keepnet LABS

Keepnet Labs Cybersecurity Awareness Report

Cybersecurity Awareness Report Score: **D**

accelerate.

Table of Contents

1. Overview

Raising awareness amongst employees against phishing attacks and its possible outcomes are major precautions in ensuring the safety of an institution's cybersecurity. Phishing emails continue to be the primary method for cybercriminals for cyber attacks because they are more effective than other methods. Statistically;

- 95% of successful attacks on corporations start with a phishing email! [1]
- 97% of users do not notice a complicated phishing email. [2]
- Only 3% of users notice a phishing email and inform their management. [3]
- The total cost of cybercrime and data leaks for sectors is estimated at $ 2.1 trillion for 2019. [4]
- Phishing attacks will continue to be the primary method to be used in target-oriented/spear phishing attacks up to 2020 . [5]

Today, human error is the reason behind 90% of successful cyber attacks. For this reason, it is important for employees to recognise the phishing indicators in e-mail. Also, employees need continuous awareness training to obtain accurate information against evolving cyber threats as well as understanding of the different threats of social engineering attacks.

2. Executive Summary

In this report, cyber awareness of **Accelerate Technologies**'s employees against cyber threats has been analyzed. The situation of the users has been revealed and a general evaluation has been made according to the results of the simulation post campaign. **9** phishing campaigns were sent to **9** users. Furthermore, **10** trainings were assigned to **9** users.

2.1. Key Findings

9 carried out for **Accelerate Technologies**. Simulated phishing emails were sent to **9** users.

- Number of employees opened this fake email is **8** which corresponds to **88.89**% of total users.
- **4** employees clicked on the link in the fake email, that corresponds **44.44**% of users total users.
- **1** employees submitted their credentials to the fake landing page, that corresponds **11.11**% of total users.
- **9** people **0** users, **0.00 %** of total users opened attachment in tha fake email.
- Moreover,**1** users, **11.11**% total users choose not to respond to this email.
- When you look at Campaign Summary a total of **0** people reported this fake email a suspicious. The fact that a single target email account attacked by social engineers can lead to events that could jeopardize the entire system and the company, it is important to report suspicious emails to the related departments.

10 trainings were sent to a total number of **9** employees. **Accelerate Technologies** got the **31.40** score, which suggests company is "**F**".

- **6** users out of **9** total number opened training email, which corresponds to **66.67** % of total users.
- The number of employees clicked on the training link in email are **4**, **44.44**% of the total users.
- The number of employees completed the training is **1**, **11.11**% of the total users.
- The number of employees who gave no response to the training email is **5**, **55.56**% of the total users.

3. Grade

Total Score	Phishing Score	Training Score	Exam Score
D 47	C 63	F 31	F 0

Campaigns Count	Opened Rate	Clicked Rate	Captured Rate
9	88.89%	44.44%	11.11%

Trainings Count	Opened E-Mail Rate	Clicked E-Mail Rate	Training Duration
10	66.67%	44.44%	10.00%

3.1. Total Grade

As a result of all simulation and training, the overall score has been determined by the system as **D**. Although phishing simulations have major influence on grades, starting and finishing the training as well as s starting and finishing the exams including giving the correct answers, significantly influence the score. In general scorecard, evaluations have been made by taking the average of all the works done.

3.2. Total Phishing Grade

Total Phishing grade is the sum of Opened, Clicked, and Captured data. (Opened **88.89**%, Clicked **44.44**%, Captured **11.11**%). As seen in the picture 1, the phishing score determined by the system for **Accelerate Technologies** is **C**.

3.3. Total Training Grade

Total training grade is the sum of Opened, Clicked, and View Duration data (Opened **66.67**%, Clicked **44.44**%, View Duration **10.00**%). As seen in the picture 1, the training score determined by the system for **Accelerate Technologies** is **F**.

3.4. Benchmarking

The companies registered and used Keepnet Labs phishing simulation platform are also evaluated and given a score. **Accelerate Technologies** is give **D** , while the average of industry has **C** score.

4. Phishing Campaigns

4.1. CIN7 Billing-CIN7 Phishing

Accelerate Technologies got **D** score. The proportion of employees who leak information is **0.00%**. However, it is essential for users to be continuously prepared for cyber attacks and to provide the necessary infrastructure for the development of event response capabilities.

4.1.1. Phishing Email

Hi Zoe,

Please find below a link to your online statement which gives you access to your account status. You will be able to view all invoices and print them for your records.

My Online Statement
or if the link above does not work paste the url below into your address bar
https://go.cin7.com/Cloud/Account/Statement.aspx?ID=7130&SID=382860392

Please check your balance and if you have any enquiries contact us on billing@cin7.com.

