TECHNAGY IT
empowering you

Phishing Campaign Report

Phishing Campaign

It is a type of cyberattack where malicious actors impersonate legitimate entities or organizations through email messages, text messages, or other forms of communication. The goal of phishing is to trick recipients into providing sensitive information such as login credentials, credit card numbers, or personal details, or to manipulate them into performing actions that benefit the attacker, such as clicking on malicious links or downloading malware.

Campaign Results:
Phishing simulations sent to users are initially ranked between Easy, Medium, or Hard based on their overall click rate and plausibility.

Phishing Results Overview Campaign Results:

Emails Sent: This metric indicates the total number of phishing emails distributed as part of the campaign. It serves as a measure of the campaign's scale and outreach.

Scenarios Used: Phishing campaigns often use different scenarios or pretexting techniques to lure recipients into action. These scenarios could involve posing as a trusted entity (e.g., a bank, a colleague, a social media platform) and creating a narrative that prompts recipients to disclose sensitive information or click on malicious links.

Emails Opened: This metric represents the recipients who opened the phishing emails. It indicates the effectiveness of the email subject lines, sender information, and overall presentation in capturing recipients' attention and enticing them to engage with the content.

Caught Phish: The number or percentage of phishing attempts that were successfully identified and reported by recipients or detected by security systems (e.g., email filters, antivirus software). This metric reflects the level of awareness and vigilance among recipients and the efficacy of security measures in place.

Clicked Links: The percentage of recipients who clicked on links or attachments embedded within the phishing emails. Clicking on these links could lead to the execution of malicious code, redirection to fraudulent websites, or further interaction with the attacker-controlled infrastructure.

Submitted Data: The number or percentage of recipients who fell for the phishing attempt and submitted sensitive information or performed desired actions (e.g., entering login credentials, providing personal or financial data). This metric represents the ultimate success of the phishing campaign in achieving its malicious objectives.

Each of these metrics provides valuable insights into the effectiveness and impact of the phishing campaign, helping organizations assess their susceptibility to such attacks, identify areas for improvement in security awareness and training, and implement appropriate countermeasures to mitigate future risks.

For: Altera Fund Advisors

Start Date: October 22, 2025 **End Date:** October 25, 2025

Phishing Report

Bi-Weekly Phishing Campaign -25

1. Background Information

What is Phishing?

Phishing is the most popular attack method used by cybercriminals. By posing as a legitimate individual or institution, the criminal attempts to trick their target into providing sensitive information or downloading malicious content. Information compromised in a phishing attack can be used to access important work or personal accounts that could lead to a major data breach for an organization, or identity theft for the affected individual.

Purpose of this Report

Cybercriminals are continuously improving their phishing techniques, making it difficult for technical safeguards like spam filters to identify them and keep them out of your employees' inboxes. That means employees are on the front lines to protect your network and should be trained on how to properly identify a phishing email. Sending employees fake phishing emails known as phishing simulations is a great way to test their ability in spotting these potentially malicious messages on an ongoing basis.

2. Phishing Results Overview

Campaign Results

Let's unpack the results from this phishing campaign and see how your employees fared.

33

Emails Sent

32

Scenarios Used

3

Emails Opened

0

Caught Phish

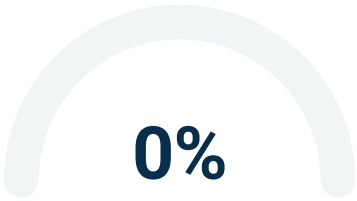
2

Clicked Links

0

Submitted Data

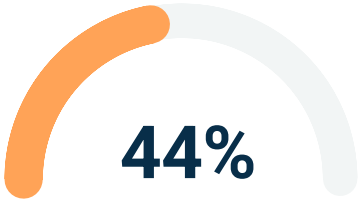
Phishing simulations sent to users are initially ranked between Easy, Medium, or Hard based on their overall click rate and plausibility. The below graphic denotes the distribution of the sent simulations between these categories.



0%

Easy Difficulty

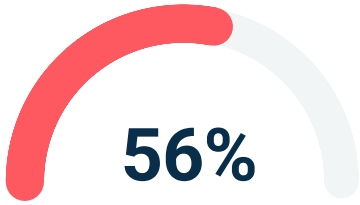
0/32 scenarios were "Easy" difficulty



44%

Medium Difficulty

14/32 scenarios were "Medium" difficulty



56%

Hard Difficulty

18/32 scenarios were "Hard" difficulty

3. Phishing Fail Rate

The figure below illustrates your organization's Phishing Fail Rate (PFR) in comparison to the Community Average Phishing Fail Rate.

