# Table of Contents

**Overview** ................................................................................................................................. 2

**Knowledge Assessment Reports** ............................................................................................... 3
- CyberStrength Performance Report................................................................................................. 3
- Knowledge Assessment and Training Progress Report................................................................. 7

**Phishing Simulation Reports** ....................................................................................................... 9
- Phishing Campaign Performance Report.......................................................................................... 9
- Phishing User Performance Report.................................................................................................. 12
- ThreatSim Campaign Overview Report........................................................................................... 14
- ThreatSim Reports on Individual Campaign Details....................................................................... 15
- ThreatSim Raw Campaign Data CSV Reports............................................................................... 18
- ThreatSim USB Campaign Details Report....................................................................................... 19

**Reported Email Performance & Analysis Reports** ...................................................................... 20
- PhishAlarm Analyzer Results Report.............................................................................................. 20
- Reported Email Performance Report.............................................................................................. 22

**Training Reports** ........................................................................................................................ 24
- Knowledge Assessment & Training Progress Report................................................................. 24
- Training Assignment Performance Report...................................................................................... 24
- Training Category Performance Report.......................................................................................... 26
- Training Module Performance Report............................................................................................ 29

**Users** ........................................................................................................................................ 33
- User Record Export......................................................................................................................... 33
- Training Report Card....................................................................................................................... 34

© 2020 Proofpoint, Inc. Private and confidential.
OVERVIEW

Proofpoint’s Security Education Platform captures each employee’s interaction with our simulated attacks, knowledge assessments, and interactive training. This means that security officers quickly have detailed information about not only who completed which assignments, but also in which topics they are strong or weak, and how they have improved over time. All user data can be characterized, filtered, and reported using administrator-defined fields, such as job function, geographic location, department, hire date, and role.

Administrators can export reports to various output formats, such as Excel and CSV, to easily share results with interested parties. Reports can be generated any time. Additionally, with our Scheduled Export feature, you can automatically send reports to managers and administrators to track progress, gauge results, and plan accordingly. This feature allows administrators to define recipients, frequency, time, and format of the report output, which aids in sharing the responsibility of driving completion of assessment training. For an LMS implementation, user performance data and results for our training modules are based on the reporting capabilities of the LMS system used.

Below is a summary of reports available in the Security Education Platform. For more details about each report, please refer to the sections that follow in the guide.

<table>
<thead>
<tr>
<th>Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge Assessment</td>
</tr>
<tr>
<td>• CyberStrength Performance</td>
</tr>
<tr>
<td>• Knowledge Assessment and Training Progress*</td>
</tr>
<tr>
<td>Phishing Simulation</td>
</tr>
<tr>
<td>• Phishing Campaign Performance</td>
</tr>
<tr>
<td>• Phishing User Performance</td>
</tr>
<tr>
<td>• ThreatSim Campaign Overview</td>
</tr>
<tr>
<td>• ThreatSim Raw Campaign Data CSV</td>
</tr>
<tr>
<td>• ThreatSim Reports on Individual Campaign Details</td>
</tr>
<tr>
<td>o All Email Campaigns History</td>
</tr>
<tr>
<td>o Individual Campaign Overview</td>
</tr>
<tr>
<td>o Geographic Distribution</td>
</tr>
<tr>
<td>o Endpoints</td>
</tr>
<tr>
<td>o Users</td>
</tr>
<tr>
<td>• ThreatSim USB Campaign Details</td>
</tr>
<tr>
<td>Reported Email Performance and Analysis</td>
</tr>
<tr>
<td>• Reported Email Performance</td>
</tr>
<tr>
<td>• PhishAlarm Analyzer Report</td>
</tr>
<tr>
<td>Training</td>
</tr>
<tr>
<td>• Knowledge Assessment and Training Progress*</td>
</tr>
<tr>
<td>• Training Assignment Performance</td>
</tr>
<tr>
<td>• Training Category Performance</td>
</tr>
<tr>
<td>• Training Module Performance</td>
</tr>
<tr>
<td>Users</td>
</tr>
<tr>
<td>• User Record Export</td>
</tr>
<tr>
<td>• Training Report Card</td>
</tr>
</tbody>
</table>

* Report pertains to both areas.
KNOWLEDGE ASSESSMENT REPORTS

The reports in this section pertain to CyberStrength assessments. They include:

- CyberStrength Performance Report
- Knowledge Assessment & Training Progress Report

CYBERSTRENGTH PERFORMANCE REPORT

OBJECTIVE

The CyberStrength Performance report displays a comprehensive array of user and assessment data so that organizations can track the progress and performance of their CyberStrength assignments.

BENEFITS

- Track the progress and performance of the organization’s cybersecurity initiatives.
- Quickly identify security risk at the organization, department, and user level or any other defined custom grouping.
- Benchmark the organization’s performance data against the same or other industries, other Proofpoint customers, and the organization itself over time to gauge results and develop an action plan to improve or maintain a competitive edge.

FEATURES

- Determine the organization’s weaknesses and strengths across a range of cybersecurity areas, identify the riskiest users or business units, identify the most missed question categories, and customize programs to reduce the identified risks.
- Track user progress and performance across all CyberStrength assignments.
- Compare company performance against the same or other industries, Proofpoint customers, and the organization itself over time.
- Display aggregate and detail-level data per assessment, user, category, and other customizable properties.
- Export options: Excel and CSV.

SAMPLE CYBERSTRENGTH PERFORMANCE REPORT

(see next page)
SAMPLE CYBERSTRENGTH PERFORMANCE REPORT (CONT.)

View includes Users Tab

CyberStrength Performance

Analyze and review assessment data to track the progress and performance of the CyberStrength assignments.

- Total Assessed Users: 1,311
- Average Score: 59%
- Average Time to Complete: 9m 21s

Strongest Category: Use the Internet Safely (62%)

Weakest Category: Protect and Dispose of Data Security (38%)

Scores by Department

Questions Details per User

© 2020 Proofpoint, Inc. Private and confidential.
View of Assignments Tab

View of Categories Tab
View of Questions Tab

View of Leaderboard Tab

User ranking is determined by the User's score on the assignment, then the number of days to complete the assignment.
KNOWLEDGE ASSESSMENT AND TRAINING PROGRESS REPORT

OBJECTIVES
The Knowledge Assessment and Training Progress report displays results and information regarding end users’ progress completing CyberStrength assessments and training modules. It lists the assignment and module completion status for all users by percentage Completed, In Progress, and Not Started.

BENEFITS
- Quickly compare completion rates across training assignments to determine which assignments require additional action to drive them to completion.
- Track all users’ progress on all CyberStrength assessments and training assignments in a single report, gauging their effectiveness at completing assignments.
- At-a-glance view of overall results and status of training assignments.
- Ability to drill-down to assignment-level details.

