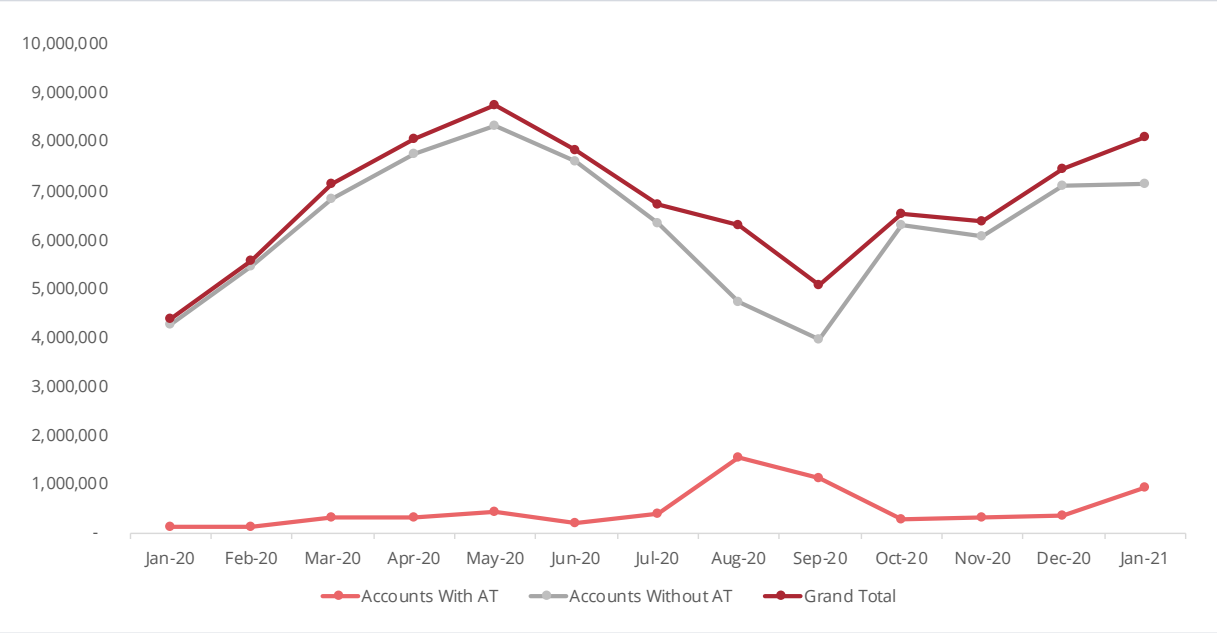


Figure 7: Unsafe URL Click Volumes, Jan 2020 – Jan 2021

13.6x

Without awareness training, employees clicked on malicious links an average of 13.6 times more often!

three.

Use third-party brand protection services

Brand impersonation exists largely beyond a brand's security perimeter, out in the world wide web. This makes it extremely hard to detect, especially since attacks can be elusive; brand phishing sites rapidly crop up and disappear to skirt detection. While many *SOES 2021* respondents say they have teams in place to detect and protect against malicious websites spoofing their brand, nearly one-third (30%) take on the responsibilities in house. According to Frost & Sullivan, that's a costly and time-consuming mistake. In Figure 8, the market research firm shows how a medium-to-large-size business could save time and more than $1.14 million per year using Mimecast's BEP service instead of attempting the same thing in house, including legal fees. In this case, DIY is more costly, time-consuming and less effective than third-party brand exploitation protection services because brand protection is the third parties' core business. These third parties enjoy expertise and close relationships with internet service providers (ISPs), enabling them to take down malicious cloned websites in seconds without the legal fights and fees.

	Manual Online Brand Protection	**Automated Online Brand Protection**
Attribute	In-House Security Analysts and Legal Resources	Mimecast Brand Exploit Protect
Mean Time to Detect (MTTD)	Several weeks or months	Between seconds and 3 hours
Mean Time to Resolve (MTTR)	336 hours or more (2+ weeks)	Between seconds and 3 hours
Number of Customer-side Analysts involved	5 to 20	1 analyst / 10 minutes (telephone call)
Hours Spent on Online Brand Protection	160 hours per month	1 hour per month
Monitoring Frequency	Sporadic / when time allows	24/7/365
Web sites evaluated / Year	Thousands / year	Billions / year
Cost per attack	Up to 13,920 USD	Up to 1,000 USD
Cost to monitor & protect 1 domain / year	Up to 1,002,240 USD	Between 12,000 - 60,000 USD
Annual Legal Fees / year	Up 144,000 USD	0 USD

Source: Frost & Sullivan

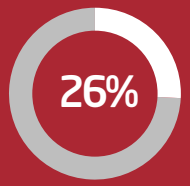
Figure 8: The Annual Budgetary Advantage of Mimecast Brand Exploit Protect[11]

Several interviewees told us they are able to take down malicious web pages within hours by using BEP. The service's automated 24/7/365 model helps reduce mean time to detect (MTTD) from several weeks to mere seconds, with mean time to respond (MTTR) just as fast. More than one interviewee expressed that the sooner sites are taken down, the more likely the criminal will stop or move on elsewhere — when a criminal's efforts are futile, there's no incentive to impersonate the same brand again, so they'll move on to an easier target.

four.