Your Company Phishing Fail Rate:

6.1%

0.8 percent **above** the Community Average which is **5.3%.**

What is the Phishing Fail Rate and Community Average?

Your Phishing Fail Rate (PFR) indicates the percentage of your employees who clicked on the simulated phishing link divided by the total number of employees the simulation was sent to. For comparison purposes, we've established a Community Average Phishing Fail Rate, which is the average simulated phishing campaign click rate across all organizations we monitor. Set organizational goals of having a PFR less than the community average but remember, it only takes one click on a real phishing email to potentially cause an issue.

Caught Phish

0

0 employee(s) were able to correctly identify this phishing simulation.

Please contact us if you do not have the Catch Phish plugin enabled.

Submitted Data

0

0 employee(s) entered in credentials after clicking on the simulated phishing link.

Not all simulated phishing campaigns have links that capture credentials. For these specific campaigns, please contact us for more information.

4. Campaign Results Details

Scenario Name

Identifies the name of the phishing scenario sent to the employee.

Phishing Result

Describes the action that the user took for this campaign.

Phishing Fail Rate (PFR) %

The rate at which the user has fallen for previous email phishing simulations. A higher PFR is considered high risk.

Employee Secure Score (ESS)

The lower the ESS, the more at-risk the user is of being a security concern. Above 630 is considered low risk, under 500 is considered high risk.

Please note: PFR(%) and ESS will display as N/A (Not Applicable) for clients in an Unlimited Training and HIPAA Compliance product.

Employee Name and Email Address	Date Sent	Scenario Name	Phishing Result	PFR (%)	Employee Secure Score (ESS)
Taylor Trent ttaylor@alteradevco.com	2025-10-22 10:32 pm UTC	Google Account Password Change	Email Sent	0.00%	
Garza John jgarza@alteradevco.com	2025-10-22 10:32 pm UTC	Apple Itunes Invoice	Email Sent	0.00%	
Gascoyne Lina lgascoyne@alteradevco.com	2025-10-22 10:32 pm UTC	Google Shared Document	Email Sent	0.00%	
Brooks Caleb cbrooks@alteradevco.com	2025-10-22 10:32 pm UTC	LinkedIn Profile Update	Email Sent	0.00%	
Allen Kimberly kallen@alteradevco.com	2025-10-22 10:32 pm UTC	UPS Package Delivery	Email Sent	0.00%	

5. Campaign Results Details

Employee Name and Email Address	Date Sent	Scenario Name	Phishing Result	PFR (%)	Employee Secure Score (ESS)
Rios Iskandar irios@alteradevco.com	2025-10-22 10:32 pm UTC	FedEx Package Delivery	Email Sent	0.00%	350
Tillman Trace ttillman@alteradevco.com	2025-10-22 10:32 pm UTC	One Drive 2 - Document Sent to You	Email Sent	0.00%	350
Runge Joanne jrunge@alteradevco.com	2025-10-22 10:32 pm UTC	One Drive New Fax Document	Email Sent	0.00%	350
Liland Davidson dliland@alteradevco.com	2025-10-22 10:32 pm UTC	Microsoft Office 365 Message Encryption	Email Sent	0.00%	340
Jones Jerusha jjones@alteradevco.com	2025-10-22 10:32 pm UTC	UPS Package Shipped	Email Sent	0.00%	350
Quinn Terry tq@alteradevco.com	2025-10-22 10:32 pm UTC	Office O365 Messages Failed to Sync	Email Sent	2.44%	293
Ordunez Arturo ardunez@alteradevco.com	2025-10-22 10:32 pm UTC	Office 365 Audio Conferencing	Email Sent	0.00%	350
Bonilla Angelica abonilla@alteradevco.com	2025-10-22 10:32 pm UTC	Skype New Message	Email Sent	0.00%	350

