MEMCYCO

2024 Survey

State of Digital Impersonation Fraud Resilience

memcyco.com

INTRODUCTION

With much of daily life now happening online, phishing-related digital impersonation fraud has never had such wealth of opportunity, and the statistics speak for themselves.

According to the U.S Federal Trade Commission, consumers lost almost USD $8.8 billion to impostor scams in 2022

Source: Federal Trade Commission

With generative AI and off-the-shelf 'phish kits' lowering the barrier to entry, even a bedroom novice can scale sophisticated attacks that make multi-million-dollar headlines.

With fraudsters more empowered than ever, how empowered are businesses to keep pace and protect customers from digital impersonation scams? This was the central question behind this Memcyco survey.

Specifically, we wanted to discover

- **What businesses are doing to proactively protect customers (and themselves) from an increasingly hard-to-see problem,**
- **what the primary 'awareness triggers' are for first detection of new phishing-related scams impacting customers,**
- **and how effective the in-place solutions are for helping businesses get a proactive grip of the digital impersonation problem.**

Some of the report findings were unsurprising. Others were eye-opening for anyone unaware of the risk gaps that even popular digital impersonation protection solutions leave open.

METHODOLOGY

We commissioned a survey of 200 full-time employees from Director to C-level in Security, Fraud, Digital, Web, and Online. 140 respondents live in the United States, with the remainder in Canada and the United Kingdom.

At the time of being surveyed, all respondents worked in companies with more than 1,000 employees across multiple industries, with 30% working in Retail and 30% in Finance. We specifically screened for companies who have online traffic of more than 10k monthly visits on a transactional site, containing either a login page or a checkout page.

This report was administered online by Global Surveyz Research, a global research firm. The respondents were recruited through a global B2B research panel and invited via email to complete the survey, with all responses collected during Q3 and Q4 2023. The average amount of time spent on the survey was 5 minutes and 22 seconds. The answers to the majority of the non-numerical questions were randomized to prevent order bias in the answers.

MEMCYCO

CONTENTS

KEY HIGHLIGHTS

Businesses rely on threat victims as part of their threat intelligence

2/3 of businesses (66%) admit to first learning of new website impersonation scams from scam-victim incident reports, rather than preemptively detecting scams before incidents occurring.

72% of businesses surveyed use a digital impersonation protection solution

The majority of businesses use solutions for detecting fake websites involved in phishing-related scams.

Only 6% of businesses using a digital impersonation solution say it solves the problem

Of the 72% of businesses using a digital impersonation protection solution, less than 10% are satisfied that it actually protects them, and customers.

Customers don't hesitate to use what little power they have to pressure businesses

Over 1/3 of organizations learn about website impersonation scams after **'brand shaming'** by customers on social media.

2024 State of Digital Impersonation

Survey Findings

How aware are businesses of website impersonation attacks?

Businesses are aware of website impersonation, but they often treat the symptoms, not the cause

Over two-thirds of businesses (68%) know that their own website is being impersonated, and almost half (44%) recognize that this impersonation directly impacts their customers. Just 2% of businesses say they are not aware of impersonation attacks at all.

Businesses understand how common website impersonation fraud is. But, in most cases, they only become aware of the fake websites behind scams when the customers report incidents.

Awareness is high, with 68% of businesses saying they're aware of 'spoofing' attacks targeting their website, and 44% claiming to be aware of such attacks targeting customers.

But, 2/3 (66%) of businesses admit their most common method for gaining awareness of website impersonation attacks is via incident reports from affected customers. That's compared with 64% who said their most common 'awareness trigger' is by identifying suspicious domains themselves, or via a third-party service.

What this suggests is that most businesses surveyed are conscious of, and trying to tackle fake-site fraud. But, too often, they rely on customers to gain attack visibility after it's too late – when customers have been either targeted, or defrauded.

With AI and phish-kits increasingly available off-the-shelf, how much longer can businesses afford to rely on customers as their main source of threat intelligence?

Worryingly, over 1/3 (37%) of businesses said they first become aware of fake websites when customers affected by phishing-related scams publicize their experience on social media – known as 'brand shaming'.

This underscores the churn, revenue and reputational risks businesses are taking in continuing to rely on customers for gaining phishing-related fraud visibility in the aftermath of attacks.

It also emphasizes the lack of effective solutions available for protecting both businesses and their customers.

How aware are businesses of website impersonation attacks?

The worst part? This is just the tip of the iceberg

Businesses need to ask themselves, what's happening below the waterline? We all know that countless customers targeted by website impersonation attacks never report incidents, so damage is likely to be far greater than what's immediately visible. The true impact on reputation and bottom line is impossible to quantify.

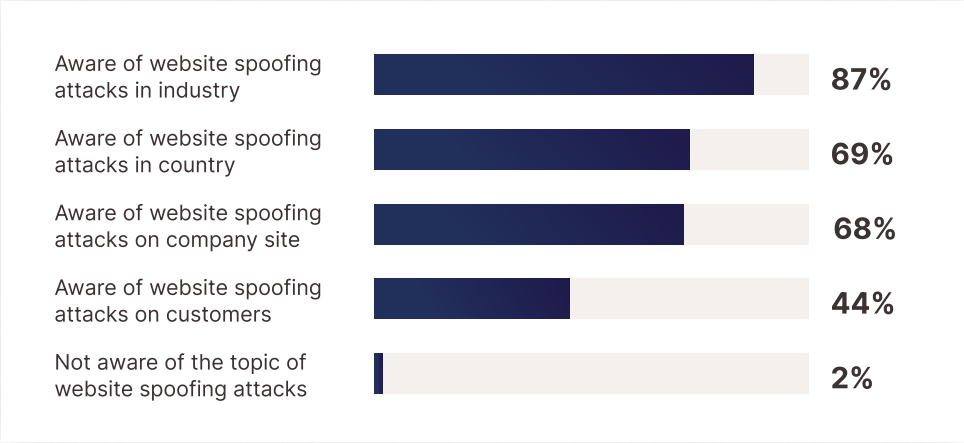


Figure 1: Awareness of Website Impersonation Attacks

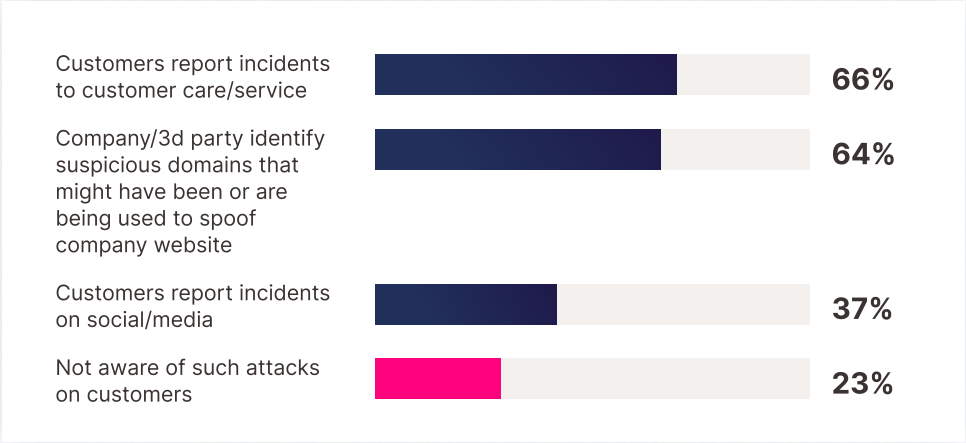


Figure 2: Awareness Trigger for Customers Being Attacked by Website Spoofers

What is the biggest fear factor about website impersonation? Clue: it's not customer financial losses

What's the biggest fear factor for organizations about the impact of website impersonation attacks?

The top three fears are closely ranked, with reputational damage, theft of Personally Identifiable Information (PII) and Account Takeover (ATO) all marked concerns for today's businesses.

89% have experienced theft of PII or are concerned about this risk, and 82% say the same about ATO.

There's more happening out of sight

It's interesting to note that more than one in four businesses (28%) say they have already experienced reputational damage due to website impersonation attacks.

If we consider the number of attacks that are never reported, this percentage is likely to be a lot higher.