KEY FEATURES
- Provides a variety of filtering options, such as by assignment, start/due date, overall assignment progress, user assignment progress, and auto enrollment assignments.
- Flexibility to select which data fields to include or exclude from the table to meet specific analysis needs.
- Displays key performance indicators for the total number of training modules, categories, correct responses, and incorrect responses.
- Displays user progress by assignment as well as assignment details.
- Results can be compared across assignments, with the ability to include or exclude deleted assignments, deleted users, and users removed from the assignments.
- Displays users’ progress in CyberStrength assessments and training assignments.
- Displays completion percentage per module that is part of an assignment.
- One-page display of all numbers and percentage details about a specific assignment and the modules included in it.
- Multiple assignments can be displayed and compared at one time.
- Export options: Excel and CSV
SAMPLE KNOWLEDGE ASSESSMENT AND TRAINING PROGRESS REPORT

Knowledge Assessment and Training Progress

Track end user progress in completing CyberStrength knowledge assessments and training assignments to identify follow-up steps.

Data updated twice a day. Last update: 2023-Apr-08 at 15:04 (UTC) (approximately an hour ago)

Assignment Start Date
- Sorted data range

Assignment Due Date
- Sorted data range

Assignments

229

Auto-Enrolled Assignments

66

Completion Rate (%)

60.7%

Unique Users

475

User Progress in Assignment

In Progress
6.9%

Users Not Started
86.7%

Total
100.0%

User Progress By Assignment

Assignment Details Table

© 2020 Proofpoint, Inc. Private and confidential.
PHISHING SIMULATION REPORTS

The reports in this section pertain to ThreatSim phishing campaigns. They include:

- **Phishing Campaign Performance Report**
- **Phishing User Performance Report**
- **ThreatSim Campaign Overview Report**
- **ThreatSim Reports on Individual Campaign Details**
- **ThreatSim Raw Campaign Data CSV Reports**
- **ThreatSim USB Campaign Details Report**

PHISHING CAMPAIGN PERFORMANCE REPORT

OBJECTIVES

The Phishing Campaign Performance report aggregates the results of multiple phishing campaigns, reflects overall performance results, displays failure trends, and shows how individuals performed in each campaign received. Administrators can compare campaign performance level trends based on overall failure rates and individual events (such as, email viewed, link clicked, attachment opened).

BENEFITS

- Determine at the campaign- and user-level which campaign types end users are most vulnerable to so that additional campaigns can be developed and implemented.
- Drill-down to the user-level details to enable deeper analysis.
- Track phishing failure performance over time and use the trends to determine the organization’s optimal security awareness training programs.
- Compare campaigns types alongside each other to gain at-a-glance insight into the most effective campaigns and campaign types.

KEY FEATURES

- Provides a variety of filtering options, such as by campaign type and status, start and end date range, and include/exclude archived campaigns.
- Flexibility to select which data fields to include or exclude from the table to meet specific analysis needs.
- Displays key performance indicators for number of campaigns, number of phish, threat emails sent, and threat emails reported.
- Provides details about each current and past campaign as well as the participating end users.
- Shows user behavior statistics for individual campaigns, such as how many times each user viewed, clicked, and submitted data.
- Compares performance results of different campaigns, whether of the same type or different type.
- Displays the failure trend of campaigns and number of reported emails of a campaign over time.
- Export options: Excel and CSV
**SAMPLE PHISHING CAMPAIGN PERFORMANCE REPORT**

View includes Campaign Comparison Tab

### Phishing Campaign Performance

- **Campaign Start Date**
- **Campaign End Date**

#### Number of Campaigns
- **7**

#### Number of Phish
- **244**

#### Threats Sent
- **244**

#### Threats Reported
- **26**

#### Campaign Performance

- **Campaign Name**: 
- **Campaign Track Views**: 
- **Teachable Moment Type**: 
- **Beacon Tracking**: 
- **Campaign Metrics**: 
- **In Auto-Block**: 
- **Campaign Type**: 
- **Campaigns Archived**: 
- **User Platform Status**: 
- **Campaign Schedule Type**: 

#### Failure Trend

- **Graph**: 
- **Time**: 

#### Reported Emails

- **Graph**: 
- **Time**: 

#### Campaign Comparison

- **Campaign Name**
- **Q1**
- **Q2**
- **Q3**
- **Q4**
- **Percent of Campaign**
- **Future**
- **Past**
- **Unique Clicks**
- **Click Rate (%)**
- **Data Submitted**

<table>
<thead>
<tr>
<th>Campaign Name</th>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
<th>Percent of Campaign</th>
<th>Future</th>
<th>Past</th>
<th>Unique Clicks</th>
<th>Click Rate (%)</th>
<th>Data Submitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2020 Phishing Campaign 1</td>
<td>2020-04-01</td>
<td>2020-04-15</td>
<td>Completed</td>
<td>38</td>
<td>100.00%</td>
<td>35.8%</td>
<td>Yes</td>
<td>15</td>
<td>5.75%</td>
<td>2</td>
</tr>
<tr>
<td>2020 Phishing Campaign 2</td>
<td>2020-05-01</td>
<td>2020-05-15</td>
<td>Completed</td>
<td>38</td>
<td>100.00%</td>
<td>66.1%</td>
<td>No</td>
<td>9</td>
<td>9.58%</td>
<td>1</td>
</tr>
<tr>
<td>2020 Phishing Campaign 3</td>
<td>2020-06-01</td>
<td>2020-06-15</td>
<td>Completed</td>
<td>38</td>
<td>100.00%</td>
<td>42.4%</td>
<td>Yes</td>
<td>7.16%</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>2020 Phishing Campaign 4</td>
<td>2020-07-01</td>
<td>2020-07-15</td>
<td>Completed</td>
<td>38</td>
<td>100.00%</td>
<td>35.9%</td>
<td>No</td>
<td>21</td>
<td>2.15%</td>
<td>2</td>
</tr>
<tr>
<td>2020 Phishing Campaign 5</td>
<td>2020-08-01</td>
<td>2020-08-15</td>
<td>Completed</td>
<td>38</td>
<td>100.00%</td>
<td>40.4%</td>
<td>Yes</td>
<td>10.5%</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>2020 Phishing Campaign 6</td>
<td>2020-09-01</td>
<td>2020-09-15</td>
<td>Completed</td>
<td>38</td>
<td>100.00%</td>
<td>61.6%</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td>2020 Phishing Campaign 7</td>
<td>2020-10-01</td>
<td>2020-10-15</td>
<td>Completed</td>
<td>38</td>
<td>100.00%</td>
<td>6.1%</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2020 Phishing Campaign 8</td>
<td>2020-11-01</td>
<td>2020-11-15</td>
<td>Completed</td>
<td>38</td>
<td>100.00%</td>
<td>6.1%</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2020 Phishing Campaign 9</td>
<td>2020-12-01</td>
<td>2020-12-15</td>
<td>Completed</td>
<td>38</td>
<td>100.00%</td>
<td>6.1%</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2020 Phishing Campaign 10</td>
<td>2021-01-01</td>
<td>2021-01-15</td>
<td>Completed</td>
<td>38</td>
<td>100.00%</td>
<td>6.1%</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Total</td>
<td>154</td>
<td>84</td>
<td>34%</td>
<td>34</td>
<td>100.00%</td>
<td>35.8%</td>
<td>Yes</td>
<td>15</td>
<td>5.75%</td>
<td>2</td>
</tr>
</tbody>
</table>
View of Campaign Details Tab