6. Campaign Results Details

Employee Name and Email Address	Date Sent	Scenario Name	Phishing Result	PFR (%)	Employee Secure Score (ESS)
Malkasian Stacy smalkasian@alteradevco.com	2025-10-22 10:32 pm UTC	DropBox - New Sign-in	Email Sent	20.00%	
Alcantar Dina dalcantar@alteradevco.com	2025-10-22 10:32 pm UTC	Walmart Order Confirmation	Email Opened	0.00%	
Winant Katrina kwinant@alteradevco.com	2025-10-22 10:32 pm UTC	Renewal of Spotify Confirmation	Clicked Link	20.00%	
Roberts Kevin kroberts@alteradevco.com	2025-10-22 10:32 pm UTC	Microsoft Teams: Company Newsletter	Email Sent	0.00%	
Aleman Enrique ealeman@alteradevco.com	2025-10-22 10:32 pm UTC	DHL- Delayed Shipment Action Required	Email Sent	0.00%	
Quinn Parker pquinn@alteradevco.com	2025-10-22 10:32 pm UTC	ChatGPT Free Trial	Email Sent	0.00%	
McDonald David dmcdonald@alteradevco.com	2025-10-22 10:32 pm UTC	Google Chrome Fake Verification Code	Email Sent	0.00%	
Curlee Rodney rcurlee@alteradevco.com	2025-10-22 10:32 pm UTC	Slack- New login	Email Sent	0.00%	

7. Campaign Results Details

Employee Name and Email Address	Date Sent	Scenario Name	Phishing Result	PFR (%)	Employee Secure Score (ESS)
Fisher Kristi kfisher@alteradevco.com	2025-10-22 10:32 pm UTC	Pay Settlement Commission Compensation Scam	Email Sent	0.00%	350
Haring Howard hharing@alteradevco.com	2025-10-22 10:32 pm UTC	Acorns Bonus Offer	Email Sent	3.70%	339
Copier Cannon copier@alteradevco.com	2025-10-22 10:32 pm UTC	HR Updated Remote Work Policy	Email Sent	0.00%	350
Tillman Eddie etillman@alteradevco.com	2025-10-22 10:32 pm UTC	HR Updated Remote Work Policy	Email Sent	0.00%	330
Rivenbark Paul privenbark@alteradevco.com	2025-10-22 10:32 pm UTC	App store- receipt for recent purchases	Email Sent	2.44%	343
Kennedy Mike mkennedy@alteradevco.com	2025-10-22 10:32 pm UTC	Coinbase Received Payment	Email Sent	2.44%	333
Watkins Jim jwatkins@alteradevco.com	2025-10-22 10:32 pm UTC	Encrypted Email	Email Sent	0.00%	300
McStay Judge jmcstay@alteradevco.com	2025-10-22 10:32 pm UTC	Wells Fargo Advisors: Security Alert: Unusual Login Attempt	Email Sent	0.00%	350

8. Campaign Results Details

Employee Name and Email Address	Date Sent	Scenario Name	Phishing Result	PFR (%)	Employee Secure Score (ESS)
Stark Ralph rstark@alteradevco.com	2025-10-22 10:32 pm UTC	Account Verification Alert (General)	Email Sent	0.00%	
Wills Rhonda rwills@alteradevco.com	2025-10-22 10:32 pm UTC	Monday.com - Project Deadline Reminder	Email Sent	0.00%	
Perez Emilio eperez@alteradevco.com	2025-10-22 10:32 pm UTC	Spotify - Family Plan Invitation	Clicked Link	100.00%	
De Nieunkerk Dena ddenieunkerk@alteradevco.com	2025-10-22 10:32 pm UTC	Stripe - Overdue Invoice	Email Sent	0.00%	

9. What's the Impact?

A Halt in Business Operations

Clicking a malicious link in a real phishing email could direct you to a malicious webpage where forms of malware or ransomware could be delivered. These infestations could wreak havoc on the device it was initiated on or could spread throughout a connected network, preventing you and your employees from accessing critical data and tools that make it possible to do your jobs. This downtime could cost you thousands in revenue, your customer's hard-earned trust, and compromise employee and customer data that could impact their lives forever.

Breached Accounts Put Data at Risk

Some phishing scams go one step further and attempt to steal login credentials to known websites by creating fake login pages, a tactic called "spoofing". If an employee enters their credentials on a spoofed website, their login information could be passed right to a cybercriminal. With that information, the criminal could get instant access into the employee's account and could try those credentials on other sites as well, which could ultimately lead to a major security breach.

Ongoing Training is Key!

As criminals continue to advance their phishing tactics to sneak through your company's spam filter, your employees play a major role in your company's overall security. So, what can you do? According to the **Herjavec Group**, "Employee training may prove to be the best ROI on cybersecurity investments for organizations globally over the next 5 years". Through ongoing training and phishing education, employees continuously practice identifying malicious emails, making spotting phishing scams second nature and greatly reducing your risk of a security incident.