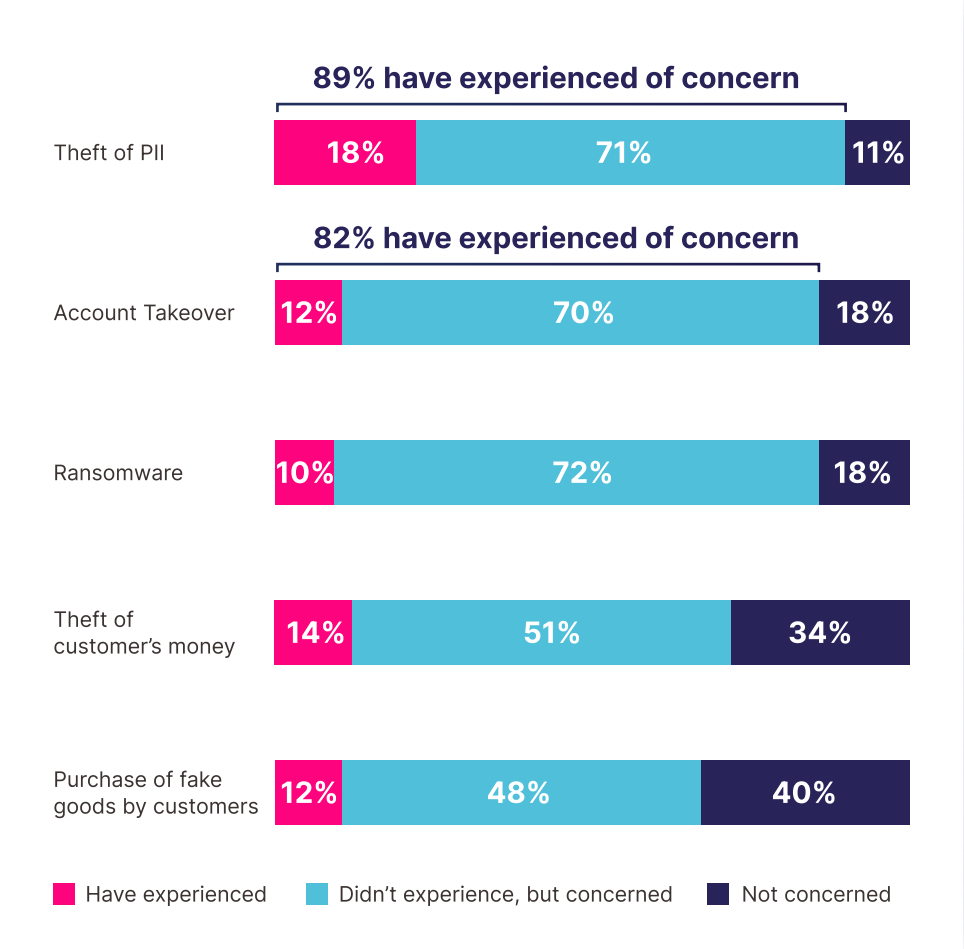


Figure 3: Negative Impact of Website Impersonation Attacks

How many spoofing incident complaints do businesses claim to receive?

Instead of wasting time complaining, some customers just say 'goodbye'

We asked respondents how many customer complaints they receive each year about website impersonation scams. On average, they reported 8 calls. 60% claim to have received between 1-10 complaints, despite third party research pointing towards the issue of phishing tripling since 2020.

It could be that organizations are reluctant to admit the size of the issue, or that respondents are simply unaware of the extent of the problem.

The silent majority

We know that website impersonation scams are growing year on year. If only a fraction of customers who experience these attacks are reporting the incident, how many more are simply severing ties with your brand and quietly walking away?

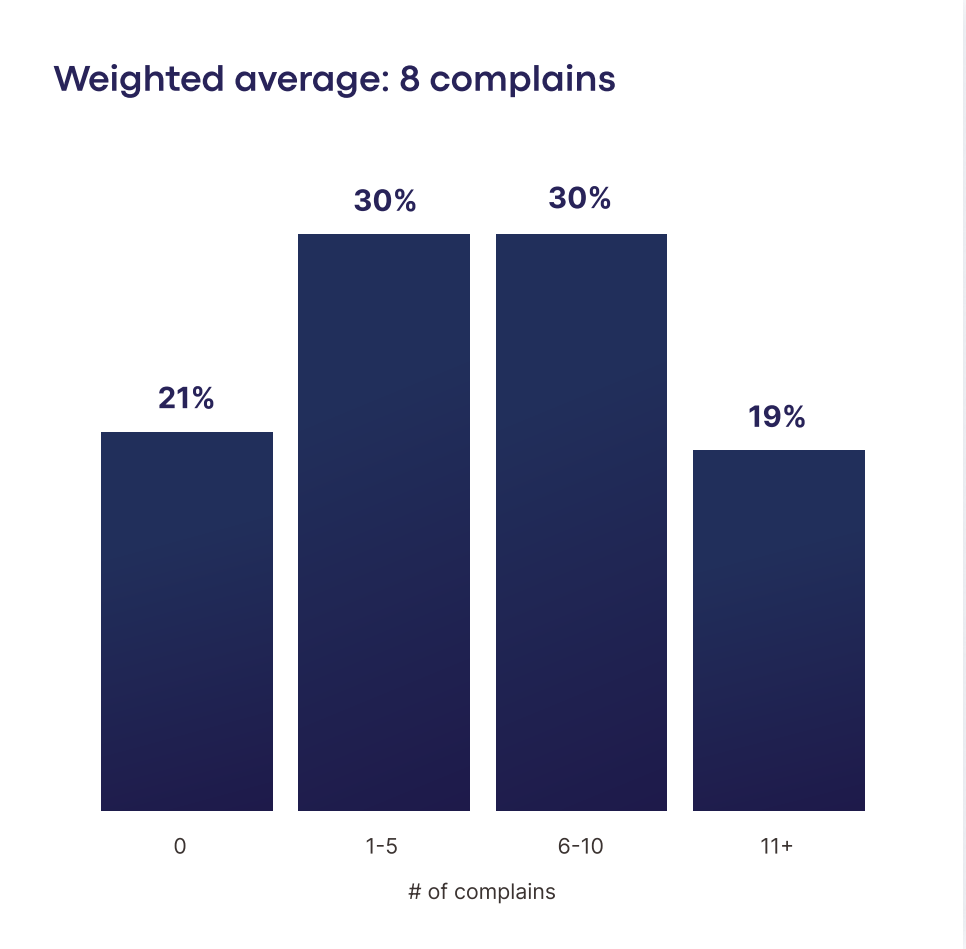


Figure 4: Number of Customer Complaints About Website Attacks, Last 12 Months

What are businesses‘ current scam protection methods?

Customers are being bombarded with awareness programs.... while scams keep exploding

We asked businesses how they are protecting their customers from the rise in website impersonation scams, and found the top protection method is education. 78% are educating customers on detecting and avoiding scams.

Despite this, successful impersonation attacks are skyrocketing. With the introduction of ready-made, off-the-shelf scamming kits, and the growth in Generative AI, attackers are leveraging ease and accessibility to convince customers to click.

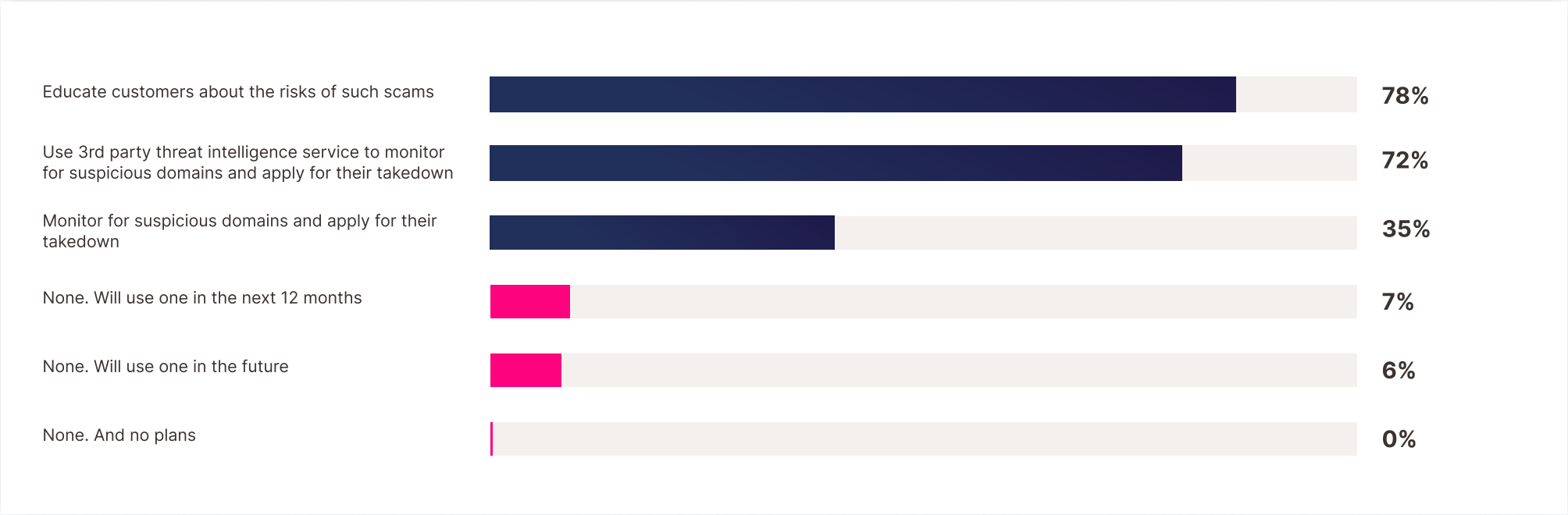


Figure 5: Current Protection Methods from Online Impostor Scams

How effective are the anti-website impersonation solutions that businesses currently adopt?