Finally we have recently updated our terms and conditions which you can view here

Thank you and kind regards

Accounts Team

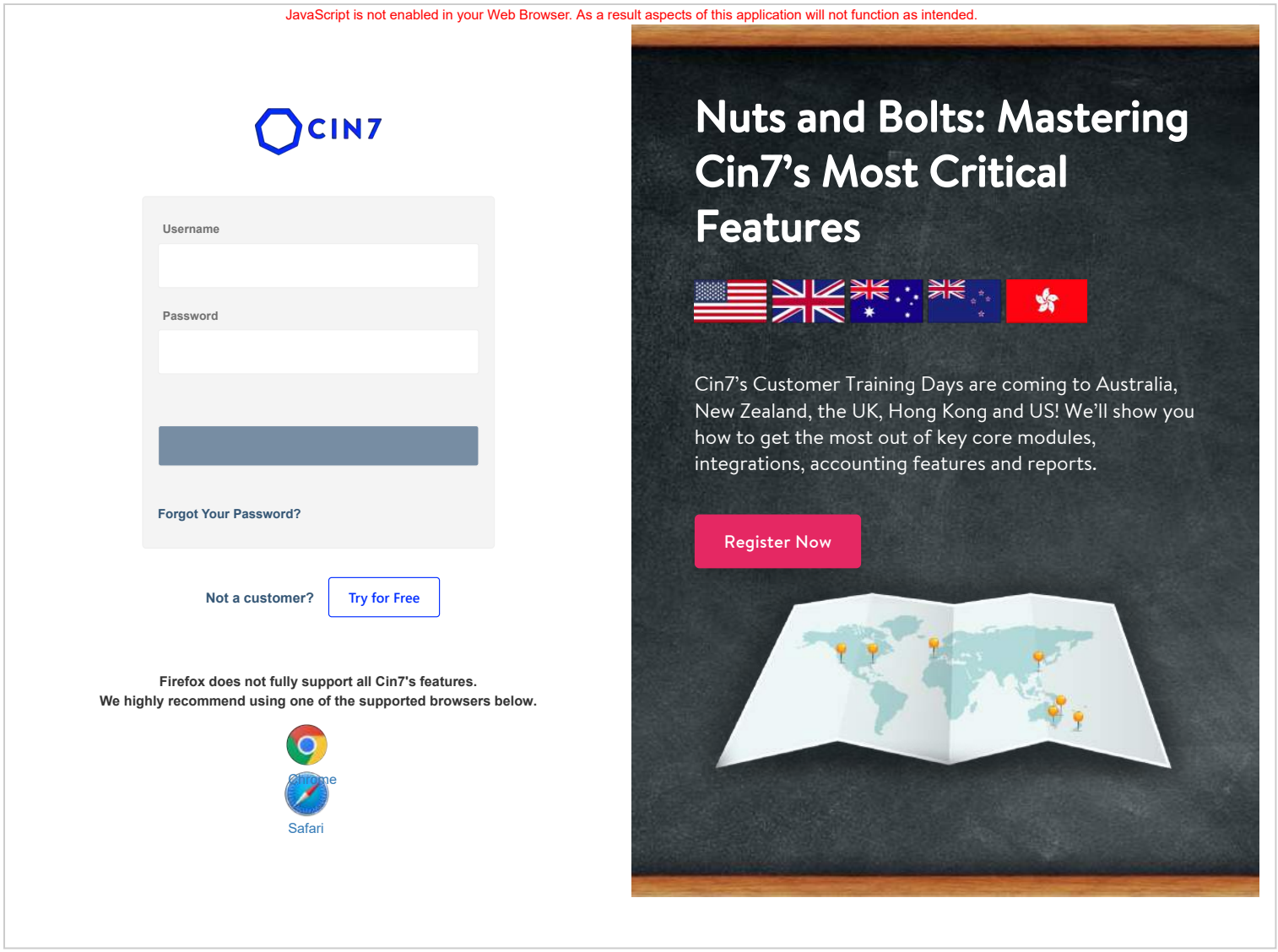
billing@cin7.com
P.O. Box 68 830, Newton, Auckland, New Zealand
cin7.com Level 12, 7 City Road, Auckland, New Zealand

Picture 1 : The Sample Phishing email used for the simulation(s)

Simulated phishing emails were sent to **1**. The Picture above demonstrates the sample simulated phishing email used in the phishing campaign(s).

4.1.2. Fake Landing Page

Once users clicked on the link in fake email, they will be redirected a fake page, as displayed in the Picture 2. below.



