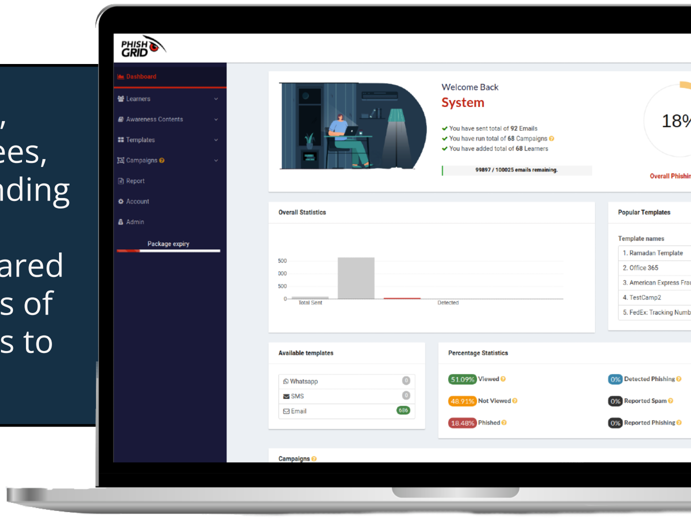
DATA SHEET

PHISHING SIMULATION SERVICES

Email remains the primary vector for most cyber attacks.

85% of the data breaches involve the human element. 36% involve phishing, that is 11% more than last year. 10% involve ransomware, doubling its frequency very fast. Plus during the ongoing pandemic, people are mostly working from home which leaves them exposed to numerous attacks starting from phishing. Even the more concerning thing is 62% of what the phishing actors obtained through their successful phishing activity was login credentials. Can your employees easily recognise which is a phishing mail?

Phishing simulation service includes creating targeted, relevant and luring campaigns, phishing your employees, further analyzing their behavior and hence understanding your organization's susceptibility to phishing attacks. Furthermore a comprehensive detailed report is prepared analyzing the organization's resilience, and the success of the campaign, which sets a path for the further actions to be taken in the course of educating your employees.



SIMULATED PHISHING AS A SERVICE

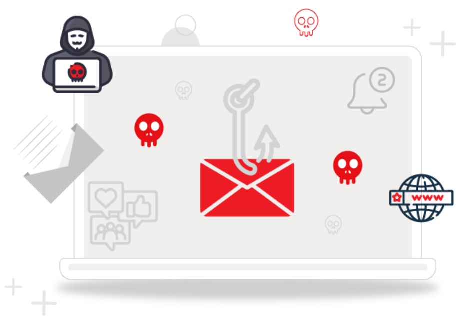
As finding solutions is just half of the trick, the main goal is to learn why the interference occurs and that's exactly what we at PhishGrid serve.

Our method of conducting simulated phishing attacks combined with our Bi-weekly awareness resources, we aim to create a strategic approach which will help you combat the phishing attacks tailored to your organization's domain, departments and other characteristics.

PhishGrid phishing simulation service utilizes social engineering capabilities to check for spear phishing, clone phishing and other phishing attacks.

At PhishGrid, we provide assurance around both technical and people control in place to prevent key assets from being compromised. We draw on our experience of performing real-world phishing attacks in red team engagements, as well as insights from responding to attacks against our customers.

MINIMIZING THREAT IS EASY!



Phishing Simulations helps you fight phishing attacks by providing continuous simulation and training to employees to understand the latest techniques, recognise subtle clues and help stop data loss, email fraud and brand damage.

As businesses continue to deploy new strategies and educate their users about cyber security, cybercriminals continue to improve phishing attacks and develop new scams.

These evolving and sophisticated attack techniques, designed to fool employees, put your organization and employees vulnerable and at risk for **data loss, financial fraud, and embarrassing exposure**, thus reputation loss as well. Phishing simulation protects your organization by helping to stop the potentially-devastating attacks that can slip through security gateways.

How are we different?

Our solutions send targeted phishing emails to your employees, report and track who clicks and opens the link on the email. Then, automatically deploy awareness brochures to the employees who "FAIL". We also support customized **multi-stage campaigns**, which makes the simulation more near to the real-world and tests the best of your organization's resilience to real-world attacks.

To monitor the improvement, we regularly deploy phishing mails to the employee. To make sure your organization and employees are aware enough to combat phishing we will keep providing the help, security advisories and awareness contents.

Key benefits

- ✓ **Mitigation In Risks** - The first and foremost importance is that it significantly decreases the attacks caused by human manipulation and deception.
- ✓ **Added Value** – With our AI-powered technology actions are taken immediately as soon as they are reported. It protects your corporate network by analyzing the changes in human behavior.
- ✓ **Employees as shield** - Since employees are now aware of the n numbers of cases where it can be phishing, with proper training your employees can act as a primary shield.
- ✓ **Stay compliant** - you can stay compliant to your regulatory needs - we generate customized reports for specific needs also we believe that a proper awareness not just stays till the workplace but extends to employees life making a better impact.
- ✓ **Nurture a culture of cyber security awareness** ingrained into your organization
- ✓ **Concise and tailored on-point training**
- ✓ **Rigorous use of metrics to prepare reports, and further campaigns**
- ✓ **Dynamic and AI based threat simulation**
- ✓ Layers of protection against phishing emails
- ✓ **Mimic real-life attacks**
- ✓ **Automated Workflow**
- ✓ Constant innovation development to keep up with trends
- ✓ A conjunction of phishing tests and awareness modules.

WHAT DO YOU GET?

Every organization has a unique architecture and thus we devise unique, tailored strategies just for you!

- **Customizable simulated phishing attacks:** The platform allows administrators to create and customize simulated phishing attacks to test the awareness of their users.
- **Realistic templates:** The platform provides a range of **700+** realistic phishing templates that can be used to create simulated phishing attacks, including emails, vishing, and social media messages.
- **User tracking and progress monitoring:** The platform allows administrators to track the progress of individual users and see how they have responded to simulated phishing attacks.
- **Reporting and analytics:** The platform provides administrators with insights into the effectiveness of the training, such as the percentage of users who have fallen for simulated phishing attacks and their overall scores.
- **Vishing Support:** The platform also supports pre-built vishing templates to perform phone based vishing attacks. (additional credits will be required)
- **SMS Support:** The platform allows administrators to create and send simulated phishing text messages (SMS) to test the awareness of their users.
- **Educational resources:** The platform also provides an inventory of educational resources, such as tips and best practices, that can be used as landing content to help users learn how to identify and avoid real phishing attacks.
- **Multi-language support:** The platform supports template creation in multiple languages to accommodate users who may not speak English as their first language.
- **Integration with other systems:** It may be useful for the platform to integrate with other systems, such as a company's learning management system or active directory.
- **Support for multiple sub-users:** The platform supports multiple sub-user management provided to the admin users.
- **Security measures:** The platform has strong security measures including encryption in place to protect user data and prevent unauthorized access.
- **Mobile compatibility:** The platform is accessible on mobile devices so that users can complete the training on the go.

?

Find out more.

Learn more about the latest phishing strategies and ways to protect your organization here.

TIKAJ

www.tikaj.com / contact@tikaj.com

TIKAJ is an enterprise security and solution development company, offering solutions and services focussed on development, security, RPA, and data intelligence. TIKAJ portfolio contains multiple products in the cybersecurity and other domains which have been deployed, for multiple clients in the finance, insurance, and healthcare sector. Currently, TIKAJ clientele spans across Saudi Arabia, Philippines, India, and Australia.