A drop in the ocean: current solutions are still behind the problem

Despite the multi-department effort identified in Figure 5, and the 72% of businesses that are using a third party threat intelligence service (Figure 7), applied solutions are failing to solve the challenge. Just 6% of respondents say that their current approach solves the issue of website impersonation completely.

The remaining 94% continue to suffer, with both the business and the customer suffering the consequences.

Both Finance and Retail are playing catch-up

We broke down the responses by industry to see whether one area is finding mitigating this growing threat easier than another.

Despite being the industry that suffers the greatest number of impersonation attacks, just 2% of Finance businesses claim to have solved the issue. In Retail, businesses overwhelmingly know that their in-place solutions are failing to protect against the current threat level. **73% of retailers say they have impersonation attacks occurring in their environment that their current tools can't address.**

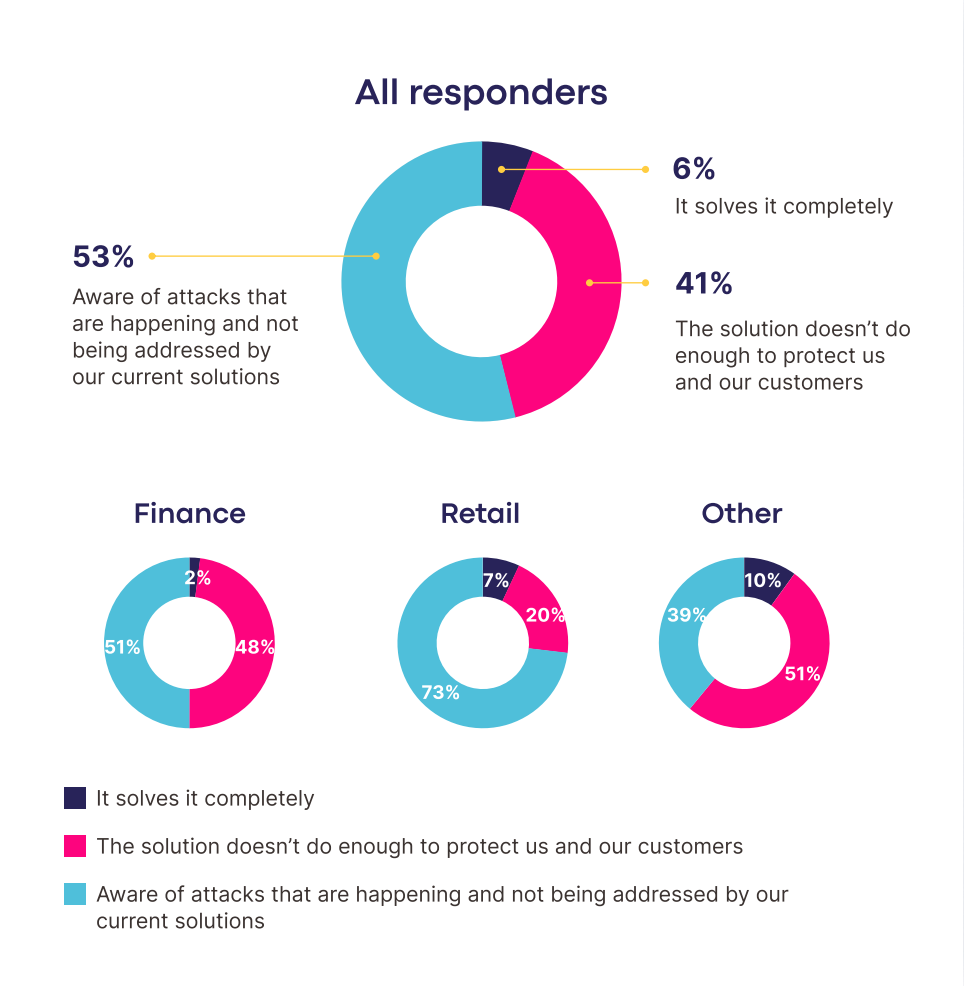


Figure 4: Number of Customer Complaints About Website Attacks, Last 12 Months

Head in the sand: Do businesses understand the need for customer reimbursement?

Despite upcoming regulation enforcing it, just 2% reimburse customers for website impersonation damages

We asked businesses whether they reimburse customers who are scammed by website impersonation, and found that 81% do not. Of that cohort, almost half are fully aware of upcoming regulation that will legally enforce reimbursement.

Last-minute U-turns: "Only when we have to"

Reading between the lines, despite being aware of the regulation, these companies are unwilling to act voluntarily, and prefer to remain inflexible and refuse reimbursement until they are legally required to comply.

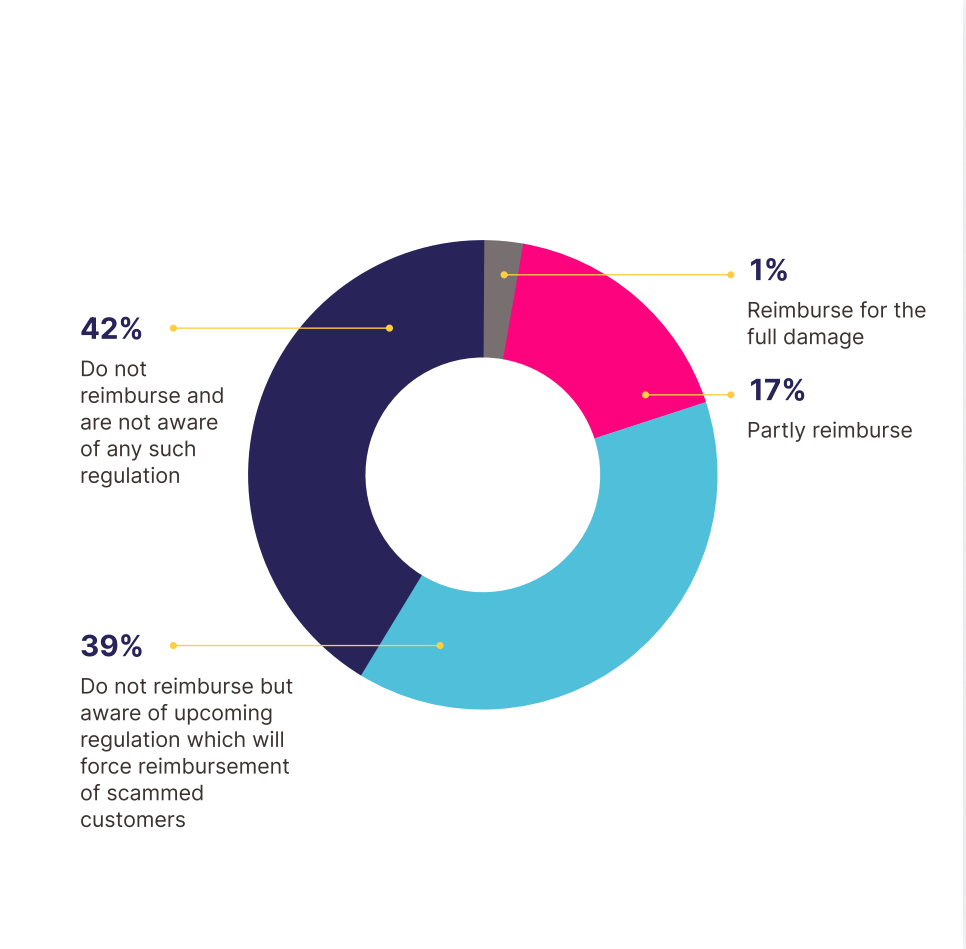


Figure 7: Reimbursement of Customer Scammed by Impersonating Sites

How much are businesses spending on treating the symptoms of impersonation fraud?