<table>
<thead>
<tr>
<th>Total Clicks</th>
<th>Messages Viewed</th>
<th>Data Entry Count</th>
<th>Auto Enroll Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>84</td>
<td>63%</td>
<td>67</td>
<td>43</td>
</tr>
</tbody>
</table>

**Campaign Details**

<table>
<thead>
<tr>
<th>First Name</th>
<th>Last Name</th>
<th>Email Address</th>
<th>Campaign Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alexander</td>
<td>Carter</td>
<td><a href="mailto:alexander.carter@amycyeworksita.com">alexander.carter@amycyeworksita.com</a></td>
<td>2020 Phishing Campaign 5</td>
</tr>
<tr>
<td>Alexander</td>
<td>Edwards</td>
<td><a href="mailto:alexander.edwards@amycyeworksita.com">alexander.edwards@amycyeworksita.com</a></td>
<td>2020 Phishing Campaign 6</td>
</tr>
<tr>
<td>Amanda</td>
<td>Collins</td>
<td><a href="mailto:amanda.collins@amycyeworksita.com">amanda.collins@amycyeworksita.com</a></td>
<td>2020 Phishing Campaign 7</td>
</tr>
<tr>
<td>Amanda</td>
<td>Rogers</td>
<td><a href="mailto:amanda.rogers@amycyeworksita.com">amanda.rogers@amycyeworksita.com</a></td>
<td>2020 Phishing Campaign 8</td>
</tr>
<tr>
<td>Amy</td>
<td>Bailey</td>
<td><a href="mailto:amy.bailey@amycyeworksita.com">amy.bailey@amycyeworksita.com</a></td>
<td>2020 Phishing Campaign 9</td>
</tr>
<tr>
<td>Amy</td>
<td>Brown</td>
<td><a href="mailto:amy.brown@amycyeworksita.com">amy.brown@amycyeworksita.com</a></td>
<td>2020 Phishing Campaign 10</td>
</tr>
<tr>
<td>Amy</td>
<td>Gray</td>
<td><a href="mailto:amy.gray@amycyeworksita.com">amy.gray@amycyeworksita.com</a></td>
<td>2020 Phishing Campaign 11</td>
</tr>
<tr>
<td>Amy</td>
<td>Holy</td>
<td><a href="mailto:amy.holy@amycyeworksita.com">amy.holy@amycyeworksita.com</a></td>
<td>2020 Phishing Campaign 12</td>
</tr>
<tr>
<td>Amy</td>
<td>Lee</td>
<td><a href="mailto:amy.lee@amycyeworksita.com">amy.lee@amycyeworksita.com</a></td>
<td>2020 Phishing Campaign 13</td>
</tr>
<tr>
<td>Andrew</td>
<td>Wood</td>
<td><a href="mailto:andrew.wood@amycyeworksita.com">andrew.wood@amycyeworksita.com</a></td>
<td>2020 Phishing Campaign 14</td>
</tr>
<tr>
<td>Andrew</td>
<td>Wood</td>
<td><a href="mailto:andrew.wood@amycyeworksita.com">andrew.wood@amycyeworksita.com</a></td>
<td>2020 Phishing Campaign 15</td>
</tr>
<tr>
<td>Amanda</td>
<td>Gonzales</td>
<td><a href="mailto:amanda.gonzales@amycyeworksita.com">amanda.gonzales@amycyeworksita.com</a></td>
<td>2020 Phishing Campaign 16</td>
</tr>
</tbody>
</table>
PHISHING USER PERFORMANCE REPORT

OBJECTIVE

The Phishing User Performance report analyzes users' interactions with simulated phishing attack campaigns, causes of single failures, and identifies repeat offenders.

BENEFITS

- Assists in identifying simulated phishing attack campaigns, campaign types, and templates that might be more effective than others within their organization.
- Focus on the phishing risk at the campaign, department, and individual user level to identify and tailor security awareness training programs.
- Instantly identify riskiest users and repeat offenders to perform immediate corrective action.

KEY FEATURES

- Displays detailed charts showing results and statistical information about users who fell for the phishing campaigns.
- Compares results of campaigns grouped by most failed users, templates, campaigns, departments, as well as any other groupings uploaded into the Platform.
- Shows repeat offenders who can be grouped and targeted for additional training.
- Outlines the comparisons of failure results for different users, departments, templates, campaigns and campaign types all in one report.
- Export options: Excel and CSV.

SAMPLE PHISHING USER PERFORMANCE REPORT

(see next page)
SAMPLE PHISHING USER PERFORMANCE REPORT (CONT.)

Phishing User Performance

Analysis used interactions with simulated phishing attack campaigns, causes of failure, and identify repeat clickers for future campaigns and training.

Data updated twice a day. Last update 2020-04-05 at 18:54 (UTC) (approximately or hour ago).

<table>
<thead>
<tr>
<th>Overall Failure Rate (%)</th>
<th>Failed Users</th>
<th>Unique Failures</th>
<th>Threats Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>34.4%</td>
<td>80</td>
<td>84</td>
<td>244</td>
</tr>
</tbody>
</table>

Aggregate By

<table>
<thead>
<tr>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
</tr>
</tbody>
</table>

User Platform Status

<table>
<thead>
<tr>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
</tr>
</tbody>
</table>

Campaign Type

<table>
<thead>
<tr>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
</tr>
</tbody>
</table>

Campaign Status

<table>
<thead>
<tr>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completed</td>
</tr>
</tbody>
</table>

Template Name

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>KT37 Simulated Payment</td>
</tr>
<tr>
<td>Building Renovation Plan</td>
</tr>
<tr>
<td>Direct Password Change</td>
</tr>
<tr>
<td>Staff Transfer</td>
</tr>
</tbody>
</table>

Campaign Name

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020 Phishing Campaign 4</td>
</tr>
<tr>
<td>2020 Phishing Campaign 5</td>
</tr>
<tr>
<td>2020 Phishing Campaign 6</td>
</tr>
<tr>
<td>Attachment</td>
</tr>
</tbody>
</table>