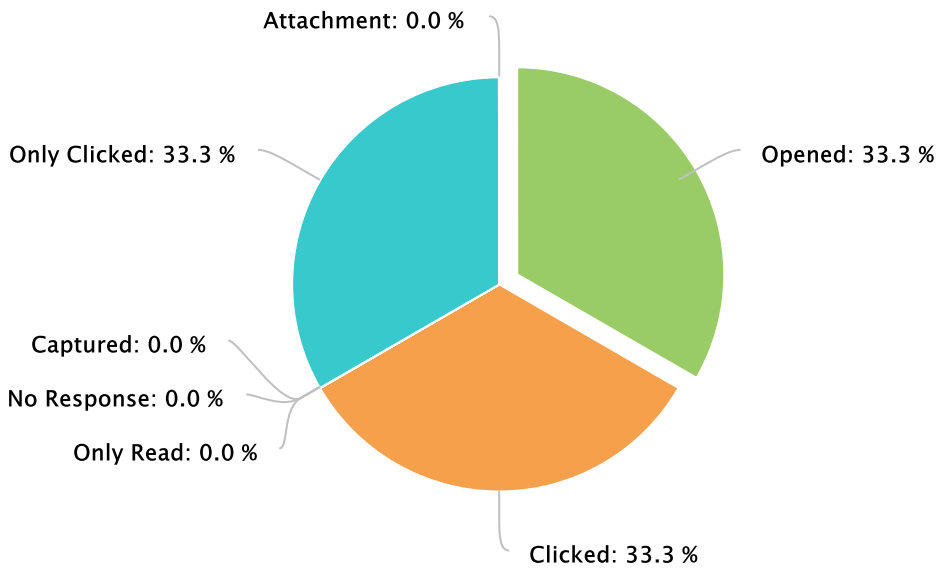
Picture 3 : The sample fake landing webpage used for the simulation(s)

If any user fills in the empty fields in the fake landing web page, he/she will hand over his/her data.

4.1.3. Key Findings

4.1.3.1. Campaign Summary

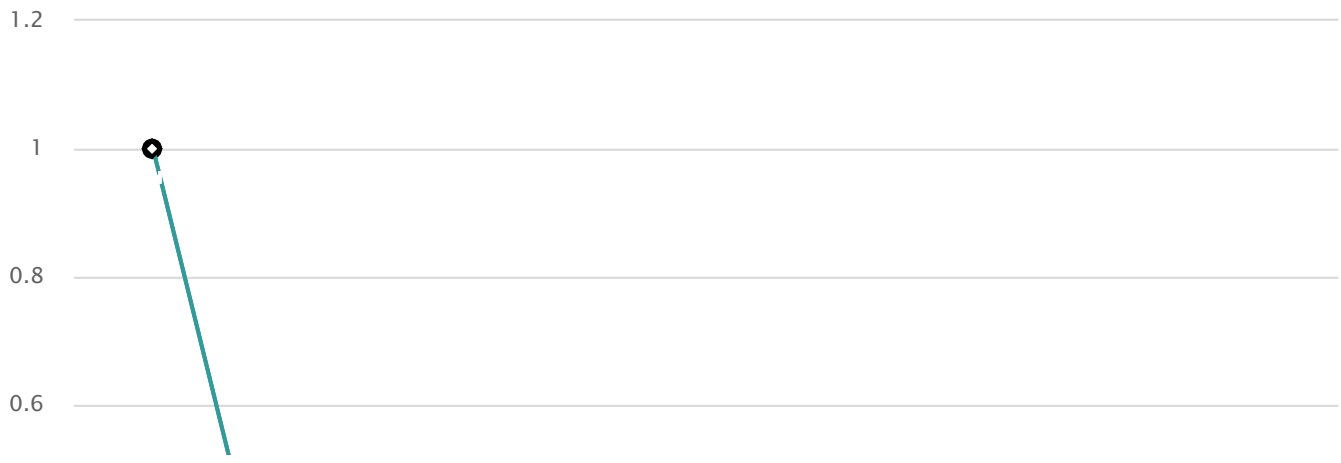
Campaign Name / Item Id	CIN7 Billing-CIN7 Phishing
Total Emails Sent	1
Opened E-Mail	1 - (100.00%)
Clicked Link In E-Mail	1 - (100.00%)
Submitted Form	0 - (0.00%)
Opened Attachment	0 - (0.00%)
Phishing Reporter	0 - (0.00%)
No Response	0 - (0.00%)
Started Time	9/2/2019 10:14:53 AM
Finished Time	9/2/2019 10:14:56 AM
E-Mail Groups	Darran Test

