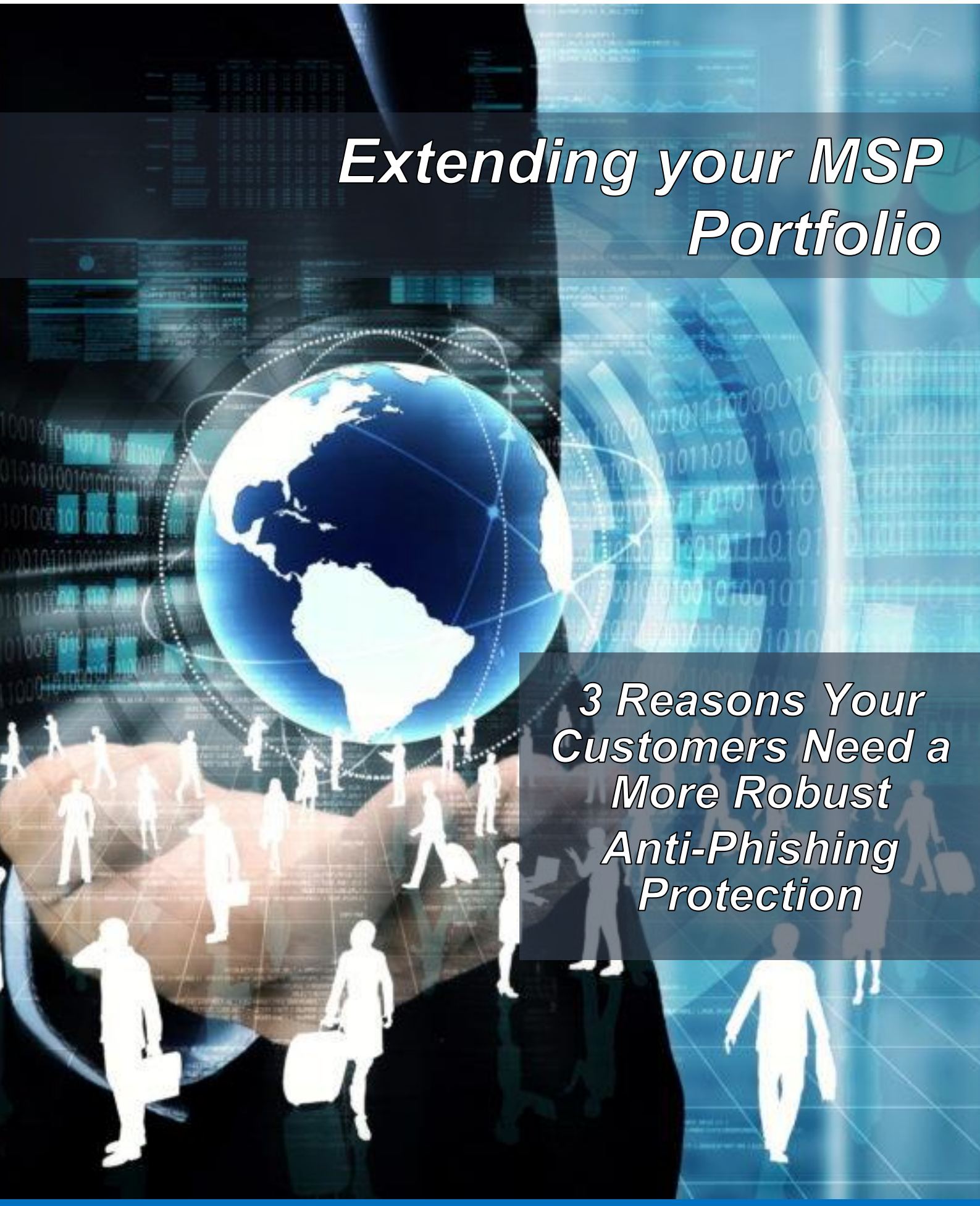
PHISHCLOUD
Empower People. Fortify IT.



Extending your MSP Portfolio

3 Reasons Your Customers Need a More Robust Anti-Phishing Protection

PhishCloud, Inc. 3250 Airport Way, Suite 534, Seattle, WA 98134

www.phishcloud.com

Let's talk about Fishing! No, not that kind, though we'd probably all like to be on a boat right now pulling in the big one! Let's talk about the number one threat to your customers today: PHISHING!

There are many different types of phishing attacks today, and list continues to evolve:

- Standard Email Phishing: en masse phishing emails
- Spear Phishing: highly targeted email phishing
- Whaling: phishing targeting high-level executives
- Smishing: SMS Phishing
- Vishing: Voice Phishing
- BEC: Business Email Compromise
- Clone Phishing: Email phishing from a compromised email account
- Evil Twin Phishing: Duplicate fraudulent website phishing
- Social Media Phishing: Social Media post phishing
- Search Browser Phishing: Fraudulent website phishing
- And more . . .

Yet most companies focus **only** on email protection with no visibility into the risk associated with phishing attacks in social media, web browsers and search engines, and corporate messaging applications. Focusing on email only creates a significant gap in your defense-in-depth security architecture and leaves your company at risk.

Phishing is now the primary attack vector in 80 percent of security incidents. 85% of global companies have been attacked with an average cost per breach of $4 million dollars, and 74 percent of attacks in the US were successful, 30 percent higher than the global average. And phishing attacks are on the rise, up 47 percent in Q1 of 2021.

If you are not delivering a robust anti-phishing service to your customers today, or you're using one of the many products that focus on email only, you are ignoring a significant gap in your customer security posture. Let's look at three reasons you need to deliver a more robust anti-phishing service to your customers.