User Details

<table>
<thead>
<tr>
<th>First Name</th>
<th>Last Name</th>
<th>Email Address</th>
<th>Last Exit Date</th>
<th>Days To Exit</th>
<th>Unique Failure Rate (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Andrew</td>
<td>Carter</td>
<td><a href="mailto:andrew.carter@proofpoint.com">andrew.carter@proofpoint.com</a> 2000-01-13</td>
<td>1</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Aparajita</td>
<td>Gopinath</td>
<td><a href="mailto:aparajita.gopinath@proofpoint.com">aparajita.gopinath@proofpoint.com</a> 2000-01-13</td>
<td>1</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Aparajita</td>
<td>Rangan</td>
<td><a href="mailto:aparajita.rangan@proofpoint.com">aparajita.rangan@proofpoint.com</a> 2000-01-13</td>
<td>1</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Aparajita</td>
<td>Linus</td>
<td><a href="mailto:aparajita.linus@proofpoint.com">aparajita.linus@proofpoint.com</a> 2000-01-13</td>
<td>1</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Aparajita</td>
<td>Angin</td>
<td><a href="mailto:aparajita.angin@proofpoint.com">aparajita.angin@proofpoint.com</a> 2000-01-13</td>
<td>1</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Aparajita</td>
<td>Virgil</td>
<td><a href="mailto:aparajita.virgil@proofpoint.com">aparajita.virgil@proofpoint.com</a> 2000-01-13</td>
<td>1</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Aparajita</td>
<td>Linus</td>
<td><a href="mailto:aparajita.linus@proofpoint.com">aparajita.linus@proofpoint.com</a> 2000-01-13</td>
<td>1</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Aparajita</td>
<td>Lew</td>
<td><a href="mailto:aparajita.lew@proofpoint.com">aparajita.lew@proofpoint.com</a> 2000-01-13</td>
<td>1</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Andrew</td>
<td>Wood</td>
<td><a href="mailto:andrew.wood@proofpoint.com">andrew.wood@proofpoint.com</a> 2000-01-13</td>
<td>1</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Andrew</td>
<td>Vinod</td>
<td><a href="mailto:andrew.vinod@proofpoint.com">andrew.vinod@proofpoint.com</a> 2000-01-13</td>
<td>1</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Andrew</td>
<td>Tanak</td>
<td><a href="mailto:andrew.tanak@proofpoint.com">andrew.tanak@proofpoint.com</a> 2000-01-13</td>
<td>1</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Andrew</td>
<td>Gopinath</td>
<td><a href="mailto:andrew.gopinath@proofpoint.com">andrew.gopinath@proofpoint.com</a> 2000-01-13</td>
<td>1</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Andrew</td>
<td>Tanak</td>
<td><a href="mailto:andrew.tanak@proofpoint.com">andrew.tanak@proofpoint.com</a> 2000-01-13</td>
<td>1</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
</tbody>
</table>

Template Details and Benchmarks

<table>
<thead>
<tr>
<th>Template Name</th>
<th>Days To Exit</th>
<th>Unique Failure Rate (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Password Change</td>
<td>24</td>
<td>0.00%</td>
</tr>
<tr>
<td>Building Renovation Plan</td>
<td>48</td>
<td>100.00%</td>
</tr>
<tr>
<td>Swift Transfer</td>
<td>2</td>
<td>50.00%</td>
</tr>
</tbody>
</table>
THREATSIM CAMPAIGN OVERVIEW REPORT

OBJECTIVE

The ThreatSim Campaign Overview report provides an at-a-glance view into the short-term phishing performance of simulated phishing campaigns and associated user activity. Information displayed includes:

- Click rate
- Multiple clicks
- No response
- Open messages
- Attachment opened
- Users who reported the mock phish
- Users who acknowledged viewing the Teachable Moment
- Browser vulnerabilities
- Compromised users (provided credentials to a fake site)

BENEFITS

- Quickly view the organization’s recent phishing campaign performance, analyze trends, and determine next steps in your program.
- Scan campaign results side-by-side and determine which campaigns are most effective for the organization.

KEY FEATURES

- Provides a bar chart of campaigns detailing and comparing the results with the ability to display campaigns over a period of up to a year.
- Displays a list of all the campaigns, overall results, create, start and end dates, status, and creator of each campaign. They can be filtered by status, shown as numbers or percentages.
- Export option: CSV

SAMPLE THREATSIM CAMPAIGN OVERVIEW REPORT
THREATSIM REPORTS ON INDIVIDUAL CAMPAIGN DETAILS

OBJECTIVE

Within the ThreatSim Campaign Overview report, each campaign can be accessed to provide administrators with statistical details in a variety of reports. Refer to the reports below.

BENEFIT

Easily analyze comprehensive details of each campaign to determine riskiest users, geography, IP addresses, devices (desktop vs mobile), and browser plug-in vulnerabilities.

SAMPLE THREATSIM INDIVIDUAL CAMPAIGN DETAILS REPORTS

All Campaigns History Report

Provides statistical details about each campaign, including visibility into past, current, and pending campaigns.
Individual Campaign Overview Report
Displays relevant incident response data such as time-to-click, time-to-open, time-to-report, time-to-open attachments, user clicks vs. no responses, vulnerable vs. non-vulnerable users, compromised vs. non-compromised users, and acknowledged vs. non-acknowledged users. Option to print Executive Summary.

Geographic Distribution Report
Displays worldwide mapping of user activity per campaign, which helps identify anomalies in the organization’s data regions with high levels of susceptibility.
Endpoints Report
Indicates the types of devices (desktop vs. mobile), operating systems, browsers, and browser versions that were used by employees who fell for a mock phishing email. Also reports on out-of-date and potentially vulnerable third-party plug-ins (via the optional Weak Network Egress feature).

Users Report
Shows detailed and complete user activity, including clicks, opens, and reported phish. Also identifies out-of-date third-party browser plug-ins and detection of off-end points (via the optional Weak Network Egress feature).
THREATSIM RAW CAMPAIGN DATA CSV REPORTS

OBJECTIVE

The ThreatSim Raw Campaign Data CSV reports provide user and user’s equipment details that are not available in other reports, reflecting all information available on campaigns in one report. Administrators can export all campaign data and build custom charts based on desired fields and stats.

BENEFIT

Simple export of comprehensive ThreatSim data for quick and easy import into the organization’s preferred analysis tool for evaluation.

KEY FEATURES

- Located under the campaign overview page under Export Data > Campaign History.
- Provides raw data of all campaigns within a selected range, which enables administrators to manipulate and create different charts from the results.
- Displays details about campaigns such as campaign title, type, template used, from name and from email fields, summarized results, and many other fields.
- Export option: CSV

SAMPLE THREATSIM RAW CAMPAIGN DATA CSV REPORTS

Campaign Overview CSV Report

Campaign History CSV Report

Campaign Details CSV Report
THREATSIM USB CAMPAIGN DETAILS REPORT

OBJECTIVE

The ThreatSim USB Campaign Details report shows the number of USB devices that were accessed and the IP addresses of the users who fell for the USB drop.