Putting a money-shaped band aid on the problem

Whether businesses reimburse customers directly, or whether they *only* have the costs of remediating an impersonation scam, the price of online impersonation is growing every year.

Over one third of businesses are spending up to a million dollars each year on incident remediation for website impersonation, and almost 5% are spending more than that.

Worryingly, 15% have no idea how much this issue is costing their business.

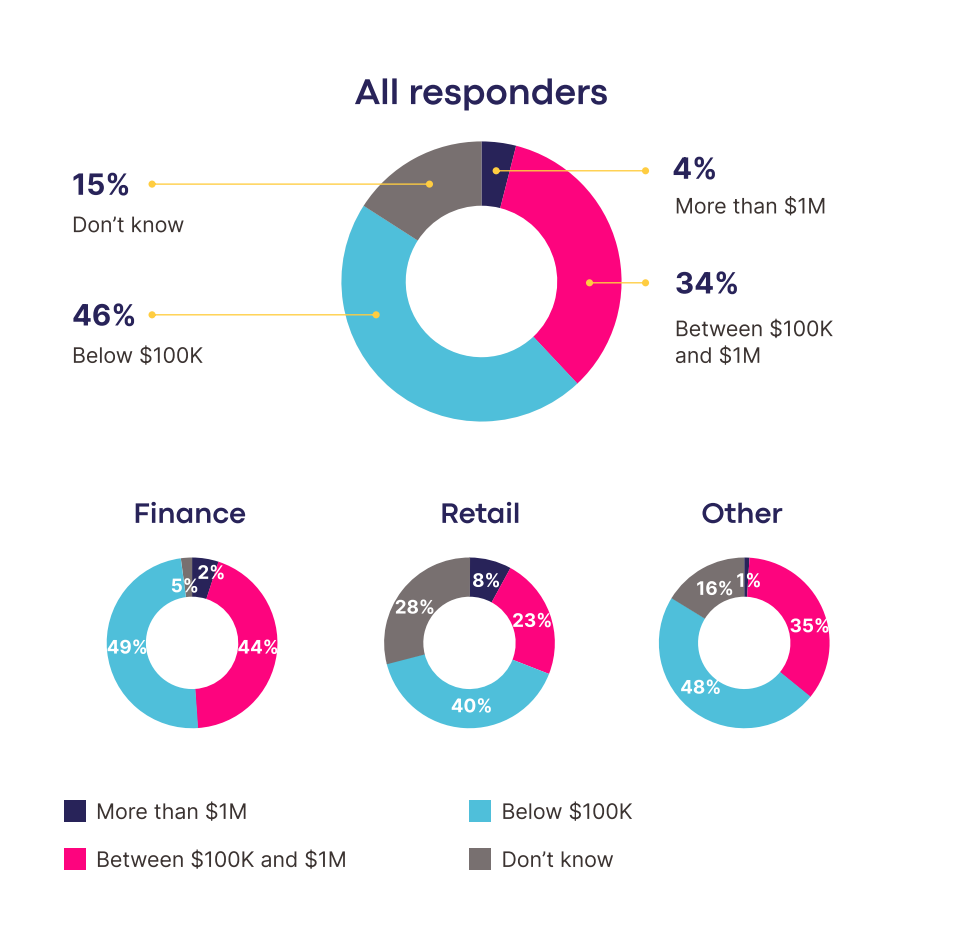


Figure 8: Costs Incurred in Direct and Indirect Compensation and Remediation of Customer Scams

How are customers responding after falling victim to website impersonation?

Most customers don't forgive and forget after being scammed

When customers have been scammed and experienced the consequences, just 22% will continue transacting as usual.

More common responses are explicitly demanding compensation (61%), expressing anger to CSRs (56%), or stonewalling communications (47%) – effectively devaluing marketing activities and adding to risk if critical correspondence is ignored. These are actually the best case scenarios.

At worst, 45% of customers will stop transacting with the business temporarily, and 40% will walk away for good.

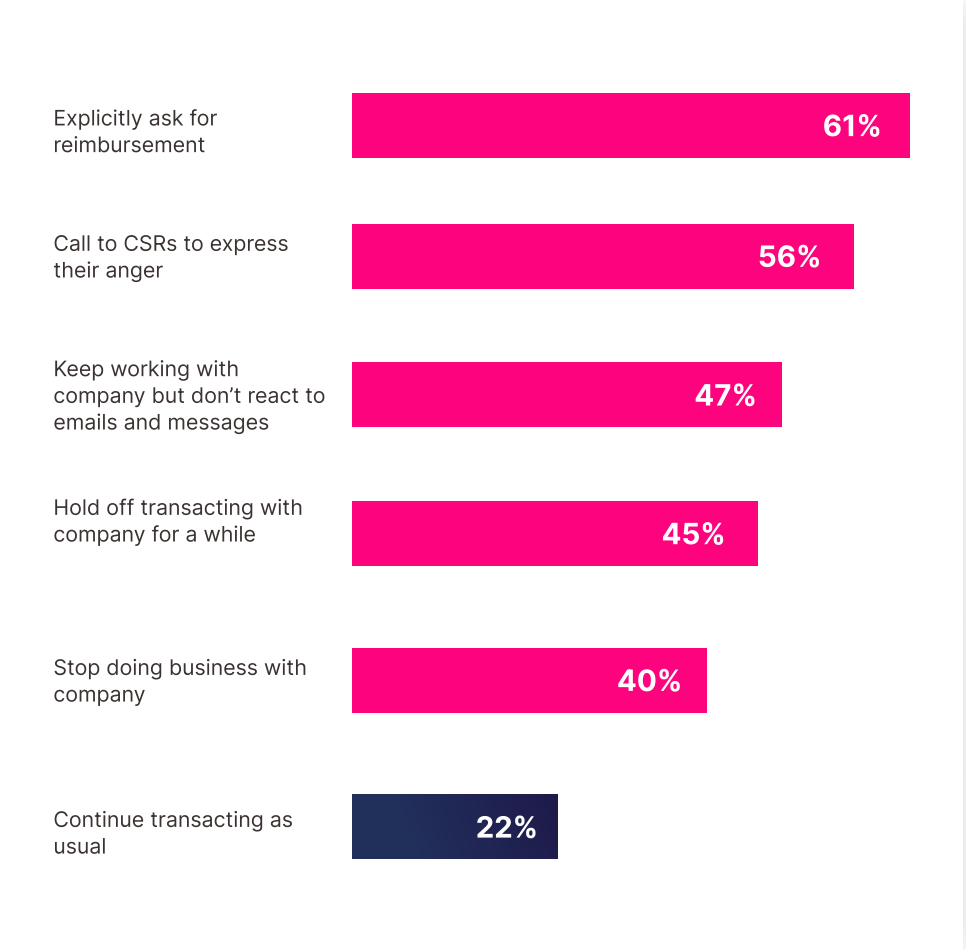


Figure 9: Customer Behavior After Being Scammed

How important do businesses consider having active protection from website impersonation?

Businesses want forensic attack visibility: yet it's still customers who raise the alarm

We asked respondents how far they agree with three statements on the value of attack visibility:

- To help protect against website impersonation
- To know which customers have been impacted
- To show customers that you're taking proactive care about their digital safety

All three were important or very important for at least 90% of businesses. No matter the motive, almost all businesses consider attack visibility to be important or critical.

Ask yourself – why is it still customers who raise the alarm?

If businesses have attack visibility so high on their list of priorities, why do we see in Figure 2 that the volume of customer-reported incidents across different channels outweighs those found by the business itself?