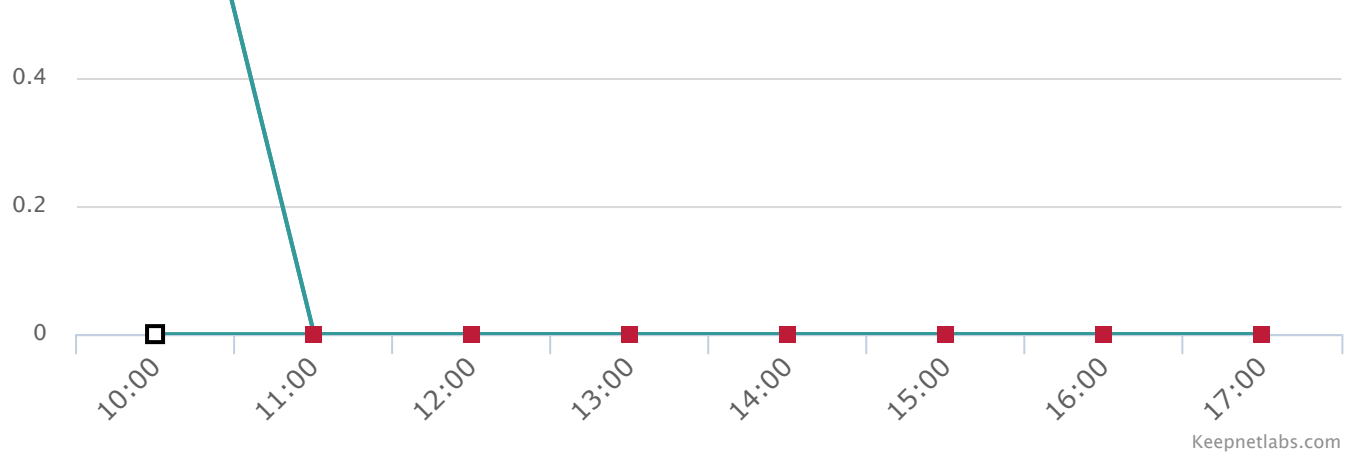


Picture 3 : Campaign Summary

Simulated phishing emails were sent to **1**. Number of employees opened this fake email is **1**, **100.00** % of total users. **1** employees, **100.00**% of users total users clicked on the link in the fake email. **0** employees, **0.00**% of total users submitted their credentials to the fake landing page. **0** people, **0.00** % of total users opened attachment in the fake email. Moreover, **0** users, **0.00** % total users choose not to respond to this email. When you look at Campaign Summary, a total of **0** people reported this fake email as suspicious.

First 8 Hours





Picture 4 : First 8 Hours

The image above indicates the interaction of employees with email and shows first 8 hours [6] of the opened email, clicked links and, submitted data.

4.1.3.2. Employees opened email

Email	Name	Surname	Department	Count
darran.clare@accelerate-technologies.com	Darran	Clare		1

Sample users opened simulated phishing email

Picture above shows the sample users who opened simulated phishing email. Number of users opened phishing email(s) is **1**, **100.00** % of total users. If you want to see the details of other users who opened the email, you can visit http://dashboard.keepnetlabs.com to download the campaign results by users; and if you need, you can compare campaign details of two different users the with benchmarking option.

4.1.3.3. Employees clicked links

Email	Name	Surname	Department	Count
darran.clare@accelerate-technologies.com	Darran	Clare		1

Sample users clicked on the fake link in the simulated phishing email

Picture above shows the sample users who clicked simulated phishing email. Number of users who clicked phishing email(s) is **1**, **100.00** % of total users [7]. If you want to see the details of other users who clicked the email, you can visit http://dashboard.keepnetlabs.com to download the campaign results by users; and if you need, you can compare campaign details of two different users the with benchmarking option.

4.1.3.4. Submitted Data

Nobody submit data.

Sample users submitted data on the fake web page

Picture above shows the sample users who submitted their data to the fake landing page. Number of users who submitted their data to the fake landing page **0**, **0.00** % of total users [8]. If you want to see the details of other users who submitted their data, you can visit http://dashboard.keepnetlabs.com to download the campaign results by users; and if you need, you can compare campaign details of two different users the with benchmarking option.

4.1.3.5. Opened Attachment

Nobody opened attachments.

Sample users opened fake attachment in the simulated simulated phishing email

Picture above shows the sample users who opened fake attachment in the simulated phishing email. Number of users who opened attachments in the fake email **0**, **0.00** % of total users [9]. If you want to see the details of other users who opened the email, you can visit http://dashboard.keepnetlabs.com to see the campaign results of different users; and if you need, you can compare campaign details of two different users the with benchmarking option.