BENEFITS

- Examine the organization’s recent USB campaigns and performance at a glance, analyze the details, and determine the next steps in cybersecurity training programs.
- View USB campaign results and determine which campaigns are most effective for the organization.

KEY FEATURES

- Provides the number of USBs that had no response, one-click or multi-clicked responses, and the total number of users who acknowledged the Teachable Moment.
- Displays details about the USBs within each campaign, USB unique ID, external and internal IP addresses of users’ PCs as well as the Windows login used on the PC.
- Lists the filename the user fell for and clicked on.
- Shows the event types and when an event took place.
- Export options: PNG, JPEG, SVG and PDF.

SAMPLE THREATSIM USB CAMPAIGN DETAILS REPORT
REPORTED EMAIL PERFORMANCE & ANALYSIS REPORTS

The reports in this section pertain to PhishAlarm and PhishAlarm Analyzer. They include:

- PhishAlarm Analyzer Results Report
- Reported Email Performance Report

PHISHALARM ANALYZER RESULTS REPORT

OBJECTIVE

The PhishAlarm Analyzer Results report shows the number of reported threats identified over time (hours, day, weeks, months, quarters). Results are displayed for the three classification categories – “Likely a Phish,” “Suspicious,” and “Not Likely a Phish” – for all email domains analyzed by PhishAlarm Analyzer.

BENEFITS

- Quickly review the total number, types, and trends of phishing emails reported for a given period so you can gauge the effectiveness of your awareness and training of reporting suspected phish.
- Evaluate users’ ability to identify and report actual phishing emails and track performance over time.

KEY FEATURES

- Provides the total number of phishing emails reported monthly.
- Shows the trend of reported emails over a specific date range.
- Assists in identifying the overall understanding of cybersecurity topics within an organization based on the emails reported as well as the trend of the type of emails reported.
- Breaks down the number of emails reported, per category.
- Export option: CSV

SAMPLE PHISHALARM ANALYZER RESULTS REPORT

(see next page)
SAMPLE PHISHALARM ANALYZER RESULTS REPORT (CONT.)

PhishAlarm Analyzer Report

Select a Date Range

---

Total Potential Phish This Month

1590 ↓

down 76% since last month

---

Likely Phish

597 ↓

down 78% since last month

Suspicious Phish

71 ↓

down 74% since last month

Unlikely Phish

922 ↓

down 81% since last month

---

© 2020 Proofpoint, Inc. Private and confidential.
REPORTED EMAIL PERFORMANCE REPORT

OBJECTIVE

The Reported Email Performance report displays the information reported by end users via the PhishAlarm button. It lists the users’ names and email addresses, type of email (simulated phish, training email, or potential phish), action taken by end users (opened, unopened with preview, or unopened), associated phishing campaign name, and time elapsed to report potential phish. Additional information, such as the end users’ operating system and email client version, can also be displayed.

BENEFITS

- Gauge end users’ ability to identify phishing emails and their responsiveness to reporting phish to determine further training needs.
- Identify most active and accurate phish reporters for rewards and recognition.

KEY FEATURES

- Provides a variety of filtering options, such as email type, email action taken by users, and campaign name.
- Flexibility to select which data fields to include or exclude from the table to meet specific analysis needs.
- Displays key performance indicators for the total emails reported, potential phish, and simulated phish.
- Displays detailed results on who reported the email, the type of email reported (simulated phish, potential phish, or training email), the action taken by the end user (opened, unopened, or unopened with preview), and the associated phishing campaign.
- Provides an elapsed time stamp between the receipt of the email and the time reported.
- Specifies end users’ operating system and email client version.
- Export options: Excel and CSV

SAMPLE REPORTED EMAIL PERFORMANCE REPORT

(see next page)
TRAINING REPORTS

The reports in this section pertain to Training modules. They include:

- Knowledge Assessment & Training Progress Report
- Training Assignment Performance Report
- Training Category Performance Report
- Training Module Performance Report

KNOWLEDGE ASSESSMENT & TRAINING PROGRESS REPORT

Refer to Knowledge Assessment and Training Progress Report under Knowledge Assessment.

TRAINING ASSIGNMENT PERFORMANCE REPORT

OBJECTIVE

The Training Assignment Performance report provides comprehensive user-level information for training assignments. Administrators can drill down to the user-level and module-level to view several data points, including standard information such as user module score percentage, time to complete the module, and total questions answered.

BENEFITS

- Easily view and analyze detailed user-level results, progress, and completion rates across training assignments and modules.
- Use gathered information to notify users who have not completed assignments, identify poorly performing users for further training, and identify top performing users for rewards and recognition.

KEY FEATURES

- View detailed results about progress and assignment completions for users within an assignment.
- Flexibility to select and display different column headers within the report, to see progress by different departments, regions, or other properties.
- Administrators can include or exclude deleted assignments, deleted users, and users removed from assignments in their view.
- Ability to create and save different views based on Administrator’s preferences.
- Export options: Excel and CSV.

SAMPLE TRAINING ASSIGNMENT PERFORMANCE REPORT

(see next page)
SAMPLE TRAINING ASSIGNMENT PERFORMANCE REPORT (CONT.)

Training Assignment Performance

Review detailed user and assignment scores, progress, and completion rates across training assignments and modules.

Data updated twice a day. Last update: 2020-04-08 at 16:04 (UTC) (approximately an hour ago).

