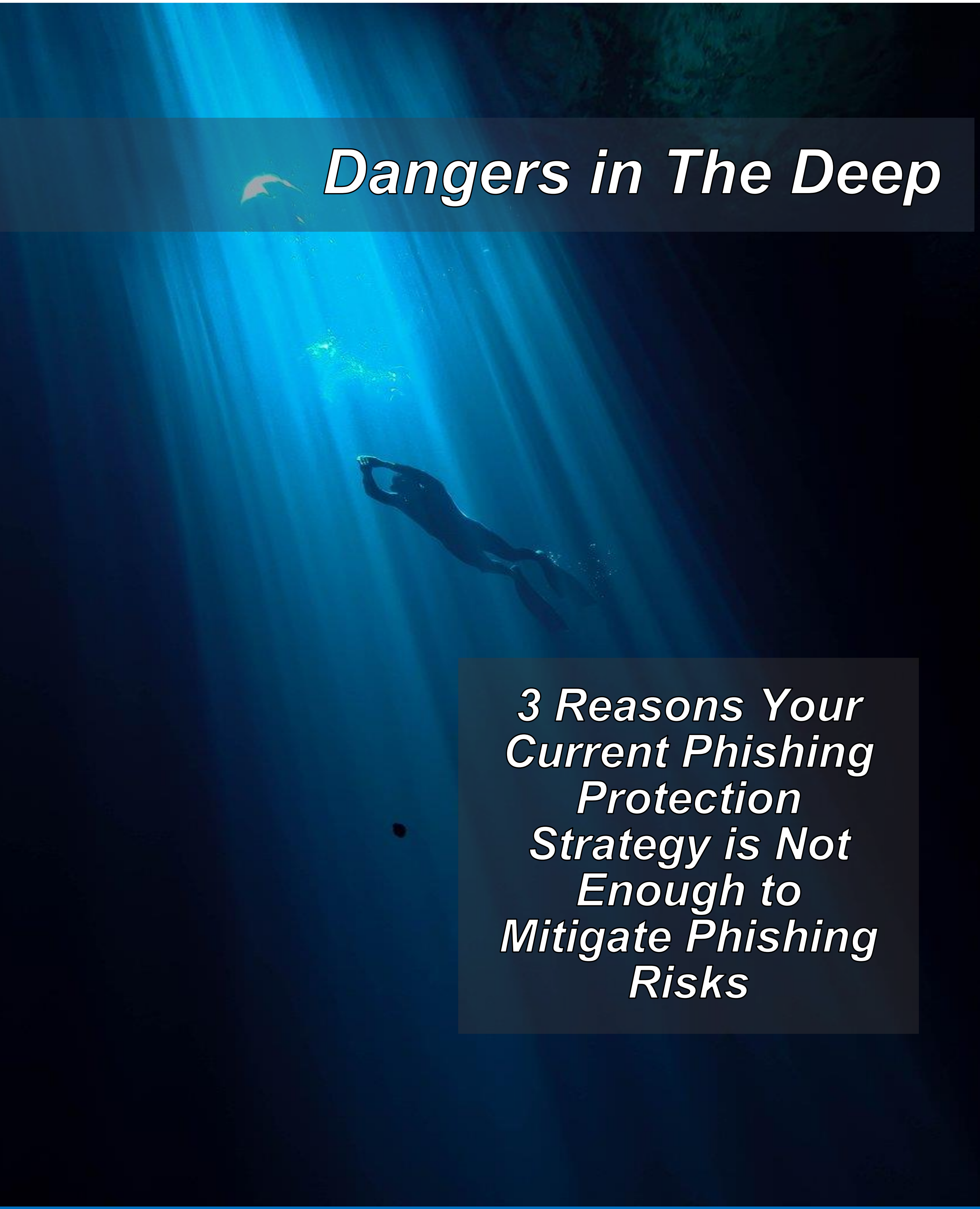

Dangers in The Deep

3 Reasons Your Current Phishing Protection Strategy is Not Enough to Mitigate Phishing Risks

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. Despite your significant investment in security tools and training programs, your business risk remains the same!

Many organizations focus only on email phishing attack prevention, and while email continues to be the primary source of phishing attacks, web browsing and search engines, social media and even corporate messaging application attacks are on a significant increase. Attacks are becoming more sophisticated and targeted, making it even harder for your employees to recognize malicious messages, files, and links.

