mimecast

Brand Trust:

One cyberattack is enough to lose consumer trust and custom

It takes years to build a brand. A cyberattack that exposes customer data or even simply paints the company in a negative light can cause catastrophic loss of trust in an instant.

Trust is a cornerstone of any successful business. Some professions – hairdressers, for example – spring to mind more than others. But the fact remains: every brand is built on trust, and once it's broken, a loss of custom almost certainly follows.

In today's digital economy, consumers have more choice than ever when it comes to spending their hard-earned cash. In such a fiercely competitive environment, companies are going to great – and sometimes headline-grabbing – lengths to win customers' attention.

The investments are significant, the expected return high. However, most companies either ignore or underestimate the most important competitive differentiator of all – trust. All the marketing in the world counts for nothing when cybercriminals use the brand to dupe loyal customers by preying on that trust.

It takes years to build a brand. A cyberattack that exposes customer data or that even simply paints the company in a negative light can cause catastrophic loss of trust in an instant. In the last twelve months, attack volumes skyrocketed, as bad actors sought to exploit the pandemic. Experts don't expect threat levels to abate, if anything, it may well continue to rise, as hackers look to exploit the fear and confusion stemming from the pandemic and the slow return to some form of 'new normal'.

Fortunately, all is not yet lost. Cybersecurity companies are continuing to fend off cybercriminals and consumers are slowly but surely becoming wiser to everyday threats. But there's still more to be done in this never-ending battle.

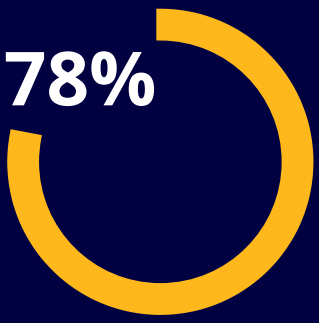
Mimecast's latest round of research, which features insights from over 9000 adults (aged 18-65) in the Benelux, Nordics, United Kingdom, Germany, South Africa, Australia and the Middle East.

The goal? To raise awareness, get brands on the front foot, and make loss of trust a problem CTOs and CMOs never have to face.

Understanding the cyberthreat landscape

When it comes to understanding cyberthreats, it's promising to see that over three-quarters of respondents agree that anyone can be a victim of cybercrime – and that they also understand the risks involved.

Knowing the risks and being able to mitigate them are two very different challenges, however. As the saying goes, awareness is the first step to action.



78% **agree anyone can be a victim of cybercrime**

75% **understand the risks of phishing or spoofing**

SA **middle aged men most knowledgeable**

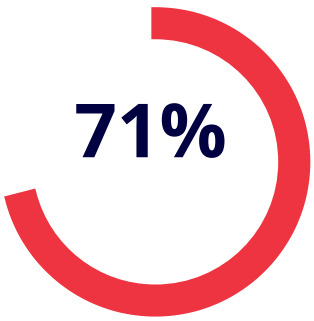
DE **18-24 year olds least knowledgable**

Understanding the risks of phishing or spoofing

Perhaps unsurprisingly, it's a similar story when understanding the risks – if you're more aware that anyone can be a victim, it seems logical that you'd be more mindful of the risks of phishing and spoofing.

In summary, middle aged South African men are the most knowledgeable when it comes to cybersecurity risks. On the other end of the spectrum, 18-24 year old Germans would benefit from brushing up on their cybersecurity awareness training and improving their cyber hygiene.

of South African respondents are aware of their susceptibility to cybercrime



of Danish respondents are aware of their susceptibility to cybercrime

Understanding anyone can be a victim

Looking across all the markets surveyed, South Africa is the country most aware of its susceptibility to cybercrime (92%). This is followed closely by 81% of Saudi and UAE respondents and 80% of Australians. Denmark, on the other hand, is more (perhaps blissfully) unaware of the risks (71%).