1. Email Phishing Attacks are Still Successful

Despite secure email gateways and services that block 98% of bad email (1.2 trillion phishing email per year), 50 million bad emails get through every day. Of those that get through, 5 to 15 percent of these are opened, and malicious links are clicked. Hard working employees with no ill intent are putting your company at risk because they, through lack of training, lack of focus, or lack of concern do not know how to spot a phishing attack. This problem is compounded when you add on web browser, social media and messaging app attacks that can be significantly harder to spot.

Email phishing remains the number one attack vector for ransomware, the most prominent malware threat. There are over 4000 ransomware attacks daily in the U.S., resulting in significant loses for those organizations affected. An additional layer of protection is needed to make sure both IT and employees have visibility into phishing attacks so that risk is mitigated.

2. Email is Not the Only Phishing Attack Vector

Today there are 75 times as many phishing sites as there are malware sites on the internet – let that number sink in! Compromised email, web pages and social media accounts can mimic safe links or files. URL redirection and even SSL encryption are luring employees to phishing sites and successfully getting their credentials. Social Media attacks are now 23.6 percent of all attacks, up from 11.8 percent inQ4 of 2020. According to Google, there were 40 billion pages of spam detected every day in 2020, a 60% increase from the previous year. These 40 billion pages included hacked sites, deceptively created sites, and other forms of web spam, scams and fraud. It's clear that providing email phishing protection is NOT enough! Your customers need a more comprehensive solution to stop phishing attacks from all threat vectors.

3. Employees are the Weakest Link

From the moment the first email was sent, phishing has been a top security concern for one primary reason: it targets the weakest link in the security chain – PEOPLE! And

phishing is a top concern for good reason: 97 percent of users are unable to recognize a sophisticated phishing email. Regardless of how robust your security training program is, 20% of all employees are likely to click on phishing links, and 67.5 percent go on to enter their credentials or other data requested. Clicking on links has become second nature, thanks to social media, and threat actors are continuously looking for ways to fool users into a response. Employee training, though not a silver bullet (which does not exist), is an important part of your overall security architecture. In fact, when properly trained, 82% of employees reported a phishing email within an hour of receiving it. Unfortunately, most training is high level awareness training and does not delve deeply into the myriad of ways one can spot a phishing attack, making your training program ineffective. And only 10% of companies spend more than 3 hours per year on this vital training. With the stakes this high, those on the front line should not be so ill-prepared. Your customers need the ability to deliver real-time visibility as well as training based on the type of malicious event the user sees or clicks on, improving the ability to spot and avoid a malicious link.

A Human Approach to Anti-Phishing

Tools that focus on email alone are creating a blind spot for your customer's IT security administrators who have no visibility into emails that make it through gateways and filters, or malicious links that are clicked in web browsers, social media post and messaging apps. With no visibility, they cannot block an attack, properly triage an attack, or understand what kind of malicious content your users are encountering daily.

You need to take a different approach – a human approach. You need a solution that clearly identifies malicious, suspicious, or safe content – like a traffic light - in email, web browsers, social media and messaging apps, so your customers know what they can and cannot click on, and so they can block a threat before it's clicked. You need a solution that gives your customer real time visibility into malicious content that is being viewed or activated so you can respond in real time and focus on only the most critical events. And you need a solution that delivers real-time training based on what malicious content is being viewed by your users, making sure they are properly trained to spot the threats before they put their company at risk.

What if you could offer a cloud-based service to your customers that delivers employee visibility as simple as a traffic light - green for safe, yellow for suspicious, and red for malicious content – so that your customers could make the right decisions and avoid malicious content?

What if you could offer your customers complete visibility into suspicious or malicious activity so that their IT security administrators could automatically block bad links from being clicked, with proactive threat attribution and contextual event data, so you know who, what machine, when, etc.?

And what if you could deliver this multi-tenant, 24/7 security service without any capital outlay, without the need for additional resources, and without having to acquire high-end security intelligence, all the while preventing phishing risk for your customers and closing yet another gap in their security posture.

Now you can empower both your customer and their IT and Security teams to:

- Avoid risky clicks with intelligent, traffic-light-style visual indicators that clearly identify safe, suspicious, or malicious content in email, web browsers, social media and messaging apps.
- Automatically block malicious content before it can do damage.
- Significantly reduce the time to risk prediction, incident prediction, and incident response with real-time attribution reporting
- Take advantage of machine learning and AI technology that protects your users from threats seen across the globe
- Integrate data streams with your existing tools and workflows, including SIEM platforms.
- Reduce risk across multiple email, browser, social media and messaging app platforms.
- Deliver targeted training to employees, in real-time, based on malicious content seen, so that they are trained to spot malicious content.

So, if you want to provide the most comprehensive phishing protection on the marketing today, there's only one way add this capability to your existing portfolio: **PhishCloud!**

About PhishCloud

PhishCloud, an IT Security Services company, makes people a key ingredient of your security architecture, not the weakest link, giving IT both visibility and confidence in how their people work every day. PhishCloud provides tools that empower people to make intelligent decisions on digital phishing threats, fortifies IT visibility so they can quickly respond to that threat, and delivers targeted education to reduce the risk of phishing attacks.

Founded in 2018 and headquartered in Seattle, WA, PhishCloud delivers comprehensive visibility into phishing attacks across all digital threat vectors, including email, web, social media, and messaging apps – not just email – so that IT can respond to and block phishing threats that people see in real time. PhishCloud then delivers training based on what your people see so that training is targeted, meaningful and teaches your people their role in your security architecture.

PhishCloud. Empowering People. Fortifying IT.

For more information, visit **http://www.phishcloud.com/**.