PhishMe Intelligence™

HUMAN-VETTED, PHISHING-SPECIFIC THREAT INTELLIGENCE

PhishMe Research determined that ransomware accounts for over 97% of all phishing emails in 2016. With such alarming numbers, how do you prevent your enterprise from becoming another statistic? PhishMe Intelligence provides accurate and timely alerts to strengthen your organisation's ability to quickly identify and respond to phishing attacks in progress.

Our Solution

PhishMe Intelligence is the leading cyber security service designed to help enterprises stop dangerous malware and phishing attacks. We use proprietary methods to automatically identify top threats to your enterprise, and provide you with timely actionable intelligence, tools, and coaching to respond to attacks that would otherwise go undetected.

Email attacks are the primary mechanism to deploy malware into enterprises, either directly or indirectly. Phishing emails with malicious attachments or links continue to be able to bypass most organisations' security stack and reach the end user.

Most security vendors wait until a threat is at your doorstep before they analyse it and declare it as malicious. This typically involves waiting until a certain number of customers report a suspicious file or endpoint systems pass information back up to the vendor. Consequently, there is a delay between when an attack is launched and when your enterprise finally has reliable information about it. Since each threat is investigated in isolation, all threats are reported as equals without any context about the attack or related attacks.

As a result of this approach, security experts do not have the threat intelligence to disrupt the attack or prioritise threat response.

PhishMe takes a fundamentally different approach in identifying threats as they emerge daily—before your network gets hit.

We receive more than a million messages daily from a wide variety of sources. Attacks are automatically dissected to determine relationships between them. Our unique clustering algorithms sort malicious emails based on a number of factors and watch for new and emerging threats in the form of emails containing dangerous links and/or attachments. Once a new threat cluster is identified, its characteristics are documented and updated in our threat repository.

Payloads for each confirmed phishing campaign are analysed using proprietary methods to determine nature of each threat. This information is then updated in our data mines for additional analysis across campaigns and time-frames. Threat intelligence derived from this analysis is published in multiple formats for your security teams and security infrastructure to consume and appropriately respond.

This proactive approach of threat analysis enables you to prime your existing security infrastructure to disrupt these potentially nefarious attacks. Attack tactics used to penetrate your network are also exposed along with the relationships between phishing campaigns and Indicators of Compromise (IOCs). The combination of actionable threat intelligence and understanding the correlation between phishing attacks and their motivators helps your team prioritise, investigate, and respond.

Key Benefits

- ✓ Timely, Accurate, and Actionable Phishing Threat Intelligence
- ✓ Consumable Phishing Threat Intelligence
- ✓ Expert threat analysts to help operationalise threat intelligence and provide guidance
- ✓ Attack analysis and context to help make rapid, informed decisions

PhishMe's unique security intelligence gives you the weapons you need to identify, block, and investigate threats hitting your enterprise daily. This precise information is available in multiple forms for your teams to prepare and respond to active attacks to your network.

- **Human-readable threat intelligence reports provide deep-dive and trending analysis of your biggest threats. These reports include our expert analysis of the attack methodology.**
- **Machine-readable threat intelligence (MRTI) that can feed directly into security devices and threat repositories. Firewalls, IDS/IPS, SIEM can now detect and block emerging threats at the earliest stages of the attack.**
- **SaaS investigation apps to investigate phishing and malware attacks. These on-demand tools provide the latest insight on which attacks are related and how the attacks are being executed.**
- **Expert guidance from PhishMe's world-class security team to help your team implement best practices to reduce threats against your network.**

> We process PhishMe reports first because we know if you're reporting it, it's bad. PhishMe Intelligence is the most accurate phishing threat info we receive and it's easy to consume.
>
> **Threat Analyst at a Large Financial Organisation**

PhishMe's Intelligence service is actionable because it is:	
Consumable	PhishMe Intelligence delivers threat intelligence in multiple forms. Machine-readable threat intelligence (MRTI) follows industry standards for quick integration with your existing security devices. Analysis reports in PDF and HTML format are optimised for threat analysts and incident response teams.
Reliable	PhishMe Intelligence only notifies customers about confirmed threats that are vetted by our trained analysts, resulting in high-signal intelligence.
Timely	MRTI is published throughout the day as new attacks are confirmed. Strategic analysis reports are published weekly. The investigation app is available 24x7x365.
Fresh	PhishMe Intelligence service derives threat intelligence from a variety of sources of malicious email and spam that are used to deliver dangerous payloads to your employees every day.
Contextual	PhishMe Intelligence publishes threat intelligence that shows how individual elements of an attack are related and the relationships between seemingly disparate attacks.
User-friendly	We will help you operationalise the service and provide on-going support to make sure you are getting the most from the service.

PhishMe is the leading provider of human-focused phishing defence solutions for organisations concerned about their susceptibility to today's top attack vector — spear phishing. PhishMe's intelligence-driven platform turns employees into an active line of defence by enabling them to identify, report, and mitigate spear phishing, malware, and drive-by threats. Our open approach ensures that PhishMe integrates easily into the security technology stack, demonstrating measurable results to help inform an organisation's security decision making process. PhishMe's customers include the defence industrial base, energy, financial services, healthcare, and manufacturing industries, as well as other Global 1000 entities that understand changing user security behaviour will improve security, aid incident response, and reduce the risk of compromise.

PHISHME

For more information contact:

W: phishme.com/contact T: 703.652.0717
A: 1608 Village Market Blvd, SE #200 Leesburg, VA 20175