The generational gap when it comes to cyber awareness is even more striking, with Gen X (45-55 YO) appearing a lot more savvy compared to the (supposedly) digital native Gen Z (18-24 YO). 75% of millennials (25-34 YO) agree that anyone can fall victim to cybercrime, which seems to follow a trend to more mature reasoning than their younger counterparts.

80%
females agree

76%
males agree

85%
45-55 YO agree

75%
25-34 YO agree

70%
18-24 YO agree

How often are consumers being targeted?

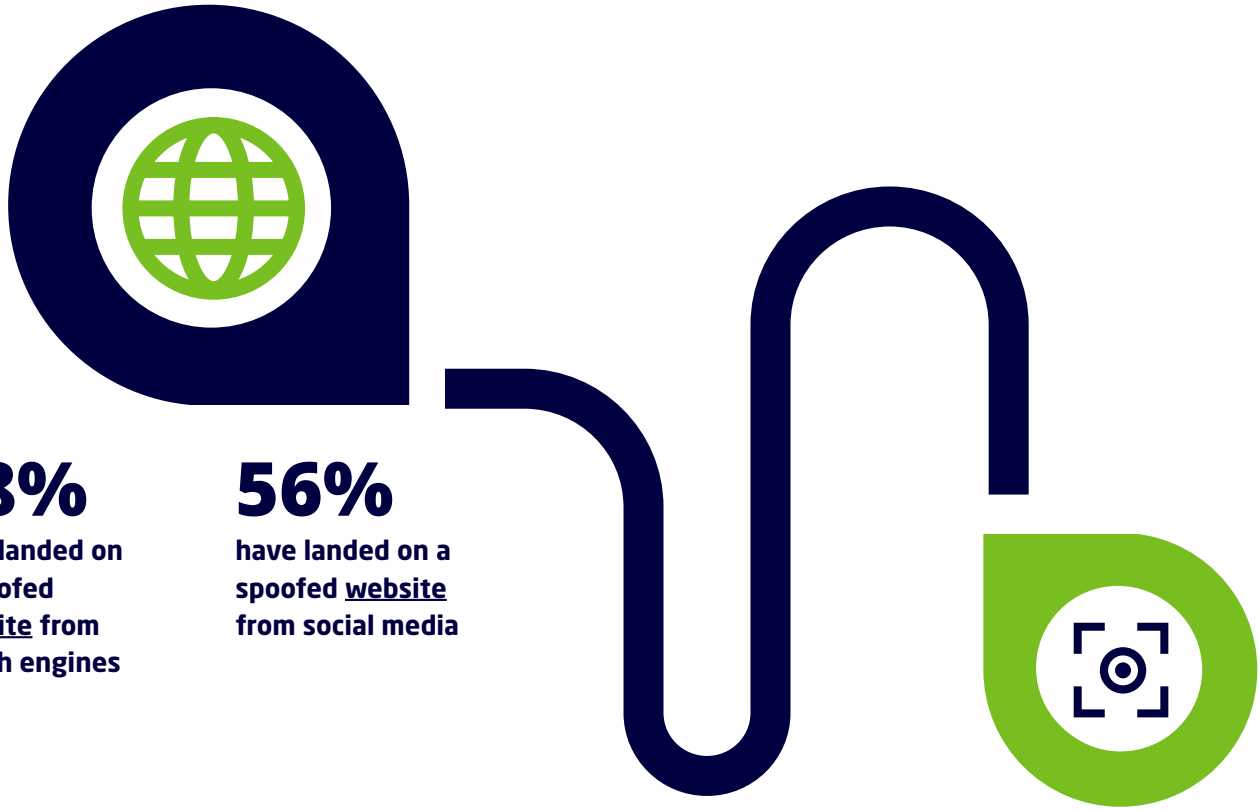
Since the start of COVID-19, cybercriminals have worked tirelessly to expose the vulnerabilities that come with widespread remote working. In Mimecast's State of Email Security 2021 report (SOES), it was revealed that email-based security threats soared by 64% in 2020.