User Progress In Assignment

- In Progress: 54.04%
- Completed: 14.1%
- Not Started: 35.86%

Completion Rate (%)
- 14.1%

Unique Users
- 358

Assignments
- 79

Auto-Enrolled Assignments
- 66

Assignment Details

<table>
<thead>
<tr>
<th>Assignment Name</th>
<th>Assignment Start Date</th>
<th>Assigned Due Date</th>
<th>First Name</th>
<th>Last Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020 Phishing Campaign IA</td>
<td>2020-01-13</td>
<td>2020-01-13</td>
<td>Catherine</td>
<td>Barnes</td>
</tr>
<tr>
<td>2020 Phishing Campaign IA</td>
<td>2020-01-13</td>
<td>2020-01-13</td>
<td>Daniel</td>
<td>Ross</td>
</tr>
<tr>
<td>2020 Phishing Campaign IA</td>
<td>2020-01-12</td>
<td>2020-01-12</td>
<td>Eric</td>
<td>Kelly</td>
</tr>
<tr>
<td>2020 Phishing Campaign IA</td>
<td>2020-01-12</td>
<td>2020-01-12</td>
<td>George</td>
<td>Collins</td>
</tr>
<tr>
<td>2020 Phishing Campaign IA</td>
<td>2020-01-21</td>
<td>2020-01-21</td>
<td>James</td>
<td>Gray</td>
</tr>
<tr>
<td>2020 Phishing Campaign IA</td>
<td>2020-01-21</td>
<td>2020-01-21</td>
<td>Jeffrey</td>
<td>Hall</td>
</tr>
<tr>
<td>2020 Phishing Campaign IA</td>
<td>2020-01-21</td>
<td>2020-01-21</td>
<td>Jessica</td>
<td>Gray</td>
</tr>
<tr>
<td>2020 Phishing Campaign IA</td>
<td>2020-01-21</td>
<td>2020-01-21</td>
<td>Kevin</td>
<td>Bailey</td>
</tr>
<tr>
<td>2020 Phishing Campaign IA</td>
<td>2020-01-13</td>
<td>2020-01-13</td>
<td>Margaret</td>
<td>Johnson</td>
</tr>
</tbody>
</table>
TRAINING CATEGORY PERFORMANCE REPORT

OBJECTIVE

The Training Category Performance report tracks the questions and topics end users are having the most trouble with based on the training assignments they have completed. By highlighting weaknesses, an organization can more effectively focus on training efforts.

BENEFIT

Quickly pinpoint the most missed categories across training modules or by individual module so that security awareness training programs can be implemented to focus on those areas for improvement.

KEY FEATURES

- Provides a variety of filtering options, such as by training module name, date, assignment, and include/exclude deleted users.
- Flexibility to select which data fields to include or exclude from the table to meet specific analysis needs.
- Displays key performance indicators for the total number of training modules, categories, correct responses, and incorrect responses.
- Clearly identifies the most missed training categories in a bar chart.
- Ability to view per category details on percentage and total number of incorrect and correct questions and total user responses.
- Ability to view user-level details on how many questions were answered correctly and incorrectly, the corresponding category, module, and assignment names, and the module and assignment completion dates.
- Results include topics in modules taken as part of an assignment and as a standalone (Free Play).
- Export options: Excel and CSV

SAMPLE TRAINING CATEGORY PERFORMANCE REPORT

(see next page)
SAMPLE TRAINING CATEGORY PERFORMANCE REPORT (CONT.)

View includes Category Tab

Training Category Performance
Evaluate end user training performance by content category across training modules to identify weak knowledge areas for improvement.

Data updated twice a day. Last update: 2020-Apr-08 at 16:04 (UTC) (approximately 2 hours ago)

<table>
<thead>
<tr>
<th>Number of Modules</th>
<th>Number of Categories</th>
<th>Correct Responses</th>
<th>Incorrect Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>140</td>
<td>16,168</td>
<td>2,285</td>
</tr>
</tbody>
</table>

Most Missed Categories
- Security managing passwords
- Using password managers
- Creating Strong Phrases
- Identity app basics
- Insecure storage
- Technical debt etiquette
- Handling sensitive data
- Verifying links in Email
- Accessing secret resources
- Recognizing Spoofing Email
- Required compliance
- Downloading, Installing apps or software
- Defining passwords...

Category Details

<table>
<thead>
<tr>
<th>Category Name</th>
<th>Incorrect Question Percent</th>
<th>Correct Question Percent</th>
<th>Total User Responses</th>
<th>Incorrect Responses</th>
<th>Correct Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to Restricted Areas</td>
<td>50.00%</td>
<td>50.00%</td>
<td>16,168</td>
<td>2,285</td>
<td>14</td>
</tr>
<tr>
<td>Apply basic test procedures...</td>
<td>15.00%</td>
<td>85.00%</td>
<td>85</td>
<td>10</td>
<td>75</td>
</tr>
<tr>
<td>Assess the risk...</td>
<td>75.00%</td>
<td>25.00%</td>
<td>25</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Avoiding Phishing Scams</td>
<td>10.00%</td>
<td>90.00%</td>
<td>90</td>
<td>10</td>
<td>80</td>
</tr>
<tr>
<td>Real Phishing</td>
<td>10.00%</td>
<td>90.00%</td>
<td>90</td>
<td>10</td>
<td>80</td>
</tr>
<tr>
<td>Distraction in Browsing</td>
<td>10.00%</td>
<td>90.00%</td>
<td>90</td>
<td>10</td>
<td>80</td>
</tr>
<tr>
<td>Business Security</td>
<td>10.00%</td>
<td>90.00%</td>
<td>90</td>
<td>10</td>
<td>80</td>
</tr>
<tr>
<td>Business Data on Home Computer</td>
<td>10.00%</td>
<td>90.00%</td>
<td>90</td>
<td>10</td>
<td>80</td>
</tr>
<tr>
<td>Connecting to Safe WIFI</td>
<td>10.00%</td>
<td>90.00%</td>
<td>90</td>
<td>10</td>
<td>80</td>
</tr>
<tr>
<td>Corporate Mobile Device Policy</td>
<td>10.00%</td>
<td>90.00%</td>
<td>90</td>
<td>10</td>
<td>80</td>
</tr>
<tr>
<td>Create a Password Family</td>
<td>10.00%</td>
<td>90.00%</td>
<td>90</td>
<td>10</td>
<td>80</td>
</tr>
<tr>
<td>Defining passwords</td>
<td>10.00%</td>
<td>90.00%</td>
<td>90</td>
<td>10</td>
<td>80</td>
</tr>
<tr>
<td>Detecting Smudge Passwords</td>
<td>10.00%</td>
<td>90.00%</td>
<td>90</td>
<td>10</td>
<td>80</td>
</tr>
<tr>
<td>Defining passwords</td>
<td>10.00%</td>
<td>90.00%</td>
<td>90</td>
<td>10</td>
<td>80</td>
</tr>
<tr>
<td>Dangerous URLs at Symbol</td>
<td>10.00%</td>
<td>90.00%</td>
<td>90</td>
<td>10</td>
<td>80</td>
</tr>
</tbody>
</table>