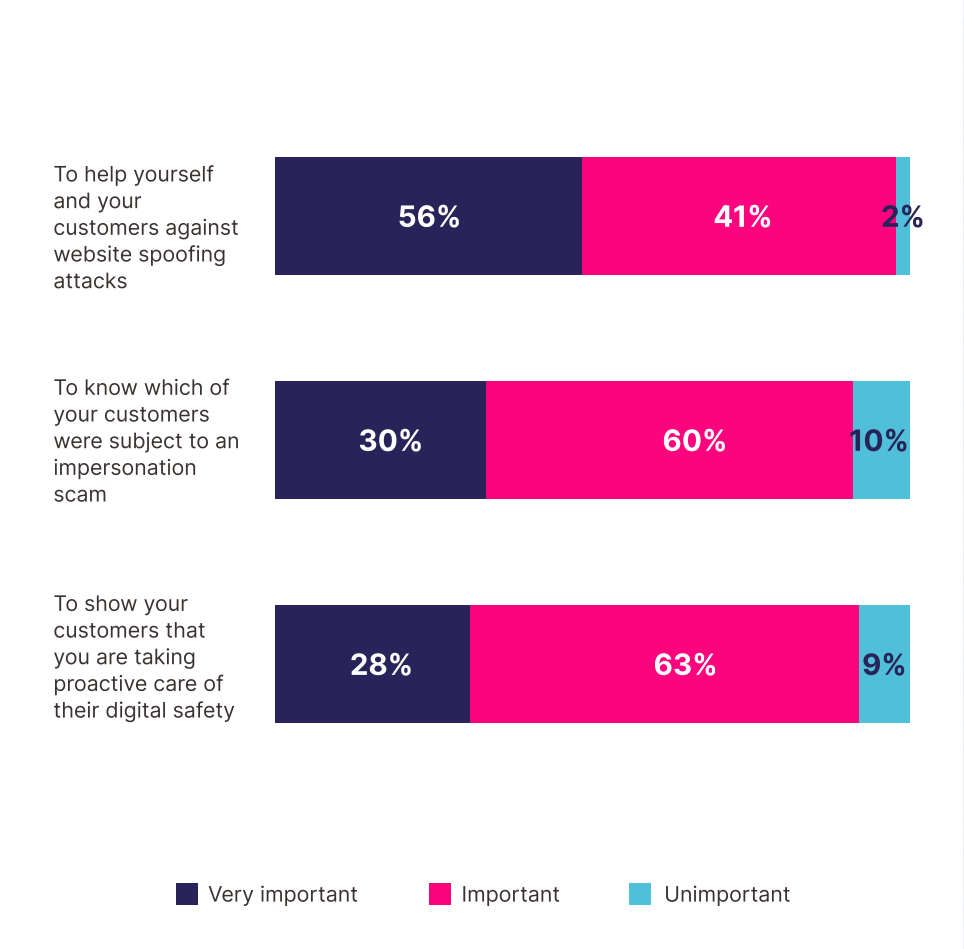


Figure 10: Importance of Customer Protection and Transparency

Which website impersonation solutions would businesses consider?

Businesses would largely say no to a solution that intrudes on their customers

Despite the desire for visibility and reducing risk, businesses are not willing to adopt website impersonation solutions that rely on the customer downloading an agent, as this would add friction in the relationship.

80% of respondents say they would not onboard technology that requires their customers to install software or an agent on their devices to protect against website impersonation.

The demand is clear – for effective, agentless solutions like Memcyco that can be rolled out and implemented without customer buy-in.

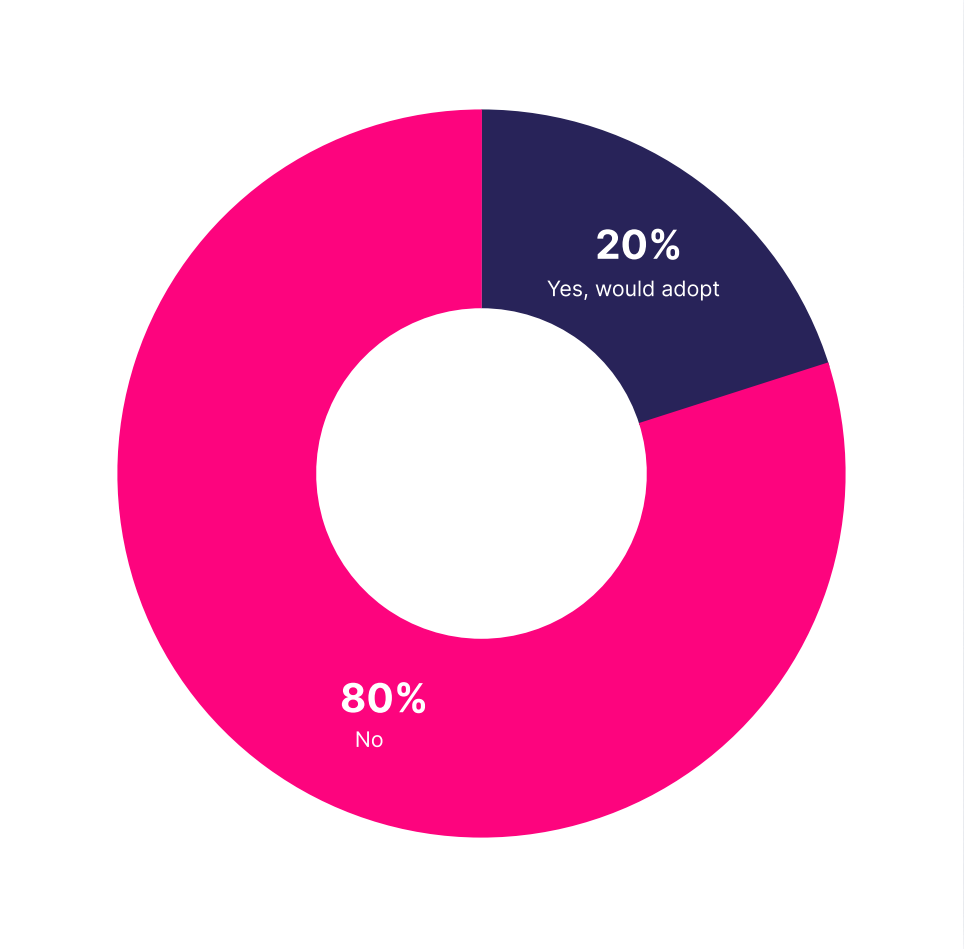
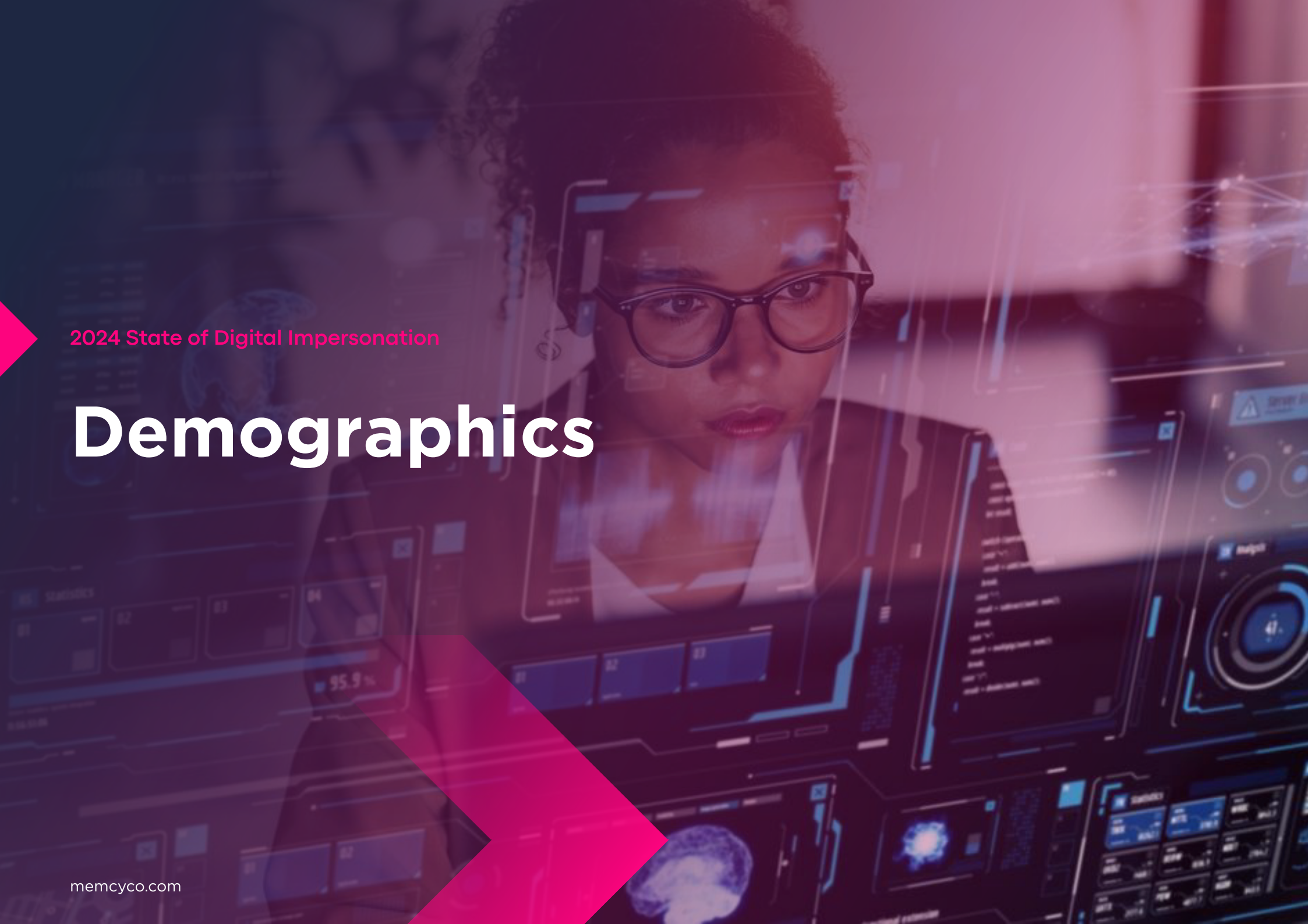


Figure 11: Adoption of a Solution that Requires Mandating Installation of Software by Customers to Protect them Against Impersonation Attacks.