These latest findings return equally worrying results, and it seems no country is immune, with consistently high averages across all the surveyed countries. South Africa and the UAE battle it out for top spot. Over a quarter of respondents from both countries have landed on a spoofed website from social media or search engines or have been directed to a fake website from a phishing email. This is in contrast to the Netherlands and Germany where only around 4 in 10 reported the same.

79%
received a phishing email to their inbox

50%
received a forwarded phishing email

54%
have opened a phishing email



58%
have landed on a spoofed website from search engines

56%
have landed on a spoofed website from social media

55%
have been directed to a fake website from a phishing email

Threat-spotting: how are consumers mitigating risk?

Most respondents check before they click

It's promising to see that most respondents from all regions do at least apply some form of checking before opening an email or landing on a website. While around a half of respondents in most of the regions carry out the necessary checks, only around a quarter to a third of respondents in the Middle East do the same. Meanwhile Australia appears to be consistently good at looking out for warning signs.

There are a few ways consumers keep an eye out for anything untoward. But a minority are still unaware of the overall threat. Of those who don't carry out any checks (6%), 53% don't know or are unsure of what they should be looking for and over a quarter (27%) wouldn't know how to check whether an email is valid.

Perhaps more worryingly, 2% said they would just open an email, regardless of whether they thought it was suspicious. Brave or downright reckless? We'll let you be the judge of that.

Younger vs Older

Despite a majority of respondents from every region taking the right measures on their email and landing page checks, can the same be said for all ages?

You might assume that doing the relevant checks would be second nature to the younger, digital natives, but surprisingly they fell behind the other generations with only 43% taking the necessary precautions. On average around half of respondents in all the other generations did the four main security checks. It's clear that for Gen Z, more needs to be done when it comes to cyber hygiene.

Who is checking what is in phishing emails?

53%

check spelling of the email address

60% **UK**
58% **BE**
57% **AUS**
54% **DK**
54% **DE**
53% **SE**
53% **NL**
53% **SA**
35% **KSA**
27% **UAE**

52%

check spelling within the email

59% **BE**
59% **SE**
57% **AUS**
57% **UK**
54% **DE**
53% **DK**
53% **NL**
50% **SA**
29% **UAE**
25% **KSA**

47%

check email subject line

54% **RSA**
54% **AUS**
52% **SE**
49% **UK**
48% **DE**
47% **BE**
45% **DK**
40% **NL**
28% **KSA**
27% **UAE**

43%

check URLs within the email

49% **RSA**
48% **NL**
46% **BE**
46% **UK**
41% **SE**
41% **AUS**
41% **KSA**
37% **DK**
35% **UAE**
34% **DE**

Top 10 most trusted industries across all countries

70% **Healthcare**

69% **Online banking**

65% **Utilities**

63% **Entertainment**

59% **Local council/gov**

57% **Online retailers**

55% **Transport**

53% **Insurance**

51% **Delivery**

47% **News**

What are the most (and least) trusted industries?

Once again, our findings return some interesting results; and it's clear that when it comes to trust, not all industries are created equal. Healthcare leads the way in terms of being most trustworthy and ranks well above the least trustworthy industry: holiday providers. This is despite a surge in cyberattacks targeting healthcare organisations amid the pandemic – from emails impersonating the NHS and the WHO to vaccine scams and DDoS attacks on hospitals.

What are the most (and least) targeted industries?

There is surprisingly little correlation between consumers' perception of brand trustworthiness and cyberthreats targeting those industries. For example, while online banking was the second most trusted vertical we surveyed, it is also the most targeted across all geographies. This trend may be explained by a surge in cybersecurity measures among banks over the past few years. In effect, banks have revisited their entire operating models, setting up dedicated fraud desks handling any possible issues customers may face around the clock and communicating extensively about it. Offering this level of security is now a Unique Selling Point (USP) for many banks, particularly for online and mobile customers.

Holiday providers, on the other hand, are among the least trusted, despite facing one of the lowest rates of attacks.

