

The logo for PHISHME, featuring the word in a bold, white, sans-serif font. The background of the top header is dark blue with a grid of small white dots. There are also some faint white lines and symbols, including a plus sign and a target icon, scattered across the header area.

PHISHME

+

+

A simple menu icon consisting of three horizontal white lines.

Quotation for City of Fort Collins August 3rd, 2017

Roman BeDan

303-941-1323

Roman.BeDan@phishme.com

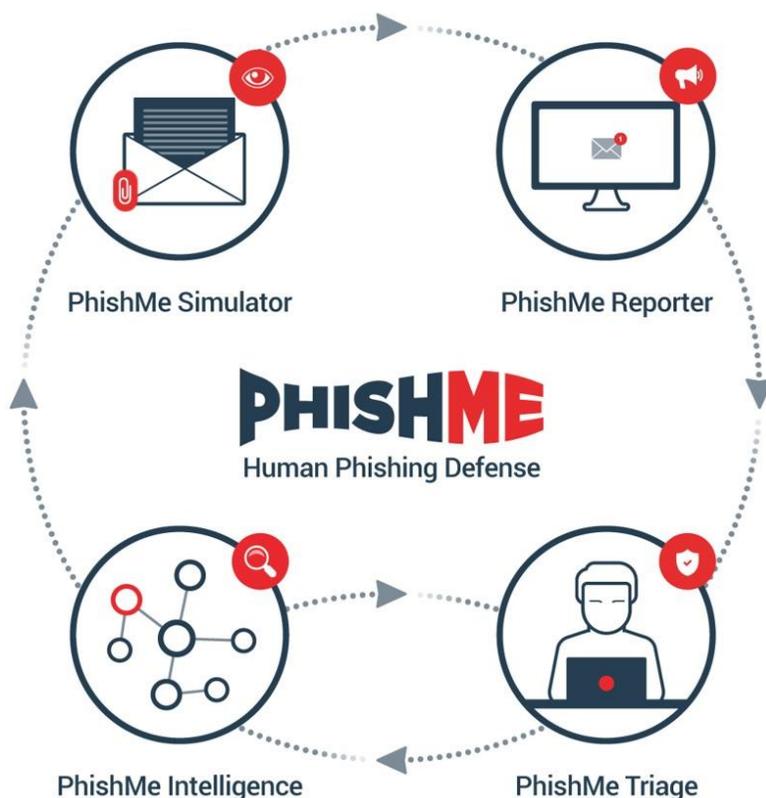
TABLE OF CONTENTS

- OVERVIEW 1
 - PhishMe Simulator 1
 - PhishMe Reporter 1
 - PhishMe Triage 1
 - PhishMe Intelligence 1
- WHY PHISHME? 2
- PRICING 3
- ABOUT PHISHME, INC. ERROR! BOOKMARK NOT DEFINED.



OVERVIEW

Thank you for your interest in the PhishMe suite of solutions designed to assist you in securing your network and your users from attack. The combination of our four products – Simulator, Reporter, Triage and Intelligence – work to complement the defenses you are already using at the perimeter and at the host level in your enterprise. With over 90% of successful attacks today starting with a phishing email, bolstering your staff's ability to avoid and rapidly report suspicious emails is critical to the successful defense of your network. Our analysis platform also provides you the ability to decrease the amount of time needed to respond when such attacks attempt to penetrate your corporate environment. A brief overview of the solution set is provided below; please refer to the individual product overviews for more detailed information. A formal quotation is provided on page three of this document.



PhishMe Simulator

A Software as a Service solution that provides a rich environment for sending simulated phishing attacks to your staff. Users that are susceptible are immediately provided succinct training. Over 100 scenarios and a vast variety of training formats (including videos, info graphics, and quizzes) are available for you to customize. Included at no additional cost are 15 complete CBT training modules on a variety of security and security compliance topics. Comprehensive reporting provides you with a detailed understanding of user susceptibility, trends over time, repeat offenders, and the ability to sort this data by department, geography, and cost center.

PhishMe Reporter

A customizable plug-in to major mail clients which allows users to report suspicious emails with the click of a button. By educating your team with PhishMe Simulator you create a network of trained people, increasing the volume and quality user reports proven to provide real-time insight into phishing emails currently in your environment.