4.1.3.6. Departments

Department Name	Send E-Mail	Opened E-Mail	Clicked E-Mail	Submitted Form	Opened Attachment
General	1	1	1	0	0

Top 10 risky departments

The most vulnerable units of **Accelerate Technologies** are shown in detail above picture. The users in the departments that have entered their information into the fraudulent website are listed in the most up-to-date list, only the first 10 departments are shown. If you want to see the details of other departments, you can visit http://dashboard.keepnetlabs.com to see the campaign results of different departments.

4.1.3.7. Phishing Reporter

Nobody used phishing reporter, yet. This means either phishing reporter add-in is not installed, or nobody is aware of the add-in, or low awareness against phishing attacks.

Sample of users reported suspicious email

The number of people who reported suspicious email is **0**. In the Picture above, 10 sample employee who reported suspicious email are shown in the order of letters. [10]

4.1.3.8. No Response

All of your users responded to the email.

Sample of users gave no response

Picture above shows the sample users who gave no response to simulated phishing email. Number of users who who did not respond to the fake email **0**, **0.00**% of total users. If you want to see the details of other users who did not respond to the fake email, you can visit http://dashboard.keepnetlabs.com

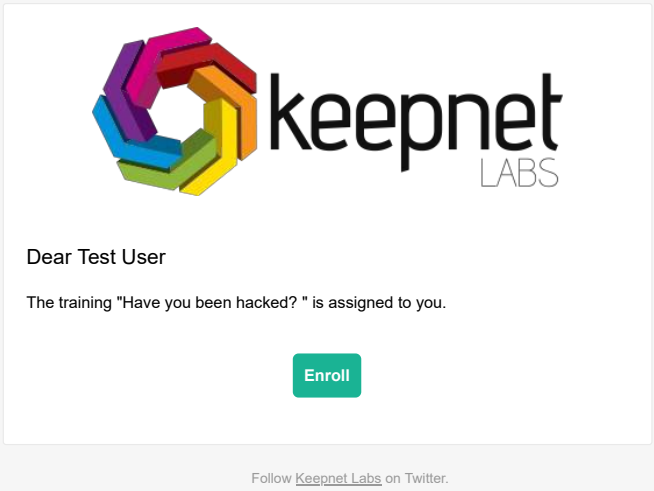
5. Training Campaigns

Since you didn't select any training campaign, the system generated the report of the last campaign you launched.

5.1. Have you been hacked?

The training emails were sent to a total number of **1** employees and **Accelerate Technologies** got **F** score.