2024 State of Digital Impersonation

Demographics

Demographics

Country, industry, company size, monthly online traffic, and job seniority

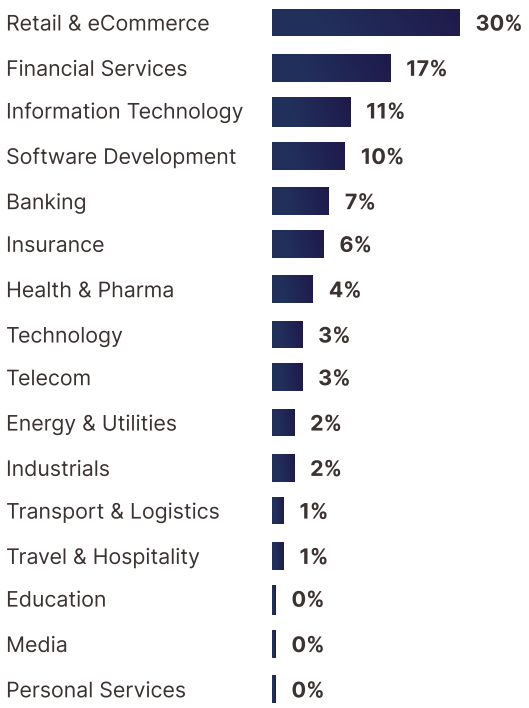


Figure 12: Industry

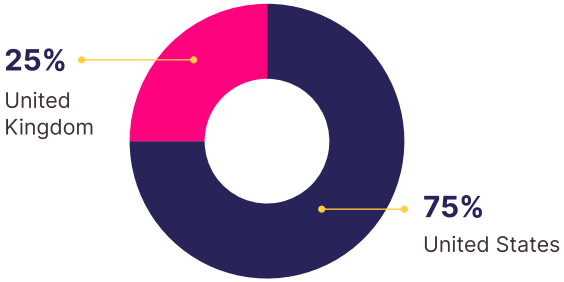


Figure 13: Country

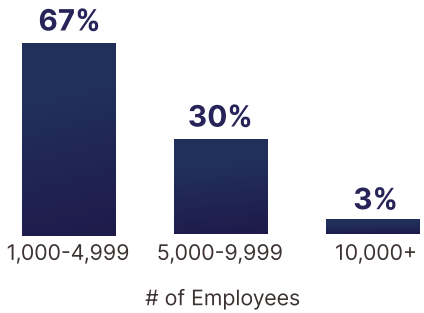


Figure 14: Company Size

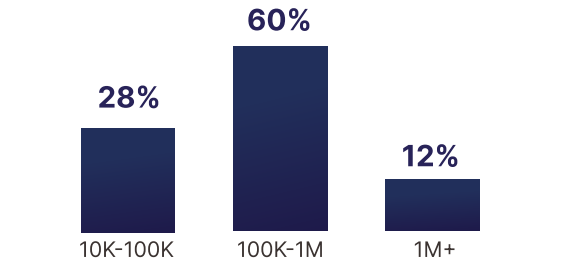


Figure 15: Monthly Online Traffic

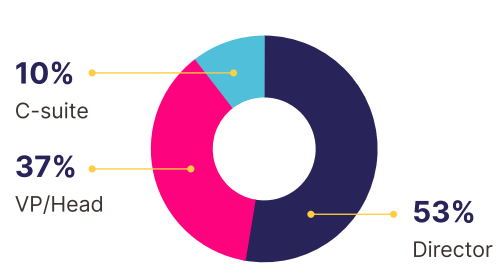


Figure 16: Job Seniority

Job function, and website content

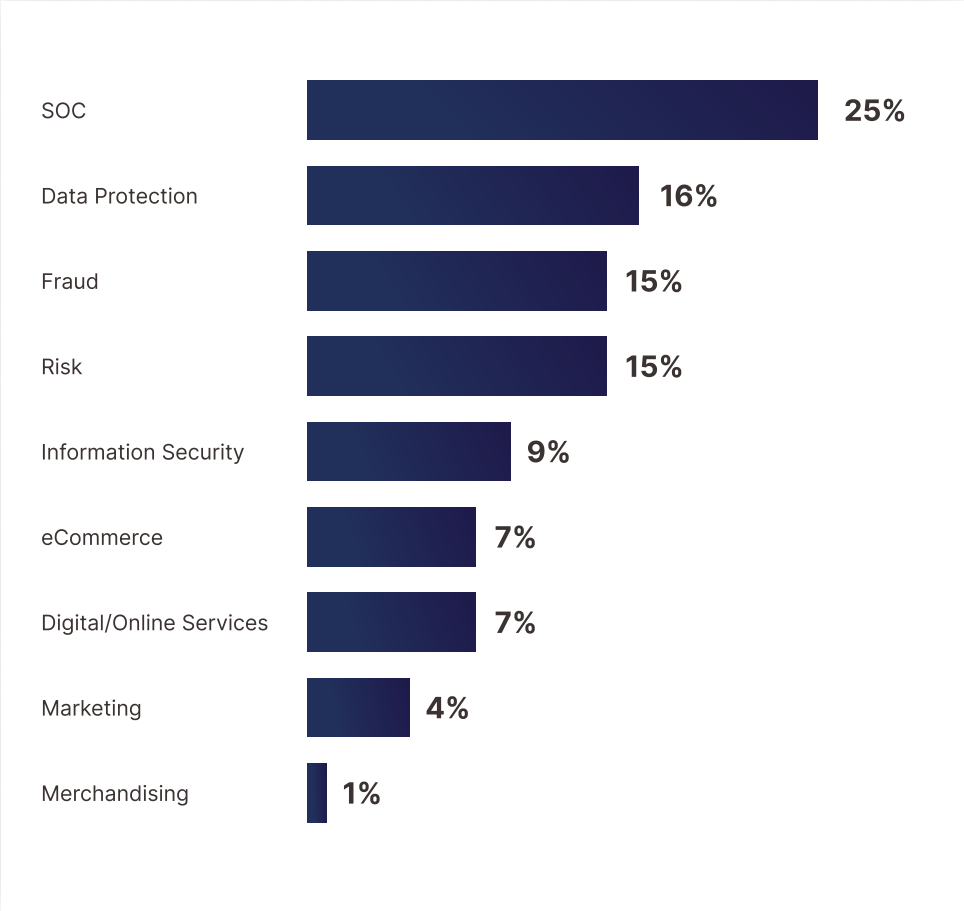


Figure 17: Job function

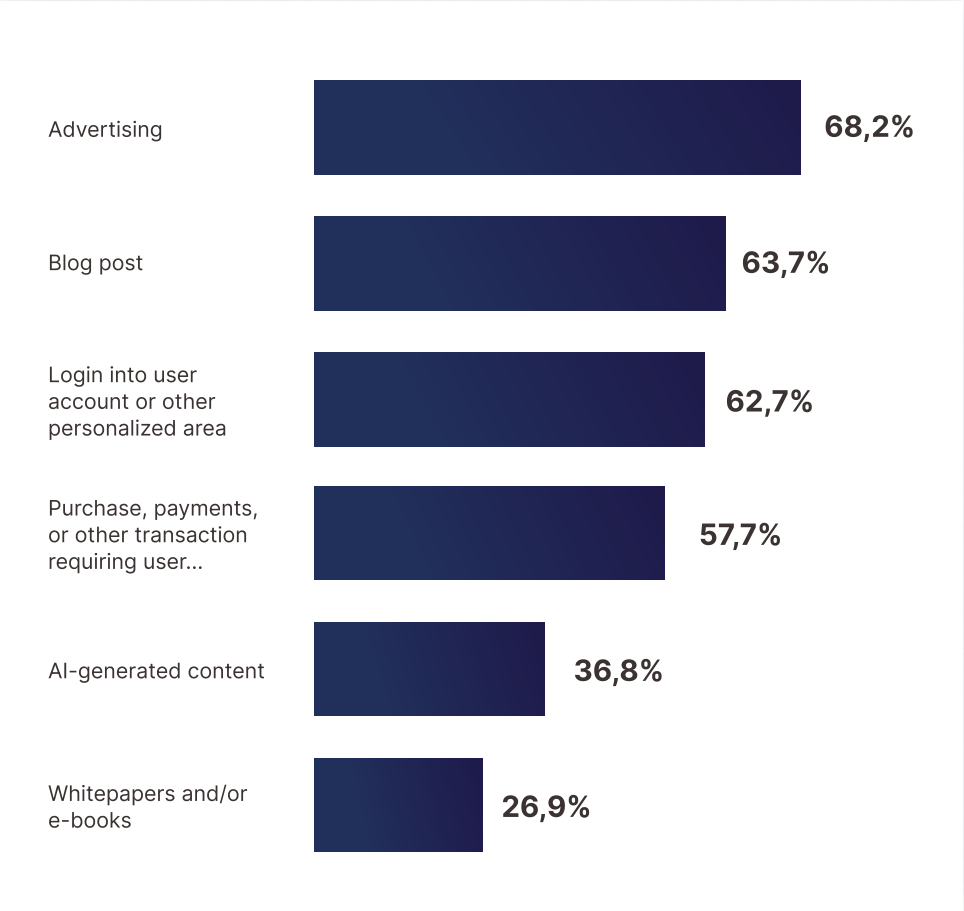


Figure 18: Website Content/Function

2024 State of Digital Impersonation

Gap Analysis

memcyco.com

GAP ANALYSIS

200 people answered this survey.

Just 6% with an in-place solution said it's 'effective'.
The only remaining question is...

What risk gaps does your digital impersonation detection solution leave wide open?

Fraud, Security, Risk – ask whoever you need to ask in relevant teams to get specific answers to the following questions.
By evaluating the answers, you'll be better-able to assess where you are in your maturity curve towards closing critical digital impersonation fraud risk gaps.

You'll also know which digital impersonation protection capabilities to look for when considering a replacement solution able to keep you two steps ahead of phishing-related website impersonation scams.

1 SOLUTION COVERAGE

Are you covering fake-site detection, protection *and* response? In one solution? Or across several?

Find out *if* and *how much* your organization is investing in three critical areas for effectively dealing with phishing-related digital impersonation attacks:

Detection, Protection and Response

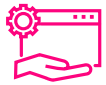
It may be that you have *some* or *most* of these capabilities, though they may be spread across different solutions, or departments.

If that's the case, or if you can prove you're over-investing in multiple solutions, you might want to consider streamlining investment with a single solution that offers:

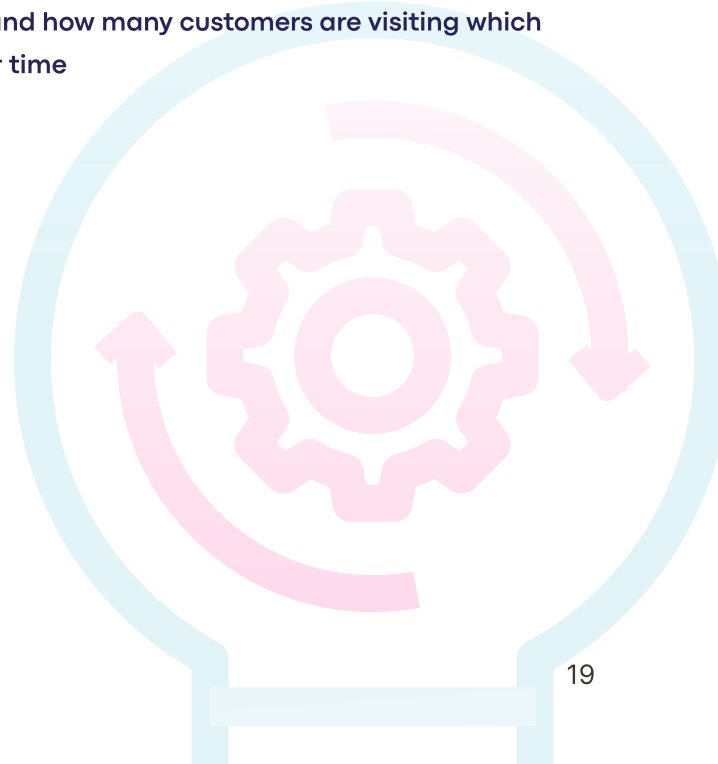
Real-time detection

For spotting fake-site reconnaissance attempts - of bad actors snooping around your site, to research your code with intent to impersonate it and launch a fake