PhishMe Triage

A virtual or hardware appliance deployed in your network, or cloud-based deployment, to harvest and analyze user reported incidents from PhishMe Reporter and other user data reports. With patent pending technology to cluster user reports based on the context of the email and the ability to assess the reputation of the individual, Triage provides incident responders a streamlined workflow to prioritize and rapidly conduct analysis on the most suspicious emails that may be an attack waiting to occur. Your security team can use the advanced YARA editor to create rules to manage further user reporting as well as update your other security solutions with the findings of their analysis.

PhishMe Intelligence

A human-verified, phishing-specific threat intelligence service that allows security teams to manage and prioritize alerts, speed incident response, and stay current with evolving threats. Intelligence brings additional insights and analysis—based on phishing attacks that we detect outside of your network—that complement PhishMe's Triage and Simulator products and enhance your incident response program. PhishMe Intelligence provides timely threat intelligence regarding the tactics, infrastructure, and other indicators used by today's phishing and malware campaigns. Your company is notified almost immediately after these attacks are launched, allowing your security team to understand, remediate, and block these threats before they affect your company.

WHY PHISHME?

PhishMe is widely recognized as an innovator and leader in the area of anti-phishing solutions. Originally developed in 2008, PhishMe has operations across the globe serving over 700 enterprise customers. With offices in Washington, New York, San Francisco, London, Dubai and Singapore, PhishMe is able to provide local support to our worldwide customer base. Operations are run both in the United States and in Europe, providing a privacy framework that meets differing regional legal frameworks.

In the **2015 Red List** published by Justin Somaini, PhishMe was recognized by over 40,000 information security practitioners as the **Number 1 Security Start-Up**. *“PhishMe has taken the top spot with their solution to help customers learn about email and URL link security. One of the major methods of compromise is the ability to get unsuspecting users to click on a malicious link. PhishMe’s solution has resonated in helping customers train employees on this issue.”*

Gartner noted in their most recent study on Computer Based Training that, *“PhishMe is the leading provider of anti-phishing CBT and enjoys robust success globally... This capability is supported with flexible and effective analysis and reporting capabilities. The PhishMe brand is well-known throughout the security industry, and the success of its marketing program and technical innovations has established it as the company to beat when it comes to anti-phishing solutions.”*

With the 2015 release of the PhishMe Triage product, industry analysts at the **451 Group** noted, *“Detectives have long known the value of a reliable informant, so why not groom similar relationships between users and incident responders in the enterprise? PhishMe has essentially built a product set to do this. Simulator tells you how good users are at spotting threats and grooms them to be better. Reporter allows them to exercise these skills every day with live email, and Triage adds a platform for incident handlers to act on Reporter’s data in an automated manner that can also integrate with other security product investments within the enterprise.”*

PRICING

Quotation City of Fort Collins – Pricing listed in this quote is valid until August 31st, 2017

Customers may be responsible for sales or other taxes as a result of a purchase from PhishMe, depending on applicable state and local laws.

Product	Price
<u>PhishMe Simulator Enterprise</u> <ul style="list-style-type: none"> Annual or upfront license to run phishing exercises to 1,940 unique email recipients in your enterprise Unlimited number of administrators Unlimited number of phishing scenarios during the annual term Access to over 300 scenario templates, education and features Access to 15 complete CBT training modules on security Unlimited product support Includes initial customer onboarding and administrator training Access to all feature enhancements and updates during the annual license Includes PhishMe Reporter with unlimited deployment of the plug-in across your enterprise and customizable icon and language for plug-in button 	\$15,919.00
Additional 4-month co-term to 12/31/2018	\$3,980.00
<u>Discount</u> <ul style="list-style-type: none"> Purchase completed by 8/31/2017 	Included
Total	\$19,899.00

For Customer signatory: By signing below, you represent and warrant that you have the authority to bind your organization to purchasing the above Product(s) for the corresponding fee(s).

IN WITNESS WHEREOF, this Quotation has been duly executed on behalf of each Party as of _____, 2017.

City of Fort Collins	PhishMe, Incorporated
By: _____	By: _____
Name: _____	Name: <u>James R. C. Hansen</u>
Title: _____	Title: <u>Chief Operating Officer</u>

PhishMe® is the leading provider of human-focused phishing defense solutions for organizations concerned with their susceptibility to sophisticated cyber attacks. PhishMe's intelligence-driven platform turns employees into an active line of defense by enabling them to identify, report, and mitigate spear phishing, malware, and drive-by threats. Our open approach ensures that PhishMe integrates easily into our customers' existing security technology, demonstrating measurable results to help inform an organization's security decision-making process. For additional information, please visit: www.phishme.com.