Consumers received phishing emails from brands in the following industries

28%	Online banking
26%	Delivery
23%	Online retailers
21%	Entertainment
16%	Insurance
13%	Holiday providers
16%	News
12%	Utilities
10%	Local council/gov
10%	Healthcare

Congratulations you've won a prize

Digging a little deeper, it also seems cybercriminals have some go-to tactics and messages of choice. It won't come as a surprise that the most common threat is emails or texts claiming that 'you've won a prize' (55%).

Often, phishing attempts are so ridiculous it's clear they're from untrusted sources. But occasionally, especially as bad actors refine their tactics, consumers could be forgiven for confusing those communications with those sent by legitimate organisations.

Other popular phishing email or text messages includes

40%
Claim your payment now

37%
You've received an offer

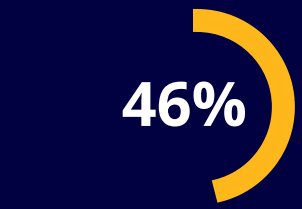
32%
Your delivery is delayed or on hold

32%
Check your account NOW

32%
Someone has been trying to access your account

Just how much do consumers trust their favourite brands?

Unfortunately, as we've alluded to previously, while consumers can spot many phishing attempts, cybercriminals are unrelenting in their efforts to trick the masses. In recent years, we have seen a surge in impersonation attacks – starting with emulating popular brands. While many consumers are cyber-aware, these attacks are still successful for over one third of respondents.



of consumers don't hesitate to open an email from brands they use regularly

of consumers don't hesitate to click on links in emails from their favourite brands

Brand trust: how do the countries fare?

Looking across the surveyed countries there's also a disparity when it comes to brand trust. Sixty nine percent of South Africans don't hesitate to open an email from brands they use regularly and 69% in the UAE don't hesitate to click on links from their favourite brands. The European countries and Australia tend to be more neutral on the matter, with only 24% of the Dutch not hesitating to click on links in emails from their favourite brands and 35% opening emails from brands they use regularly.

One statistic that tells a slightly different story, however, is the fact that almost a third (30%) of consumers think they're just as likely to open a phishing email as it is for their sensitive data to be stolen due to a data breach suffered by a brand they use regularly.

In the grand scheme of things, this final point doesn't reflect too kindly on brands, and we must ask the question: can they be doing more? In the following section, we explore the consumer-brand relationship in more depth and the damage that almost inevitably ensues once trust is broken.

Being the subject of spoofing or phishing spells bad news for brands

The jury is in: the impersonation of household brands by bad actors can have a huge impact on the trust (and spending) of consumers.

In fact, 61% agree they would lose trust in their favourite brand if they disclosed personal information to a spoofed version of its website. Similarly, 61% agree they would lose trust in their favourite brand if they disclosed personal information to a faked website spoofing that brand.

And as is probably to be expected, this loss of trust is directly related to a loss of revenue. Over half (57%) of all respondents agree they would stop spending money with their favourite brand if they fell victim to a phishing attack involving that brand.

61%

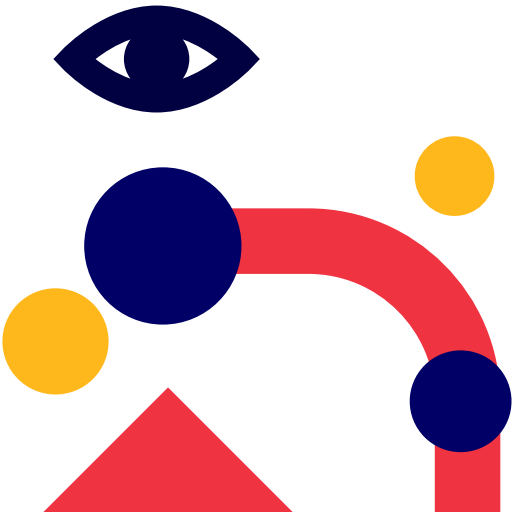
would lose trust in their favourite brand if that brand disclosed personal information to a spoofed version of its website

61%

would lose trust if their money was stolen due to impersonation

57%

would stop spending money with a brand if they fell victim to a phishing attack



Breaking the research down on a country-by-country basis

The Middle East and Africa are by far and away the least forgiving towards their favourite brands if their money is stolen due to a phishing email impersonating them. South Africa leads the pack.