For detecting new, fake URLs that go live, impersonating your site, without the risk and delay of active scanning



For gathering detailed intelligence (without significant effort) about website impersonation attack magnitude, individual scam victim identities, and how many customers are visiting which fake websites over time



2 SOLUTION COVERAGE

Real-time protection

For guaranteeing site authenticity to customers? Can you warn customers when they access fake sites impersonating yours

For knowing when customers click phishing/smishing links to fake sites. Or, the moment they attempt fake-site login, inadvertently sharing their credentials with fraudsters

For protecting customers from account takeover (ATO), even if they fall for phishing-related fake-site scams and have their credentials stolen

Remember, your customers are your biggest asset, but they're also the weakest link when it comes to phishing-related digital impersonation fraud risk.

Real-time response

For taking down fake sites promptly and protecting customer accounts from post-takedown ATO risk of stolen credentials being used in future attacks

For auto-blocking bad actors behind fake-site scams from customer accounts and your real website

For selectively allowing legitimate 'trusted-device access' to your website and user accounts

For leveraging attack forensic data (scope and magnitude) to enrich and improve fraud risk engine predictions and future response posture

Gather information from your Risk, Fraud and Security teams. It may be that you're operating a number of siloed solutions that individually benefit each team, but aren't combining to inform and optimize phishing-related fraud prevention strategies.

3 COST-BENEFIT ROI

How much are you investing in digital impersonation detection annually vs. incident handling costs?

Monitoring, takedown, response – digital impersonation detection solutions offer different capabilities and (needless to say) your annual subscription cost alone isn't an indicator of value. If you invest cheap, you'll get cheap outcomes.

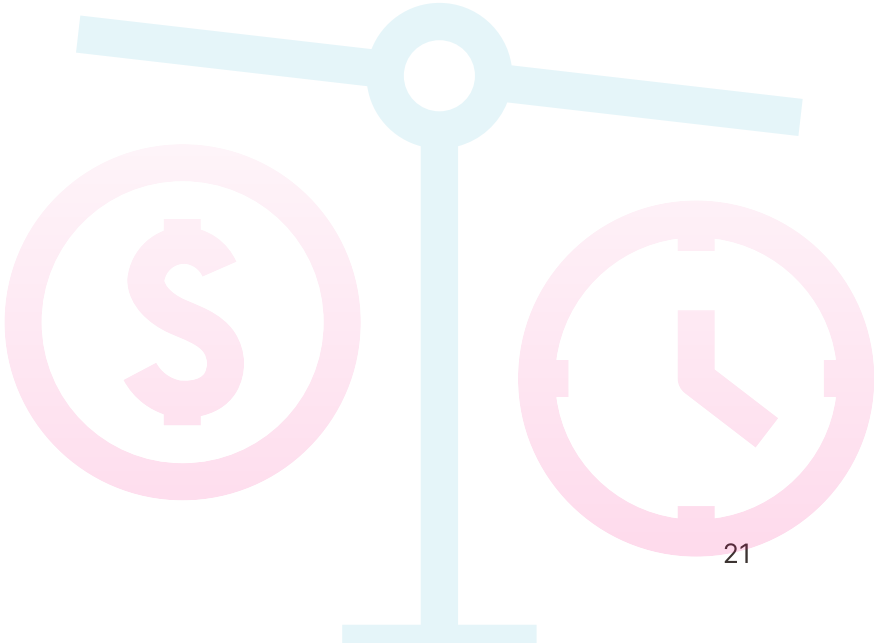
Try evaluating 'investment' vs. 'benefit' using calculable metrics like account takeovers (ATOs) that are among the most common outcomes of phishing-related digital impersonation attacks.

