

TRIDENT 

Automated Spear Phishing Platform

WHAT IS SPEAR PHISHING?

Spear Phishing is an email based attack technique used by attackers to penetrate a company's network during a targeted attack. It is also the most commonly used and successful method for targeted attacks. 76% of organizations reported being victim of a phishing attack in 2017.



STEP 1

Attackers gather information on any individuals working for the target company.



STEP 2

Using the gathered information an email message is created for the targets along with a malicious attachment or hyperlink.



STEP 3

The target receives the malicious email in their inbox and opens it, viewing the malicious attachment and hyperlink.



STEP 4

The attachment executes malware or the hyperlink leads the target to a forged login page to collect their user credentials.



WHAT IS TRIDENT?

AND WHAT CAN IT DO FOR YOUR BUSINESS?

TRIDENT is an automated spear phishing platform that allows you to constantly test your employees with real world spear phishing simulations. After just one month most companies see a 10% to 20% drop in employee vulnerability to spear phishing.

About TRIDENT

Most Security is Reactionary. Not TRIDENT.



What if you could train your employees automatically? **TRIDENT** makes that possible.

Increasingly companies and employees are being attacked and compromised by hackers all around the world. **If you think only high profile companies get targeted, you're wrong.**

What if you could protect your company from these threats before they happen? What if you could prepare and empower your employees to be vigilant against hackers trying to compromise your corporation? With **TRIDENT** you can!

1

Fully Autonomous

Truly a "set it and forget it" service. Campaigns can run automatically once, monthly, quarterly, or yearly.

2

Easy Setup

No coding necessary. After sign up you can start a campaign within seconds.

3

Easy Configuration

Pick a template, from domain, attachments, targets, landing page, and time frame for each campaign.

TRIDENT Features

INSTANTLY KNOW YOUR VULNERABILITY EXPOSURE TO SPEAR PHISHING
WATCH IN REAL TIME AS YOUR EMPLOYEES LEARN WHAT TO LOOK FOR



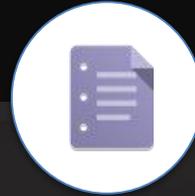
SET IT & FORGET IT

Schedule campaigns once and allow them to run once, monthly, quarterly, or yearly.



SAFE WEAPONIZED ATTACHMENTS

Weaponized attachments that mimic real world attacks and detect when a user accesses the attachment.



DETAILED EMAIL TEMPLATES & LANDING PAGES

Various scenarios, multiple templates per scenario, countless combinations.



FULLY AUTOMATED & CUSTOMIZED REPORTING

Generate campaign or target group specific reports for total visibility across all your employees and campaigns.

Overall Campaign Dashboard

Monitor Detailed Campaign Statistics

Total Phished Ratio

Instantly see where your employees rate at a glance

Phished Ratio Over Time

Determine the effectiveness of the campaigns and your employees' performance over time

Campaign Success Rates

See which campaigns your employees are most susceptible to

Performance Tracking

See which employee/target groups perform the best and which ones need more training



Detailed Template Information

Full scope details on every recorded attack

Attack Scenarios

Numerous attack scenarios ripped straight from the attacker's playbook

Weaponized Attachments

Several safely weaponized attachments that mimic real world attacks

Custom Landing Pages

Custom landing pages for victims, download files, collect credentials, play training videos and more

Full User Activity Tracking

Never inadvertently send out a campaign. All user activity within TRIDENT is logged and accounted for

The screenshot displays the TRIDENT dashboard interface. On the left is a dark sidebar navigation menu with the TRIDENT logo at the top. The menu items include: Dashboard, Campaigns (30), Templates (11), Fake Receipts (4), Fake Invoice (4), Fake Security Bulletin (3), Fake Personal Email, Fake Party Invite, Fake Employee Survey, Fake Social Media Notification, Fake Wrong Person Email, Fake File Sharing Email, Create New Email Template, Attachments (1), and Landing Pages (3). The main content area is titled 'TRIDENT TEMPLATES - ALL' and shows two preview cards. The first card, 'Custom Fake Receipt', displays a sample receipt for a 'WebstaurantStore' order with a table of items including 'Aussie PROCEED Stainless Steel Double Overhaul - 40" x 12" (17850580)' and 'Choice 1/4" French Fry Cutter (45747715)'. The second card, 'Fake Favor Receipt', shows a receipt for a 'FAVOR' order with a total of \$19.85. Below each preview card are buttons for 'HTML', 'Text', 'EDIT', and 'DELETE'.

Detailed Custom Landing Pages

Custom Landing Pages for victims. Download Files, Collect Credentials, Play Training Videos and More.

SPECTANT
SECURITY

You have been the victim of a Simulated Spearphishing Campaign.

Follow the Steps Below:

Step 1

DON'T PANIC

Step 2

**CONTACT YOUR ORGANIZATION'S IT/SECURITY
OFFICE**

Step 3

**WATCH THE FOLLOWING VIDEO ON
SPEARPHISHING SAFETY**

Know the Risk - Raise Your Shield: Spear Phishing

SPEAR PHISHING

Physical Social Engineering with USB Campaigns

Test your employees' adherence to data handling guidelines.

The screenshot displays the TRIDENT ATTACHEMNTS interface. On the left is a navigation sidebar with options: Dashboard, Campaigns (30), Templates (11), Attachments (3), View Attachments (3), Upload Attachment, Landing Pages (3), Targets (7), Reports, Users, Logs, and Settings. The main content area is titled 'TRIDENT ATTACHEMNTS' and shows four attachment cards:

- Employee Termination Report**: File name 'Employee_Termination_Report.docx'. Description: 'This is a fake employee termination document.' Preview shows a document with text and a signature line. Buttons: EDIT, DELETE.
- Monthly Newsletter**: File name 'Monthly_Newsletter.doc'. Description: 'This is a fake monthly newsletter.' Preview shows a newsletter layout with a header, images, and text. Buttons: EDIT, DELETE.
- Employee Salary Distribution Report**: File name 'CONFIDENTIAL_Salary_Report.xlsx'. Description: 'This is a fake salary distribution report.' Preview shows a spreadsheet with columns for employee names and salaries. Buttons: EDIT, DELETE.
- Formal HR Grievance Reprimand**: File name 'HR_VIOLATION_WRITEUP.doc'. Description: 'This is a fake HR reprimand.' Preview shows a document with a header, a circular progress indicator, and a table. Buttons: EDIT, DELETE.

At the bottom of the interface, it says '2017 © SPECTANT SECURITY'.

1

Safely Weaponized

Several safely weaponized attachments that mimic real world attacks. No actual exploitation occurs.

2

Zero Risk

No internal data exposure. Weaponized documents only beacon out to the trident platform.

3

Physical Testing

Drop USB flash drives in high traffic areas for maximum coverage. Measure employee adherence to data handling procedures.