PHISHCLOUD
Empower People. Fortify IT.

GROWING MSP REVENUES

3 Reasons to add PhishCloud to your MSP Portfolio

Revenue growth is a common problem with MSP's, large and small. How to you attract new customers and expand your customer base? How do you expand within your existing customer base with new offerings that generate additional revenue per customer? Very few MSP owners and executives are happy with their current revenue growth and are looking for ways to extend the revenue curve.

The current MSP market for small and medium sized businesses is approximately $50 billion. For MSSP's focused on delivering cyber security solutions to their customers, choosing the products they will use in their security architecture from a glut of point products is a daunting task as few provide comprehensive protection for any cyber attack vector.

Phishing, the number one attack vector for cyber criminals today, is an area that lacks comprehensive coverage from any one vendor – until now. If your MSP portfolio does not offer phishing protection, or offers only protection from email phishing attacks, there are 3 reasons you need to add PhishCloud to your MSP portfolio!

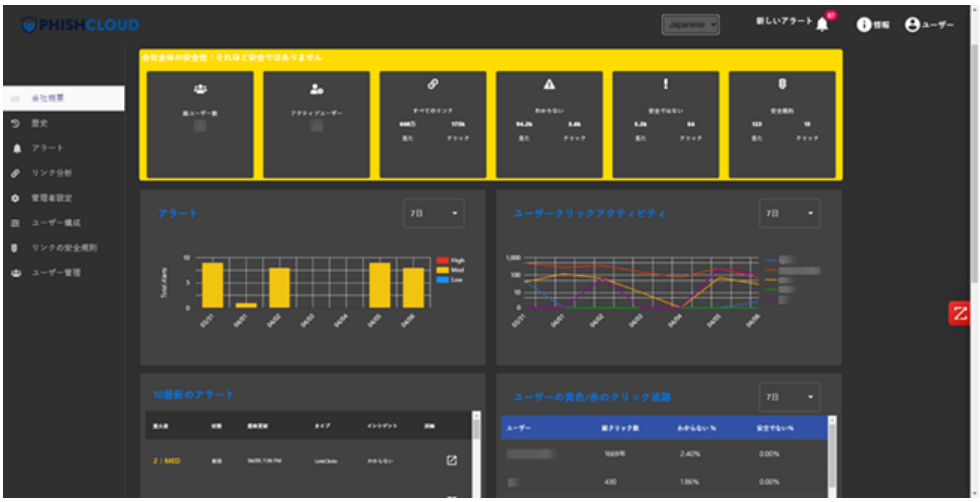
1 Phishing is NOT just an email problem!

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.

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.

IT HAS NO VISIBILITY INTO WHAT THEIR USERS CLICK ON!

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, 25% 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.



While more than 80 percent of companies have a process for employees to report phishing emails, less than 25 percent of malicious or suspicious emails are actually reported. Some tools make it easy for users by providing a button to report suspicious activity, but this approach still relies on the knowledge of the user, something we'll address in the 3rd reason to add PhishCloud to your MSP portfolio.

IT has no visibility into what their users are seeing and/or clicking on, and by the time it is reported, if it is, the damage is done. This lack of visibility is compounded by phishing attacks in social media, web browsing and search engines, and corporate messaging applications. IT needs the ability to see what malicious or suspicious links their users encounter, across all digital platforms, so that they can take action to mitigate risk.

3 Training and Simulations aren't working!

Despite the awareness training and simulations that companies employ, 97% of users are unable to recognize a phishing email, especially as those attacks become more sophisticated. 20% of employees will click on phishing links and two thirds of those will enter credentials and other data into fraudulent web sites. This is a direct result of the fact that only 10% of companies spend more than 3 hours in cyber security training per year, and that training is typically high level. And only 60% of companies provide formal education. The remainder rely on newsletters, bulletins, videos, and user reporting to make their employees "aware." Unfortunately, this awareness does NOT arm employees with the ability to spot and avoid phishing attacks.

Though well intentioned, phishing simulations can often have a negative effect on employee morale, especially when not paired with effective, reality-based training. Many companies today are using the "name and shame" approach to force compliance in their user base. The Consequence Training Model is gaining traction as companies look to punish users who regularly fall for phishing attacks. Consequences can range from additional in-person training to monetary penalties to termination. These measures, however, can be counterproductive. According to John LaCour, founder and CTO of PhishLabs, "It (simulations) really demotivates people, and it doesn't really teach them anything about how to be more diligent about phishing attacks. He further explained, "each phishing simulation program needs to be accompanied by a robust training program, where you teach employees what to do when they see something "phishy." Otherwise, it just creates resentment among employees."

PhishCloud – Designed for MSP's

You need a phishing solution that clearly identifies malicious, suspicious, or safe content, in email, web browser, social media and messaging apps, so you can block a threat before it's clicked. You need a phishing solution that gives you and 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 phishing 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 sink you.

What if employee visibility were a simple as a traffic light - green for safe, yellow for suspicious, and red for malicious content – so that your users could be a step ahead to make the right decisions and avoid malicious content?

What if you could deliver complete visibility into suspicious or malicious activity so that you could automatically block bad links from being clicked, and full attribution of phishing clicks within minutes, so you know who, what machine, when, etc.?

And what if you could deliver reality-based training to your users based on the type of malicious activity, they see so that training is specific and real time?

Now you can empower both your employees and your 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, reality-based training to employees, in real-time, based on malicious content seen, so that they are trained to spot malicious content.

PhishCloud was built for MSP's and MSSP's, making it easy and profitable to add to your portfolio:

- Our **Multi-tenant** management console let's you manage your customers independently.
- Our cloud-based service requires **no up-front infrastructure costs**, making it simple to add to your service architecture.
- We never collect or store data, so we are **GDPR/CCPA compliant**.
- We deliver **real-time metrics and reports** so you can respond to threats as they happen.
- Enjoy a **strong monthly/annual reoccurring revenue** stream with opportunity to add on additional service offerings.
- We **integrate with your business**, not vice versa.

PhishCloud provides the most comprehensive phishing protection and reality-based training available in the market today, all in one, easy-to-manage platform. Learn more at www.phishcloud.com.

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/**.