Enforce DMARC

Less than a third of *SOES 2021* respondents (26%) use the DMARC email authentication protocol to stop bad actors from delivering harmful emails that appear to come from their brand's domain. While it's promising that 59% are either planning to start or are in the process of rolling out a strategy, it's important to remember that DMARC is not something that can be simply switched on — it requires monitoring, strategic analysis and planning. If a brand isn't using it to authenticate legitimate emails properly, those legit emails could be seen as spam by mailbox providers, hurting deliverability — and email marketing ROI.



Less than a third of SOES 2021 respondents use the DMARC email authentication protocol to stop bad actors from delivering harmful emails that appear to come from their brand's domain.

There are three phases to DMARC deployment:

1. Monitor:
The first phase of enforcing DMARC illuminates all the email that comes from, or appears to come from, your brand's domains. Some may be from legitimate third parties engaged by marketing or other groups within the business; others may be illegitimate. One organization we spoke with saw 300,000 abusive emails being sent on behalf of the brand at this stage, which they were unaware of before.

2. Analysis:
The next step is to suss out illegitimate senders, and it requires a collaborative effort between the security team, marketing and potentially other departments. Depending on how many service providers are sending out emails on behalf of the organization, this can be a lengthy process — especially since marketing teams commonly partner with dozens of third-party email providers to get closer to customers and prospects. With a block and allow list in hand, you can set your DMARC policy to "quarantine" suspicious emails by sending suspicious emails into the recipient's spam folder.

3. *Rejection!:*
The ultimate goal of DMARC is to reach a "reject" policy, in which any time an unauthorized sender uses a brand's domain, that email is rejected by the receiving email server — it never reaches the intended recipient.

Third-party solutions are available to streamline the DMARC process, and are "often the most effective way of getting to the point where emails can be rejected if they fail DMARC," according to Gartner Inc.[12] As one interview told us: "I'm excited by DMARC. I think it will close down another loophole exploited by cybercriminals, thereby making the internet a safer place for our customers and staff."

Be transparent with your customers

While brand protection solutions and DMARC email authentication can greatly reduce brand impersonation attempts, the threat isn't likely to disappear any time soon.

So a robust brand exploitation strategy must include customer education. According to one interviewee, this is key: "We pride ourselves in working very closely with our customers. We communicate with them extensively and warn them the minute we become aware of a bad actor's tricks. We like to think we're a trusted name and a trusted partner." Being transparent about brand impersonation while providing guidelines that empower your customers to say safe — such as basic awareness training and cyber hygiene practices — can reassure customers and demonstrate that a brand is actively working in their best interests, thus building brand equity. Consider the approach of the U.S. Internal Revenue Service (IRS): In light of many common IRS scams, the agency regularly reminds citizens that the IRS will never make phone calls requesting certain personal information.

The Bottom Line

Without a doubt, brand marketers are losing leads, brand affinity and customer loyalty to cybercriminals who impersonate their brands to scam their customers and prospects. And our analysis of the world's top 100 most valuable brands shows that the bigger and more respected the brand, the more it is at risk for brand impersonation. Meanwhile, many marketers, particularly at smaller brands, remain unaware of these risks because brand impersonation is virtually invisible to them — unless they monitor for it proactively.

Even once identified, brand impersonation sites can be time-consuming and costly to remove from the web, often requiring legal action.

However, relatively new brand protection and email authentication technologies can help marketers once again become the masters of their own brand domains. Doing so requires cross-silo collaboration between enterprise marketing and security teams and can be greatly accelerated through the use of expert third-party brand protection services.

mimecast®

Relentless protection. Resilient world.™

1. *2020 Global Marketing Trends*, Deloitte | 2. *The Global State of Online Digital Trust*, Frost & Sullivan
3. *CMO's Guide to Email Marketing ROI*, Litmus | 4. *Phishing Activity Trends Report*, 4th Quarter 2020, Anti-Phishing Working Group
5. Ibid. | 6. Ibid. | 7. *2019 Internet Crime Report*, FBI Internet Crime Complaint Center | 8. "*The biggest GDPR penalties for noncompliance*," Spirion
9. *The Global State of Online Digital Trust*, Frost & Sullivan | 10. "*News UK finds high levels of domain spoofing to the tune of $1 million a month in lost revenue*," Digiday
11. *Managing Digital Risk: The Security Challenge Beyond Your Perimeter*, Frost & Sullivan | 12. *Protecting Against Business Email Compromise Phishing*, Gartner Inc.

Mimecast is a cybersecurity provider that helps thousands of organizations worldwide make email safer, restore trust and bolster cyber resilience. Mimecast's expanded cloud suite enables organizations to implement a comprehensive cyber resilience strategy. From email and web security, archive and data protection, to awareness training, uptime assurance and more, Mimecast helps organizations stand strong in the face of cyberattacks, human error and technical failure.