

PhishDefense

Datasheet

Phishing simulation service enables organizations to effectively test, train and build cyber resilience



Phishing attempts +400% in 2019



32% of breaches involved phishing



Execs compromised in 20% breaches

Phishing is The Top Cyber Attack, People Are The #1 Defense

According to the FBI, phishing represented over \$26 billion in worldwide business costs due to BEC fraud between 2016 and 2019.

The Verizon 2019 Data Breach Investigations Report predicts phishing costs will continue to grow as criminals adapt their attack strategies to reap faster returns via higher-value targets and distracted mobile users who are already at 18% of compromised clicks.

Watching these trends, it's clear that phishing is still one of the most pervasive, insidious cyber threats of our time. And the problem remains unresolved despite increasing investment in hardware, software and cloud-based technologies to combat it.

Why? Vulnerable users are easy targets for cyber criminals. Your most effective line of defense is arming your staff with the skills and knowledge they need. An effective security awareness training program is the solution -- one that is engaging, interactive, and ultimately changes behavior.

PhishDefense Phishing Simulation Service

PhishDefense is a cloud-based phishing simulator that:

- Automates and simulates phishing attacks across an organization
- Identifies vulnerable employees and takes immediate action to train them
- Captures user data and generates real-time reports

PhishDefense integrates with the Security Mentor Security Awareness Training Platform to help ensure your employees are security savvy.

Security Mentor provides what you need to protect your organization against phishing attacks, data breaches, risky behavior and insider threats. Used together, the integrated services enables you deliver a comprehensive, scalable, measurable program in a way that's easy-to-use, addresses your top challenges, and offers users a memorable, best-in-class experience.

	T mone of	ense		
Dashboard				
The Dashboard page shows up to date graphic an	d tabular results for all campaigns, wheth	her active, completed, or set-up but not ye	t launched. Note: no results are dis	played until a campaign is created.
The "Phishing Success Over Time" chart display cumulative phishing success percentage for all ca	s the percentage of users who were phish mpaigns combined. These charts both an	ned in all campaigns; each data point repre e representations of how successful a phis	isents a single campaign. The "Ave hing campaign has been.	rage Phishing Results" chart shows the
Below the charts is a table showing all campaigns	To see results for a specific campaign, cl	lick on the green chart button.		
Phishing St	access Over Time		Average Phishin	gResults
10 (100)				🔴 At Risk
				Phish Resistant
M				
N				
	61.02.03 62.02.03 62.02.03			
20 20 2020/20 20 2020/20 20 2020/20 20 20 20 20 20 20 20 20 20 20 20 20 2				
	00000			
Campaigns	GUERS			
Campaigns				Sauch
Campaigns	Goog			Search
Campaigns	SUIS	Created Date *	Status®	Search
Campaigns	United	Created Date * 02/15/2019	Status [©]	Search
Campaigns blow 10 entries Name [©] Campaign #3		02/15/2019	In Progress	
Campaigns Show 10 entries Name [©]				
Campaigns blow 10 entries Name [©] Campaign #3		02/15/2019	In Progress	
Campaigns thow 10 entries Name ⁰ Campaign #3 Campaign #2		02/15/2019 01/18/2019	In Progress Completed	

Automate & Test

Phishing simulation should be conducted regularly and often.

Using PhishDefense pre-built templates, or your own customized templates, you can quickly and easily configure and schedule campaigns to test and measure phishing risk and progress over time.

Identify & Act

PhishDefense automatically detects and records campaign results per user.

Vulnerable users are immediately alerted to their mistake and redirected to targeted training sessions. Positive behavior is rewarded using gamification and friendly competition across your organization.

Measure & Report

Your security awareness program should be based on current, actionable insights and data.

The PhishDefense Dashboard enables you quickly track how your campaigns are doing and assess whether you are lowering your organizational risk by building user resistance.