ME is also leading the way in agreeing they would stop spending money with their favourite brand if they fell victim to a phishing attack involving that brand. The UAE would be the first to stop spending money.

On the surface of things, it might seem that Danish respondents are more forgiving. But the fact just under half (45%) would also stop spending money would be a significant financial dent for brands.

This data makes for a sobering read for companies relying on consumer trust and loyalty: despite spending years building a strong rapport with their target audience, all it takes to lose that trust is one single cyberattack. This alone should make companies more cautious when it comes to their cybersecurity – and make deploying tools to better monitor their email communication or find and remove faked versions of their website a strategic priority.

loss of trust in their favourite brand if their money is stolen due to phishing or impersonation

81% RSA

78% KSA

78% UAE

67% UK

62% AUS

53% DE

50% SE

49% NL

48% BE

45% DK

customers that would stop spending money with a brand they use regularly if they fell victim to a phishing attack

77% UAE

75% KSA

74% RSA

64% UK

58% AUS

48% DE

48% SE

47% NL

47% BE

45% DK

Consumers expect brands to keep them safe

Brands could be doing more

It would certainly seem they need to, owing to the overwhelming volume of consumers (78%) who expect their favourite brands to ensure their services are safe to use, be it websites, email, or any other form of contact with consumers.

This figure shoots up to 93% in South Africa, with the UK (86%), UAE (82%) and KSA (81%) not far behind. But even the more forgiving Germans had 69% of respondents saying that they expected brands to keep their services safe. Consumers are therefore showing a united front on this opinion, regardless of age, gender or geography. In a digital-first world, having good products and responsive customer service is no longer enough for companies: they now also have a mandate to keep people's data safe and take steps to prevent them from falling victim to cyberattacks involving their brand name.

Should brands take accountability for cybercriminals?

And it doesn't stop there. Beyond keeping consumers safe, a fair chunk of respondents also expects brands to bear the brunt of responsibility should they ever be compromised. Be it failing to compensate customers, not being accountable, or simply being the brand associated with a spoofed website or phishing email that resulted in a loss of money, failing to avoid cyberattacks or handling them in ways that meet consumer expectations can impact perception of your brand.

Brands hope it never comes to this, but ensuring consumer safety is easier said than done. Since fake websites or phishing emails that impersonate brands are outside of the company's traditional systems and processes, they're difficult to spot – and most organisations are blind to them as a result. Even unsophisticated attackers can easily register a domain that looks similar to a legitimate one and create a fake website that is virtually identical.

Incidents most likely to negatively impact perception of a brand

35%

Brands refusing to compensate customers

33%

Brands refusing to take responsibility for customers being deceived

31%

Losing money as a result of interacting with a faked website

30%

Losing money as a result of interacting with a phishing email

“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”

Customer Testimonial

Stop direct domain spoofing with DMARC

In today's digital age, where one cyberattack is enough to lose consumer trust (and custom), brands need to be doing everything within their power to ensure consumer safety – and to protect their own positive brand image.

One way to do so is by stopping direct domain spoofing. In the ongoing mission to safeguard their brands, more and more companies are achieving this with Domain-based Message Authentication, Reporting and Conformance – better known as DMARC.

In a nutshell, DMARC is an email validation system designed to uncover anyone using a brand's domain without authorisation and then block the delivery of all unauthenticated mail, preventing customers, partners, and employees from receiving emails from impersonators. There are three key phases to DMARC deployment:

1. Monitor: The first phase of enforcing DMARC highlights all the emails that come from, or appear 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.

2. Analysis: The next step is to suss out illegitimate senders. This requires a collaborative effort between the security team and marketing; it could also involve other departments according to your setup and how serious the threat is. Depending on how many service providers are sending out emails on behalf of the organisation, this can be a lengthy process. 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, whereby any time an unauthorised sender uses a brand's domain, that email is rejected by the receiving email server – so it never reaches the intended recipient.