© 2020 Proofpoint, Inc. Private and confidential.
# View of Users Tab

<table>
<thead>
<tr>
<th>Category Name</th>
<th>First Name</th>
<th>Last Name</th>
<th>Email Address</th>
<th>Contact Res</th>
<th>Incor. Res</th>
<th>Module (Admin)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to Restricted Areas</td>
<td>Cynthia</td>
<td>Perry</td>
<td><a href="mailto:cynthia.perry@amyyo.workbaza.com">cynthia.perry@amyyo.workbaza.com</a></td>
<td>1</td>
<td>0</td>
<td>Workplace Sx</td>
</tr>
<tr>
<td>Access to Restricted Areas</td>
<td>Donald</td>
<td>Martin</td>
<td><a href="mailto:donald.martin@amyyo.workbaza.com">donald.martin@amyyo.workbaza.com</a></td>
<td>2</td>
<td>1</td>
<td>Workplace Sx</td>
</tr>
<tr>
<td>Access to Restricted Areas</td>
<td>Dorothy</td>
<td>Rostar</td>
<td><a href="mailto:dorothy.rostar@amyyo.workbaza.com">dorothy.rostar@amyyo.workbaza.com</a></td>
<td>1</td>
<td>0</td>
<td>Workplace Sx</td>
</tr>
<tr>
<td>Access to Restricted Areas</td>
<td>Emily</td>
<td>Sanchez</td>
<td><a href="mailto:emily.sanchez@amyyo.workbaza.com">emily.sanchez@amyyo.workbaza.com</a></td>
<td>2</td>
<td>1</td>
<td>Workplace Sx</td>
</tr>
<tr>
<td>Access to Restricted Areas</td>
<td>Frank</td>
<td>Howard</td>
<td><a href="mailto:frank.howard@amyyo.workbaza.com">frank.howard@amyyo.workbaza.com</a></td>
<td>2</td>
<td>1</td>
<td>Workplace Sx</td>
</tr>
<tr>
<td>Access to Restricted Areas</td>
<td>Matthew</td>
<td>Ward</td>
<td><a href="mailto:matthew.ward@amyyo.workbaza.com">matthew.ward@amyyo.workbaza.com</a></td>
<td>1</td>
<td>1</td>
<td>Workplace Sx</td>
</tr>
<tr>
<td>Access to Restricted Areas</td>
<td>Melissa</td>
<td>Rogers</td>
<td><a href="mailto:melissa.rogers@amyyo.workbaza.com">melissa.rogers@amyyo.workbaza.com</a></td>
<td>2</td>
<td>1</td>
<td>Workplace Sx</td>
</tr>
<tr>
<td>Access to Restricted Areas</td>
<td>Michelle</td>
<td>Patterson</td>
<td><a href="mailto:michelle.patterson@amyyo.workbaza.com">michelle.patterson@amyyo.workbaza.com</a></td>
<td>1</td>
<td>0</td>
<td>Workplace Sx</td>
</tr>
<tr>
<td>Access to Restricted Areas</td>
<td>Ruth</td>
<td>Thompson</td>
<td><a href="mailto:ruth.thompson@amyyo.workbaza.com">ruth.thompson@amyyo.workbaza.com</a></td>
<td>1</td>
<td>0</td>
<td>Workplace Sx</td>
</tr>
<tr>
<td>Access to Restricted Areas</td>
<td>Shirley</td>
<td>Harris</td>
<td><a href="mailto:shirley.harris@amyyo.workbaza.com">shirley.harris@amyyo.workbaza.com</a></td>
<td>1</td>
<td>1</td>
<td>Workplace Sx</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Alexander</td>
<td>Hernandez</td>
<td><a href="mailto:alexander.hernandez@amyyo.workbaza.com">alexander.hernandez@amyyo.workbaza.com</a></td>
<td>2</td>
<td>0</td>
<td>PE in Action 2</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Amy</td>
<td>Brown</td>
<td><a href="mailto:amy.brown@amyyo.workbaza.com">amy.brown@amyyo.workbaza.com</a></td>
<td>1</td>
<td>1</td>
<td>PE in Action 2</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Angela</td>
<td>Robinson</td>
<td><a href="mailto:angela.robinson@amyyo.workbaza.com">angela.robinson@amyyo.workbaza.com</a></td>
<td>1</td>
<td>1</td>
<td>PE in Action 2</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Anna</td>
<td>Sanchez</td>
<td><a href="mailto:anna.sanchez@amyyo.workbaza.com">anna.sanchez@amyyo.workbaza.com</a></td>
<td>2</td>
<td>0</td>
<td>PE in Action 2</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Anthony</td>
<td>Griffin</td>
<td><a href="mailto:anthony.griffin@amyyo.workbaza.com">anthony.griffin@amyyo.workbaza.com</a></td>
<td>1</td>
<td>0</td>
<td>PE in Action 2</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Benjamin</td>
<td>Alexander</td>
<td><a href="mailto:benjamin.alexander@amyyo.workbaza.com">benjamin.alexander@amyyo.workbaza.com</a></td>
<td>2</td>
<td>0</td>
<td>PE in Action 2</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Carol</td>
<td>Hamond</td>
<td><a href="mailto:carol.hamond@amyyo.workbaza.com">carol.hamond@amyyo.workbaza.com</a></td>
<td>1</td>
<td>0</td>
<td>PE in Action 2</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Carleen</td>
<td>Lewis</td>
<td><a href="mailto:carleen.lewis@amyyo.workbaza.com">carleen.lewis@amyyo.workbaza.com</a></td>
<td>1</td>
<td>1</td>
<td>PE in Action 2</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Deborah</td>
<td>Carter</td>
<td><a href="mailto:deborah.carter@amyyo.workbaza.com">deborah.carter@amyyo.workbaza.com</a></td>
<td>1</td>
<td>1</td>
<td>PE in Action 2</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Dorothy</td>
<td>Fowler</td>
<td><a href="mailto:dorothea.fowler@amyyo.workbaza.com">dorothea.fowler@amyyo.workbaza.com</a></td>
<td>2</td>
<td>0</td>
<td>PE in Action 2</td>
</tr>
</tbody>
</table>
TRAINING MODULE PERFORMANCE REPORT

OBJECTIVES

The Training Module Performance report displays results and information for Training modules. It tracks individual completion rates and attempts for specific or multiple modules, whether part of an assignment or not, in addition to capturing whether the user responded to a policy acknowledgment statement added through our Training Jacket feature. The report displays average scores for each module, in addition to individual user’s scores. It also tracks and ranks completion rates for individuals and departments to help determine best performing groups.

BENEFITS

- Easily view and monitor users’ training module completion status, completion rate, and scores.
- Identify cybersecurity awareness topics where individuals are strongest and weakest so that future training programs can be tailored accordingly.
- View training completion percentage and average score by module.
- Review detailed scores for each module and compare results across modules.
- Clearly identify users who have acknowledged, declined, or took no action on the company-specified policy acknowledgment to comply with organizational policies.
- Quickly identify leaderboard data showing best performing individuals or departments on training module assignment completion time and scores for rewards and recognition and, conversely, identify lower performing individuals or departments to determine action plans for improvement.