1. Find out your total annual ATOs
2. Calculate your incident handling costs per ATO
3. Multiply that by your annual ATO figure to get your total ATO cost
4. Now calculate how many ATOs your current solution actually prevents
5. Now you can work out your 'solution investment' vs 'savings' ROI

If your current solution doesn't significantly reduce incident handling costs, it's possible that it can't detect early, pre-attack signs for preventing phishing-related attacks and associated expenses.

Find out whether or not your current solution uses real time detection technology, instant protection, and auto-response capabilities to optimize ATO mitigation.

If the answer is 'no', then consider switching to a solution that includes those capabilities. The difference in annual ATO incident-handling savings could be millions.



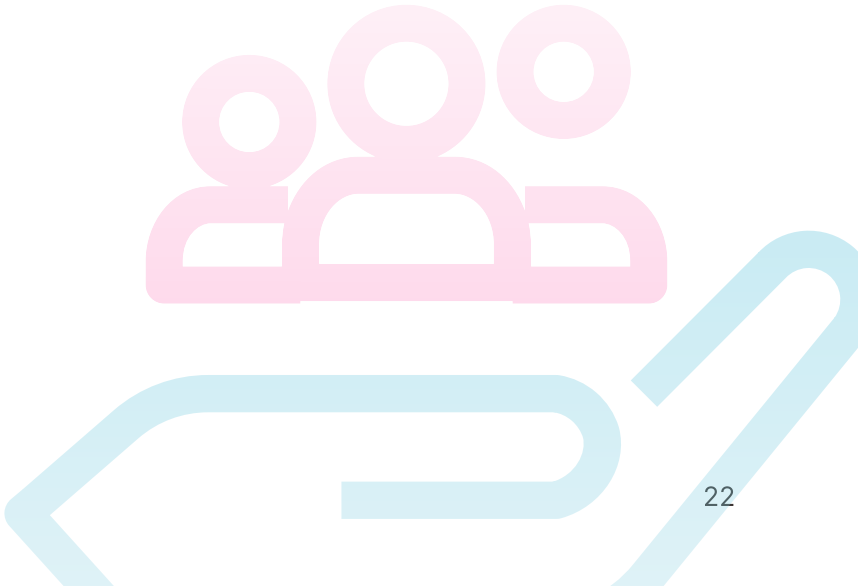
4 CUSTOMER COVERAGE

Does your current solution also protect your customers from falling for fake-site scams? Or do you over-rely on customers to be vigilant of scams?

Effective anti digital impersonation measures *must* safeguard not only your assets, but those customers. In other words, protecting business starts with protecting end-users. After all, customers are your biggest vulnerability when it comes to phishing-related scams.

Finding a digital impersonation protection solution that protects you and your customers is critical for maintaining customer trust that takes time to build, and a second to lose. With customers increasingly 'shopping around', loyalty is harder to gain and maintain than ever – and proving to customers that their data and assets are safe is a powerful way of stopping them going to your competitors.

The importance of protecting both parties cannot be overstated as the direct and indirect costs of phishing attacks (like customer reimbursement and legal fees) can be substantial.



5 'TAKEDOWN' SPEND

How much do you spend annually on takedown services? How much could be reinvested in more permanent root-cause solutions?

Investing in detecting and stopping digital impersonation attacks earlier, can be more cost-effective than fake domain takedown services that become expensive over time, while leaving post-takedown ATO risk gaps.

By gaining pre-attack digital impersonation visibility, you'll cap and control costs associated with incident response and customer churn.

You'll also safeguard (and even enhance) your market credibility as a secure and reliable entity customers and investors feel safe being associated with.

6 SOC TIME INVESTMENT

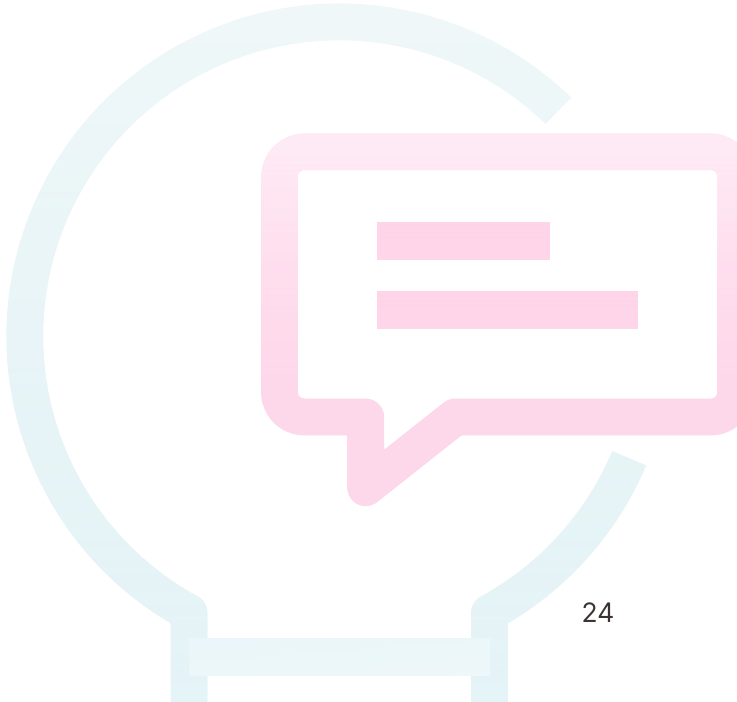
How much time is your Security Operations Center (SOC) investing on digital impersonation incident handling?

Investigation, takedown, customer communication – SOC teams spend a huge amount of time managing the aftermath of digital impersonation attacks.

Solutions able to automate early detection and response can help SOC teams reduce workload, while also preventing digital impersonation attacks form becoming ransomware or ATOs.

Digital impersonation protection solutions that offer real-time response also help SOC teams focus on strategic workloads like threat hunting, security architecture improvement, and advanced forensic investigations.

This shift from 'reactive' to 'proactive' SOC team behaviour does two things: first, it optimizes the use of skilled resources and, second, it enhances the overall security posture of the organization. In other words, by allowing the SOC team to stay in `proactive` mode longer, they can reduce post-incident firefighting and prevent more fraud incidents from happening in the first place.



2024 State of Digital Impersonation

Closing Thoughts

CLOSING THOUGHTS

Digital impersonation isn't just winning, it's reaching escape velocity

If smart technology is part of the phishing-scam problem, smarter technology needs to be part of the permanent answer.

Ultimately, businesses are highly aware of fake-site phishing fraud. But, the apparently unstoppable scale of the problem seems to cause a mindset of damage limitation as the only viable solution. As a result, consumers remain exposed and caught in the crossfire.

Worryingly, reliance on customers to detect and report fake-site scams seems to be the accepted standard – one that normalizes the damage done to customer assets and wellbeing.

With new regulations in many countries making customer reimbursement mandatory following scam-related financial losses, can businesses afford to keep normalizing customer impact as inevitable?

What's needed is a paradigm shift away from 'scanning/takedown' thinking, and customer education that both treat the symptoms, and not the cause.

Businesses can and should become better-empowered to continually and instantly detect fake-site scams in-the-making earlier, while protecting for longer.

It's not a matter of 'will'. Businesses just haven't found the right technology - but the right technology EXISTS.

ABOUT MEMCYCO

‘Instant visibility‘ digital impersonation protection you didn‘t think possible

Effortless, agentless, ‘scanless‘ digital impersonation protection

Memcyco offers a suite of AI-based, real-time digital risk protection solutions for combating website impersonation scams, protecting companies *and* their customers from the moment a fake site goes live until it is taken down.

The Memcyco difference

Memcyco‘s groundbreaking external threat intelligence platform closes the gaps even the most widely-used digital impersonation protection solutions leave wide open.

- **Finally get effortless attack-scope and magnitude visibility**
- **See the unseeable: of the attack, attacker, and each individual victim**
- **Prevent more ATO fraud, ransomware, and data breaches before they occur**

Memcyco‘s nano defender technology auto-detects, protects, and responds to attacks as they unfold, securing tens of millions of customer accounts and reducing the negative impact on workload, compliance, customer churn, and reputation.

Memcyco is 100% agentless. No need for customers to download apps or install software. Visit memcyco.com, book a demo and discover how Memcyco closes post-takedown risk gaps other solutions leave wide open

www.memcyco.com