To make matters exponentially worse, phishing attacks are on the rise, up 47 percent in Q1 of 2021, according to PhishLabs. 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 while large companies are not immune, it is the small and midsized business that are the primary target, considered low hanging fruit as they often lack the infrastructure or resources to defend themselves properly against attacks

The attacks are constantly evolving to thwart security defenses and employee training programs. Unfortunately, many organizations rely on employee training and phishing simulation programs, which are simply no longer sufficient to keep employees and your organization safe. Let’s look at three reasons that your current phishing protection strategy is simply not enough to mitigate phishing risks in your environment.

1. Clicking on Links is Second Nature

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. Clicking on a phishing link may also install malware onto the device to monitor and steal your data. Phishing links don't just target individuals but can be an attempt to compromise a company's network and secured data. If an employee clicks on the link, attackers can potentially access the whole network.

Today there are 75 times as many phishing sites as there are malware sites on the internet – let that number sink in! Compromised email 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. Email gateways and filtering tools block emails that match known signatures, but as techniques evolve, emails get through. Your employees need clear, highly visible and real-time indicators of which links in their email, web browser, social media or chat are malicious, suspicious, or safe.

2. Limited or No Visibility into Phishing Threats

Unfortunately, only 3% of users report phishing attacks, which means IT has no visibility into the true level of risk and the possibility of an ongoing attack. When an attack happens, IT administrators have only minutes to react to prevent data exfiltration, extortion or destruction. The vast majority of ransomware is delivered via phishing email campaigns and, once infected, 1000’s of files can be lost within minutes. But there are many different type 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 . . .

Sadly, only 48 percent of companies confirm they have continuous visibility into phishing/web attacks (Balbix). IT administrators need not only visibility into the phishing attempts that their users are seeing but they also need the ability to block the execution of those attempts – stop employees from clicking – before the damage is done.

3. Inadequate Training Makes Employees Your Weakest Link

Employee training, though not a silver bullet (which does not exist), is an important part of many companies' overall security strategy. 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.

You need the ability to deliver real-time training based on the type of malicious event the user sees or clicks on, improving the ability to spot and avoid a malicious link. According to Ponemon, only 39% of OT organizations surveyed had adequate staffing in their security team to scan vulnerabilities in a timely manner. And if you aren't conducting regular cyber security training that keep your employees equipped with the knowledge and expertise they need to recognize risk, you are opening your company up to numerous forms of risk:

- **Legal Risk**: compliance regulations com with their own penalties, and some are quite severe.
- **Financial Loss and Cost of Remediation**: data breaches can result in significant financial loss that can spell the end of the company.
- **Intellectual Property Loss**: data theft, include trade secrets, can result in loss of competitive advantage, market share, and the revenues associated.
- **Physical Risks**: downtime of critical assets, whether in manufacturing or utilities, can put businesses, consumers, and employee lives at risk.
- **Repeat Targeting**: once breached, an organization is likely to be breached again, often by the same attackers.

- **Lost of Customer Trust**: reputational damage can result in the loss of both current and prospect customers, impacting revenues. And once trust is lost, it's difficult to rebuild.

You Need a Different Approach to Phishing

Despite secure email gateways and services that block 98% of bad email, 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. Employees need to be empowered with intelligence to make the right decisions.

Tools that focus on email alone are creating a blind spot for IT 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, you cannot block an attack, properly triage an attack, or understand what kind of malicious content your users are encountering daily.

And if you can't see what your users are seeing, you can't deliver the right training to make sure your users are educated on the why and how of a specific phishing attack. Employees must learn to recognize common threats and be acutely aware of their role in defending against those threats, and the impact it can have on the company if they fail to do so.

The only way to address these issues is to take a ***different approach*** – a human approach. You need a 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 solution that gives you 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 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 had 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 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 training to employees, in real-time, based on malicious content seen, so that they are trained to spot malicious content.

If your goal is to empower your users to make the right decisions about suspicious and malicious content, gain the visibility you need to mitigate phishing threat to improve response, and educate your users to spot all phishing threats, there is only one way to accomplish all three: **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/**.

Disclaimer. All product and company names herein may be trademarks of their respective owners. The information and content in this document is provided for informational purposes only and is provided "as is" without any warranty, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. PhishCloud is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, PhishCloud makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. PhishCloud makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document. If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as possible.