1 Details	2 ittack Type	3 Email Template	(4) Training Page	5 From Address	6 Target List(s)	7 Review
o create a new Campa our campaign. The St he Campaign ends and	rt Date is wh	en a campaign begi	ns and by default i	set to the current	day and time. The E	
Campaign Name:	Campai	gn name				
Start Date:	02/19/2	019 6:30 PM				
End Date:		019 6:30 PM				

My Rewards	
Your Total Points Earned 350	
Your Badges Earned	
Your Lesson Points Earned	
Social Networking	50 pts 🚖
Mobile Security	50 pts 😭
Web Security	50 pts 😭
Information Protection	50 pts 🏫
Phishing	50 pts 😭
Your Phishing Resisted Points Earned	
Campaign on Feb. 15th, 2019	50 pts
Campaign on Feb. 15th, 2019	50 pts

		Campaign Events C	And the first	Email State	***
	1.00				Email Opene
	1.196				😑 Email Sent
Aumber of Users		Time of Event	·		Uink Clicked
The	etails table below show w 10 entri First Name		rin this campaign. To see an individual target's time Email [©]	line, click the triangle to the l Search: Training Group [©]	left of their name.
The	e table below show	es		Search:	
The	table below show w 10 entri First Name	es Last Name [©]	Email [©]	Search:	Status ©
The Sho	table below show w 10 entri First Name ^ Aaron	es Last Name [©] Nunoz	Email © aaron.munoz@demo03.example.local	Search:	Status [©] Link Clicked
The Sho	table below show w 10 entri First Name * Aaron Abby	es Last Name [©] Munoz Harrison	Email [©] aaron. munoz@derno03.example.local abby.harrison@derno03.example.local	Search:	Status © Link Clicked Link Clicked
The Sho	table below show www.inentri First Name Aaron Abby Abe	es Last Name [©] Munoz Harrison Fuentes	Email ® auron.munoa@demo03.example.local abby.harrison@demo03.example.local abe.fventes@demo03.example.local	Search:	Status © Link Clicked Link Clicked Link Clicked
The Sho	table below show w 10 entri First Name Aaron Abby Abe Ada	es Last Name [©] Munoz Harrison Fuentes Johnson	Email © aaron muroz@demo03.example.local abby.harrison@demo03.example.local abs.fuentes@demo03.example.local ads.johnson@demo03.example.local	Search:	Status © Link Clicked Link Clicked Link Clicked Link Clicked
The Sho	table below show 10 entri First Name Aaron Abby Abe Ada Adam	es Last Name [©] Munoz Harrison Fuentes Johnson Talkington	Email [©] aaron.muno20demo03.example.local abby.hurrison@demo03.example.local abd.johnso@demo03.example.local add.johnso@demo03.example.local add.mt.atkington@demo03.example.local	Search:	Status © Link Clicked Link Clicked Link Clicked Link Clicked Email Opened

Features

- 24x7 availability with unlimited phishing campaigns for most training packages
- Intuitive campaign wizard to easily select email templates, training pages, target lists and sending domains, and set campaign schedules
- Customized variables for inclusion of unique organization and user data to emulate spear phishing and BEC attacks
- Target list creation by adding single targets, importing from the Security Mentor Learning Management System or bulk upload
 Organization, group, and individual targeting capabilities
- Extensive library of pre-built templates, as well as the ability to create custom templates
- Automated redirection of at-risk users to relevant, real-time training
- Integration with the Security Mentor Learning Management System
- Dashboard providing real-time reporting and metrics on phishing campaigns

Why Security Mentor

Security Mentor is the industry pioneer and expert in security awareness training and education services. Since 2008, Security Mentor has consistently redefined how training is created, delivered, experienced, and embraced by combining expertise and creativity in security, technology, media, and e-learning. Trusted by customers and celebrated by users, its comprehensive training platform offers on-demand, easy-to-use, and effective solutions including security awareness training, phishing simulation, policy tracking & compliance services, and awareness materials.