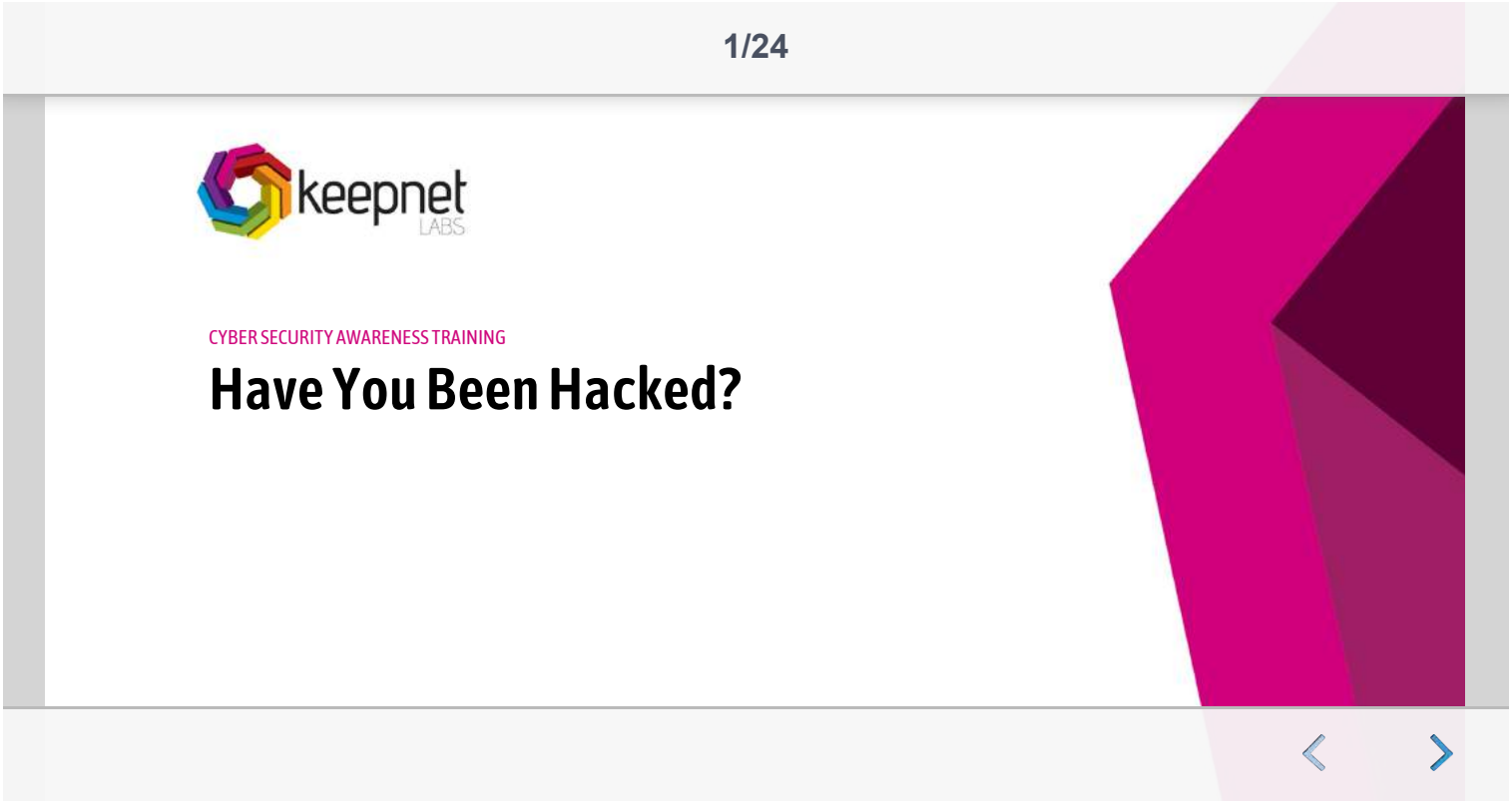
5.1.1. Sample Training Email



Picture 1 : Sample Training Email

The **Have you been hacked?** email was sent to the employees. Once users pressed the Enroll button, they were redirected to training page.

5.1.2. Sample Training Page



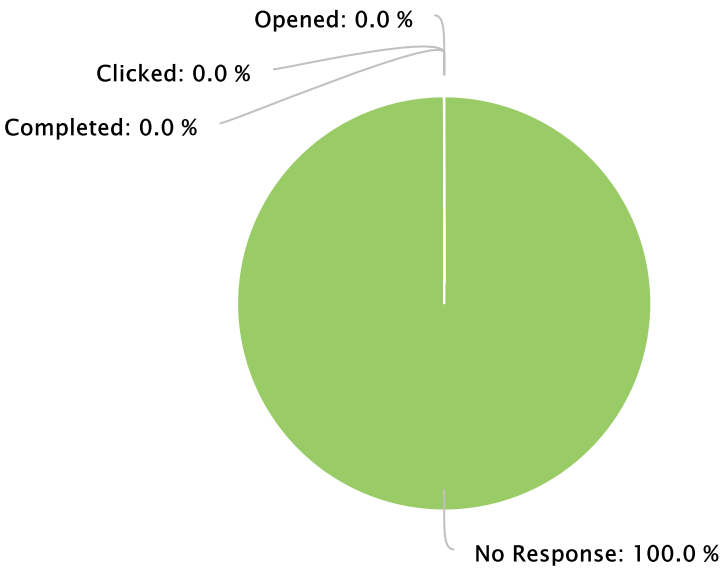
Picture 2 : Sample Training Preview

Have you been hacked? training was sent to the employees.

5.1.3. Key Findings

Training Summary

Training Name	Have you been hacked?
Details	Group Name:Darran Test
Total Training E-mails Sent	1
Opened Training E-Mail	0 - (0.00%)
Clicked Training E-Mail	0 - (0.00%)
Completed	0 - (0.00%)
No Response	1 - (100.00%)
Is Scheduled	No
Reminder Count	1



In training campaign(s), training emails were sent **1** employees. **0** users out of **1** total number opened training email, which is **0.00**% of total users. The number of employees clicked on the training link in email are **0**, **0.00**% of the total users. The number of employees completed the training is **0**, **0.00**% of the total users. The number of employees who gave no response to the training email is **1**, which is **100.00**% of the total users.

5.1.3.1. Sample Users Opened Training

Email	Name	Surname	Department	Count
darran.clare@accelerate-technologies.com	Darran	Clare		1

Sample Users Opened Training

The number of people who opened training(s) is **0**, which is **0.00**% of employees. In the picture above, sample users opened training are shown. If you want to see the details of other users who opened the training email, you can visit http://dashboard.keepnetlabs.com to see the training results of different users; and if you need, you can compare training details of two different users the with user compare option.