KEY FEATURES

- Provides a variety of filtering options, such as by module name, status, and attempt start date as well as user completion status.
- Flexibility to select which data fields to include or exclude from the table to meet specific analysis needs.
- Displays key performance indicators for the number of modules, assigned modules, attempts and completion.
- Provides detailed results about which users attempted or completed a specific module as part of an assignment or standalone (Free Play).
- Tracks user-level scores on modules taken within or outside of an assignment.
- Displays an overall acceptance rate percentage as well as a breakdown of who accepted, declined, or took no action on the Policy Acknowledgement inserted in a Training Jacket of the modules.
- Provides an exportable Leaderboard table that ranks all users with a formula that uses completion time and module scores across any combination of training modules.
- Reflects a score distribution for users who are part of an assignment.
- Export options: Excel and CSV

SAMPLE TRAINING MODULE PERFORMANCE REPORT

(see next page)
SAMPLE TRAINING MODULE PERFORMANCE REPORT (CONT.)

View includes Module Performance Tab

Training Module Performance

Track end user completion rates on specific training modules and how they performed in their training individually and in aggregate to identify their strong and weak topic areas.

Data updated twice a day. Last update: 2020-04-08 at 16:04 (UTC) (approximately 2 hours ago)

Unique Modules: 49
Modules Assigned: 1,312
Module Attempts: 1,312
Module Completion: 1,312 (100%)

Training Completion Percentage by Module

Average Score by Module

User Participation

© 2020 Proofpoint, Inc. Private and confidential.
View of Training Module Status by User Tab

View of Training Leaderboard Tab
View of Policy Acknowledgement Tab

<table>
<thead>
<tr>
<th>First Name</th>
<th>Last Name</th>
<th>Email Address</th>
<th>Date of Acknowledgment</th>
<th>Module User Display</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kathleen</td>
<td>Perez</td>
<td><a href="mailto:Kathleen.perez@emptyemail00.com">Kathleen.perez@emptyemail00.com</a></td>
<td>2020-05-17 00:55:54 PM</td>
<td>Data Entry Printing</td>
</tr>
<tr>
<td>Kathleen</td>
<td>Perez</td>
<td><a href="mailto:Kathleen.perez@emptyemail00.com">Kathleen.perez@emptyemail00.com</a></td>
<td>2020-05-17 00:55:54 PM</td>
<td>Data Entry Printing</td>
</tr>
<tr>
<td>Kathleen</td>
<td>Perez</td>
<td><a href="mailto:Kathleen.perez@emptyemail00.com">Kathleen.perez@emptyemail00.com</a></td>
<td>2020-05-17 00:55:54 PM</td>
<td>Data Entry Printing</td>
</tr>
<tr>
<td>Kathleen</td>
<td>Perez</td>
<td><a href="mailto:Kathleen.perez@emptyemail00.com">Kathleen.perez@emptyemail00.com</a></td>
<td>2020-05-17 00:55:54 PM</td>
<td>Data Entry Printing</td>
</tr>
<tr>
<td>Kathleen</td>
<td>Perez</td>
<td><a href="mailto:Kathleen.perez@emptyemail00.com">Kathleen.perez@emptyemail00.com</a></td>
<td>2020-05-17 00:55:54 PM</td>
<td>Data Entry Printing</td>
</tr>
<tr>
<td>Kathleen</td>
<td>Perez</td>
<td><a href="mailto:Kathleen.perez@emptyemail00.com">Kathleen.perez@emptyemail00.com</a></td>
<td>2020-05-17 00:55:54 PM</td>
<td>Data Entry Printing</td>
</tr>
<tr>
<td>Samantha</td>
<td>Ramos</td>
<td><a href="mailto:Samantha.ramos@emptyemail00.com">Samantha.ramos@emptyemail00.com</a></td>
<td>2020-05-17 00:55:54 PM</td>
<td>Data Entry Printing</td>
</tr>
<tr>
<td>Samantha</td>
<td>Ramos</td>
<td><a href="mailto:Samantha.ramos@emptyemail00.com">Samantha.ramos@emptyemail00.com</a></td>
<td>2020-05-17 00:55:54 PM</td>
<td>Data Entry Printing</td>
</tr>
<tr>
<td>Samantha</td>
<td>Ramos</td>
<td><a href="mailto:Samantha.ramos@emptyemail00.com">Samantha.ramos@emptyemail00.com</a></td>
<td>2020-05-17 00:55:54 PM</td>
<td>Data Entry Printing</td>
</tr>
<tr>
<td>Samantha</td>
<td>Ramos</td>
<td><a href="mailto:Samantha.ramos@emptyemail00.com">Samantha.ramos@emptyemail00.com</a></td>
<td>2020-05-17 00:55:54 PM</td>
<td>Data Entry Printing</td>
</tr>
<tr>
<td>Joel</td>
<td>Diaz</td>
<td><a href="mailto:Joel.diaz@emptyemail00.com">Joel.diaz@emptyemail00.com</a></td>
<td>2020-05-17 00:55:54 PM</td>
<td>Data Entry Printing</td>
</tr>
</tbody>
</table>
USERS

The reports in this section pertain to User records. They include:

- User Record Export
- Training Report Card

USER RECORD EXPORT

OBJECTIVE

The User Record Export provides a complete list of users and assigned attributes that were uploaded into the Platform.

BENEFIT

Enables a backup copy of all users and user attributes to be saved, in the event of any potential maintenance issues.

KEY FEATURES

- Displays all your users and their attributes for reference.
- Exportable information to retain in the event of a recovery need.
- Export option: CSV

SAMPLE USER RECORD EXPORT

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Email</td>
<td>First Name</td>
<td>Last Name</td>
<td>Archive</td>
<td>Region</td>
<td>Department</td>
<td>Division</td>
<td>Manager</td>
</tr>
<tr>
<td>2</td>
<td>admin@amydemo1</td>
<td>Admin</td>
<td>Admin</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>super.admin@amydemo1</td>
<td>Admin</td>
<td>Admin</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>training.admin@amydemo1</td>
<td>Admin</td>
<td>Admin</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>simple.user@amydemo1</td>
<td>User1</td>
<td>User1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>complicated.user@amydemo1</td>
<td>User2</td>
<td>User2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>phishing.admin@amydemo1</td>
<td>Admin</td>
<td>Admin</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>simple.user@amydemo1</td>
<td>User3</td>
<td>User3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
...
TRAINING REPORT CARD

OBJECTIVE
The Training Report Card tracks the overall progress and performance of a single user, including scores for specific modules and a cumulative performance rating.

BENEFITS
- Quickly identify users who need extra training in specific topic areas.
- Track a user’s performance over time.

KEY FEATURES
- Displays a user’s overall status and progress, for all activities, in the Platform on one page.
- Allows an administrator to see all the modules that user completed or attempted, in two tables individually and cumulative on the same page.
- Displays all modules completed by a user (even if the user was removed from an assignment) as well as the best and most recent score for each module completed.
- Administrator can see all assignments that are assigned to a user and the status for each on one page.
- Export option: CSV

SAMPLE TRAINING REPORT CARD

![Training Report Card](image-url)