It's likely for this reason that in this year's State of Email Security 2021 report, more than eight out of 10 (85%) respondents indicated that their companies are already making use of DMARC, are in the process of implementing the protocol, or plan to do so in the next year.

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

Customer Testimonial

Find and neutralise brand imitation with Brand Exploit Protect

Brand impersonation attacks that compromise customers and partners are devastating. They destroy trust, are extremely difficult to uncover, and even harder to shut down. Unfortunately, they're also all too easy for criminals to create.

Even unsophisticated attackers can register domains that look like yours and use your brand as bait to target the people who trust it. And, while DMARC can help, it's only designed to be effective against domains you own. Ultimately, it's no longer enough to protect just what's yours – it's time to move from defence to offense.

One of the most effective ways to block brand attacks before they can launch, as well as stopping live attacks in their tracks, is with Mimecast's Brand Exploit Protect (BEP). Our innovative service uses a combination of machine learning and quadrillions of targeted scans to identify even unknown attack patterns at an early stage, blocking compromised assets before they become live attacks. Or, if active attacks are discovered, they can be rapidly remediated to minimise damage.

Of the many ways cybercriminals exploit your brand, link manipulation, or the registering of domains with names very similar to legitimate brand web pages, is a popular choice for bad actors – with manipulated links often directing users to fake websites that host malicious content.

Often, this works in conjunction with website spoofing: the term we use to describe spoofed websites built by cybercriminals that look like legitimate brand sites, which users are usually directed to via manipulated links.

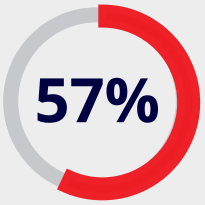
Unfortunately, anyone can be a victim of brand impersonation – especially if they have a website with a customer login. But the bigger your brand, the harder the phish, with larger companies often targeted as they can siphon away potential money or credentials.

Fortunately, Mimecast's BEP has you covered, regardless of your brand's size. Combined with full DMARC visibility, reporting and enforcement, it helps you protect against the misuse of your owned domains as well as spoofed domains, covering both external targets and your own organisation and employees.

That's end-to-end email and brand exploit protection from a single, trusted leader in the market.

Key takeaways

Consumer trust is paramount to a brand's financial success and reputation.



respondents agree they would stop spending money with their favourite brand if they fell victim to a phishing attack leveraging that brand.

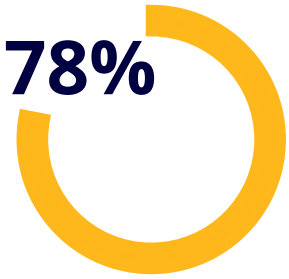
% of respondents agree they would lose trust in their favourite brand:

61%
if they disclosed personal information to a spoofed version of the website.

61%
if their money was stolen due to a phishing email impersonating them.

The onus is on brands to secure their email communications and their websites; their customers expect it.

69% AND 70%
respondents agree it is the brand's responsibility to protect itself from email impersonation and from fake versions of its website respectively.



respondents expect their favourite brands to ensure their services (website, email, communications etc.,) are safe to use.

Brands' biggest loss of reputation comes from:

35%
refusing to compensate customers who were victims of cyberattack leveraging their brand

33%
not taking responsibility for cyberattacks leveraging their brand

Top trusted industries:
Healthcare, Online Banking, Utilities

Most leveraged for phishing attacks:
Online banking, delivery services, and online retailers

Protect your brand

1. To best protect against brand impersonation, marketers and cybersecurity teams must begin a productive, constructive partnership.

2. Enforce DMARC- an email authentication protocol to stop bad actors from delivering harmful emails that appear to come from your brand's domain.

3. Use third-party brand protection services, like Mimecast Brand Exploit Protect.

4. As the research shows, transparency with customers is key.


mimecast®
Relentless protection. Resilient world.™