5.1.3.2. Time Spent on Education

Email	Name	Surname	Department	Duration Time	Duration
darran.clare@accelerate-technologies.com	Darran	Clare		158	100%

Time Spent on Education

The picture above is the example of the employees' training details such as completion state and view duration of the training. If you want to see the training details of other users, you can visit http://dashboard.keepnetlabs.com .

5.1.3.3. Exam Results

Date	Title	Email	Duration	Status	Score	Correct Answers
9/5/2019 12:00:00 AM	Have you been hacked	darran.clare@accelerate-technologies.com	00:01:34	True	80	4

The picture above is some example of the employees' exam details such as duration, score and correct answers. If you want to see the exam details of other users, you can visit http://dashboard.keepnetlabs.com .

6. Phishing Incident Response

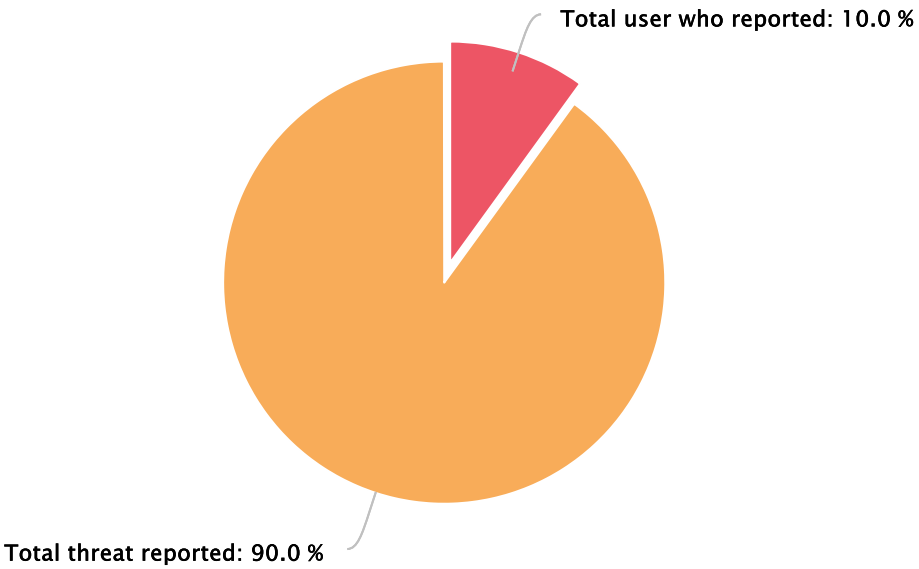
Phishing incident responder module is designed to allows users to report suspicious emails with a single click, sending the email content to Keepnet Labs for header, body and attachment analysis. According to the malware result, Incident Responder module creates a variety of attack signatures for alarm generation or blocking active security devices.

6.1. Key Findings

Total Endpoint : 0

No data avaible

Total Threat Reporter : 9



The number of active users using plugin is **0**. Total users using plugin are **0**.
Employees reported suspicious emails are **9** and **4** total active threats were discovered. Malicious tool constitutes **75.00%** of these threats ,

while phishing attacks constitute **25.00%**. Number of employees reported suspicious email is **11.11%** percent of users. Total number of threats reported is **9**.

Date	Report By	Subject	Attachment	Status
8/30/2019 10:50:24 AM	Darran.Clare@accelerate-technologies.com	3a4dba2b287fc77034ab269195827d79bd9e099d8db47484e22ec6343d91a3e6.exe	True	non-malicious
7/19/2019 9:22:26 AM	Darran.Clare@accelerate-technologies.com	File Format Exploits	True	malicious
8/30/2019 10:55:24 AM	Darran.Clare@accelerate-technologies.com	Fw: Unable to renew your TV Licence - 40277012	False	non-malicious
7/19/2019 9:22:26 AM	Darran.Clare@accelerate-technologies.com	File Format Exploits	True	malicious
8/30/2019 10:47:54 AM	Darran.Clare@accelerate-technologies.com	Request for Quote (SECU5039-1)	True	non-malicious
7/12/2019 2:49:20 PM	Darran.Clare@accelerate-technologies.com	Fw: [Alert] [New Statement update] Confirmation password changed from another IP Address CaseID: FTAXNVWTHG (7/4/2019 10:29:26 AM).[FWD]	True	malicious
9/3/2019 2:39:54 PM	Darran.Clare@accelerate-technologies.com	[New Webinar] Alleviate the stress of your Windows 7 migration	False	non-malicious
8/30/2019 10:09:07 AM	Darran.Clare@accelerate-technologies.com	Fw: Please change your account information, because someone has used your account to make suspicious payments.	True	non-malicious
7/12/2019 12:54:17 PM	Darran.Clare@accelerate-technologies.com	Password Change: Update Password Alert	False	phishing

Picture above displays some samples of the status of the suspicious emails reported by employees. Some are phishing, while some constitutes malicious tools. See in more detail at http://dashboard.keepnetlabs.com

7. Threat Intelligence

A data breach is a security incident that results from the unauthorized copying, display, playback or use of sensitive or protected data.

