



# Phishing Attack Simulation

Customized End-User Campaigns

## Train Your Employees

When it comes to cyber threats like phishing, your employees are often the largest and most vulnerable target. [iCorps Phishing Attack Simulation](#) allows your business to create customized phishing emails that facilitate security awareness through employee training and testing. Key features include:

- **Realistic Phishing Campaigns** - Simulate hundreds of realistic, challenging phishing attack emails with a few clicks. Interactive campaigns drive engagement and retention.
- **Effective Security Training** - Campaign results provide automatic testing and training to end-users when necessary. Raise awareness about complex social engineering threats.
- **Comprehensive Reporting** - Measure end-user susceptibility and overall risk across your organization. Meet compliance requirements with scheduled testing.



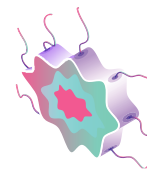
### AD HOC SIMULATED PHISHING ATTACKS

Campaigns occur over a 2-week period, concluding with a deliverable of the results and recommendations for improvement.

The fees for this service are:

**\$1,000 set-up fee per campaign**

**\$2.00 per user per campaign**



### ANNUAL PHISHING PROGRAM

There will be an initial baseline attack lasting 2 weeks. Then there will be 4 attacks, every 3 months, over a 12 month period.

Our deliverable will contain recommendations for improvement. The fees for this service are:

**\$4,500 set-up fee**

**\$24.00 per user per year**