Company users lose their passwords due to hacking the platforms they are affiliated with by using corporate emails. Occasionally, malicious software infecting computers exposes e-mail addresses and passwords they get.

No data avaible

For **Accelerate Technologies**, **0** breach(es) detected.

No data avaible

Solution:

- In this case,they should develop early measures against leakage by the cyber intelligence services.
- Unpredictable, strong and different passwords must be created for different platforms.
- Antivirus software should be kept up to date and the most up-to-date operating systems must be used.
- Corporate emails must not be used for personal affairs.
- Links in e-mail must be paid attention and must be checked if the links are correct.

See in more detail at http://dashboard.keepnetlabs.com

8. Remediation

8.1. IT/SOC Department

The traditional protection methods are inadequate. However, Incident Responder module offers the most effective cyber attack detection and defense services with multiple alternatives, to protect you against ransomware, spear phishing and 0-day exploitation attacks targeting your email.
We have expert support with our professional phishing and malware analysis team and with the strength of other SOC companies around the world that we have agreement. In various SLA time, you have opportunity to get an in-depth analysis of phishing emails and malware from a specialized team. We offer sophisticated malicious software analysis support with SOC teams based UK, USA, Estonia, Bosnia ve Turkey.
Therefore we suggest the dissemination of this module which will cause employees to examine emails more carefully and turn them into an active cyber threat sensors.

8.1.1. Direct benefit to email user:

- Employees report aggressive attacks with a single click.
- Early "Phishing" warnings are taken from users and a "sensor" network is created.
- The user is notified of this correct action when he/she clicks the "Report Phishing" button in a simulated phishing security test.
- It allows the user to send a suspicious email to analysis services and get a risk score.
- Institution's security culture strengthens.
- Employees receive immediate feedback that enhances their training.

8.1.2. Benefits of Incident Responder to the Internet Technology (IT) department or security operation center (SOC) team:

- It is cost-effective: With built-in integrated services, you do not need to invest in any other anti-malware sandbox and anti-exploitation solutions.
- It will reduce the effort that you spend to analyse malicious emails for hours.
- Unwanted emails can be deleted from the user's email box with information received from the command center.
- It reports which email message is inbox of users.
- If the existing security measures are inadequate for analysis, detection and prevention, it gives the occasion to benefit from Keepnet Labs' analysis service.
- It provides more effective security measures with integration with third party systems (SIEM, Firewall, DLP etc.)

8.2. HR/Training Department

We suggest to the training department to use our posters, tip sheets and the other training materials on cyber security awareness regularly, Also, we suggest to the training department to execute all training activities with Keepnet Labs specialists to get most of them. For more information please visit https://www.keepnetlabs.com

8.3. Management Department

We recommend to the management department to govern all awareness process with Keepnet Labs and make an annual plan. For instance, the training department can use Keepnet Labs Phishing Planning Document if they will use Phishing Simulator module. For more information please visit https://www.keepnetlabs.com

9. References

[1] SANS. https://www.sans.org/
[2] Mcafe. https://www.mcafee.com/us/about/news/2015/q2/20150512-01.aspx
[3] Verizon. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
[4] Wired. https://www.wired.com/beyond-the-beyond/2017/07/global-cybercrime-costs-trillion-dollars-maybe-3/
[5] Gartner. https://www.gartner.com/technology/home.jsp
[6] The first 8 hours risk border threshold that any company have the chance to get over with the system breaches. Thus, the actions in the first 8 hours is manifested to expose the risk level the company faces.
[7] If there isn't any clicking fake link scenario in the phishing simulation campaign, there will not be any information about employees clicked on the fake link.
[8] If there isn't any data submission scenario in the phishing simulation campaign, there will not be any information about employees submitted their data to the fake landing page.
[9] If there is not any open attachment scenario in the phishing simulation campaign, there will not be any data about employees opened attachments.
[10] If you do not use Incident Responder module or have not installed the Phishing Deporter outlook add-in, there will not be any data about employees reported suspicious emails.