SLASHNEXT CLOUD EMAIL SECURITY

EXECUTIVE SUMMARY REPORT

Company: Muller and Phipps
Interval: 1 Year | Jan 22, 2020 to Feb 22, 2021
Date: Feb 22, 2021
Report generated by: Jason Clarke

TABLE OF CONTENTS

Overview

Email is essential for modern communication but vulnerable to exploitation by malicious actors. This report's primary aim is to provide a clear and insightful view of your organization's email security. Our goal is to offer data-driven insights that empower you to make informed decisions, fortify your cybersecurity measures, and ensure your organization's protection.

598 Inboxes Protected

89 Users Targeted

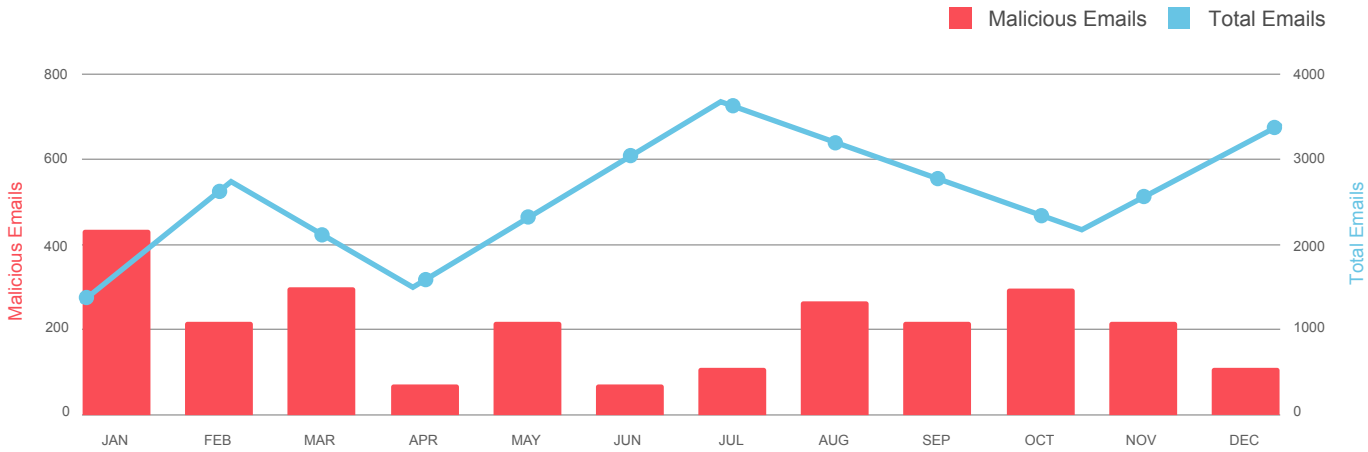
3256 Emails Scanned

784 Malicious Emails

84 Zero Hour Threat

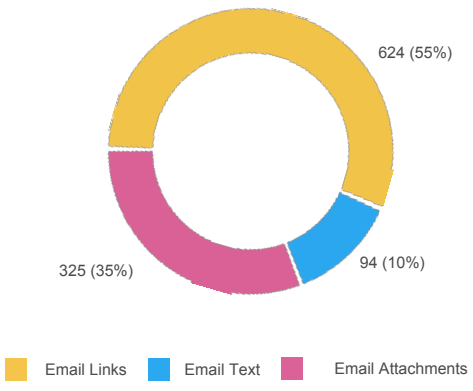
Email Threat

The information in this chart shows changes over time, depicting the overall count of scanned emails and the total number of malicious emails blocked.

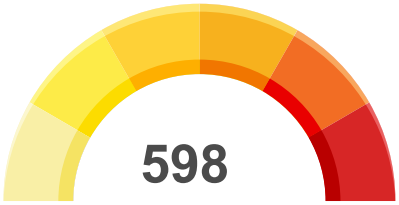


Attack Vectors Breakdown

The information in this chart describes the type of email threats blocked, based on vector. Email Text are BEC and social engineering emails are attacks that do not contain URLs or file attachments. Email Links are attacks that contain malicious URLs. Email Attachment are attacks that contain malicious files

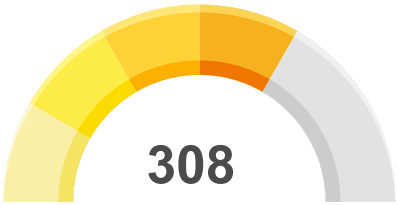


Email Threat Impact on Business



High Impact Emails Blocked

High-impact emails results in definite financial and other liabilities for the company should the attack be successful



Medium Impact Emails Blocked

Medium-impact emails results in potential financial and other liabilities for the company should attack be successful

Low Impact Emails Blocked

Low-impact emails results in low probability in financial and other liabilities for the company should the attack be successful

Top 10 Threats

The information in this chart contains the top 10 threats across the three attack vectors: Email Text, Email Links, and Email Attachments.

Threat	Threat Count
BEC: Assistance	124
BEC: Fund transfer	114
BEC: Gift card scam	107
BEC: Invoice fraud	101
BEC: Payroll theft	94
BEC: Reconnaissance	84
BEC: Request for Quotes	78
Credential Phishing	72
Malware & Exploits	68
Fraudulent Website	62

Top 10 Recipients

The information in this table are the recipients that have experienced the highest frequency of attacks.

Display Name	Email	Department	Role	Threat Count
Ruiqi Chen	ruiqi@company.com	Finance	Manager Accounts	432
Melissa Cantor	melissa@company.com	Finance	Assistant Manager Accounts	421
Franklin Tavarez	franklin@company.com	Sales	Sales Manager	395
Ryan Roslansky	ryan@company.com	Finance	Senior Manager Accounts	364
Daniel Shapero	daniel@company.com	Sales	Sales Specialist	345
Taylor Borden	taylor@company.com	Sales	Sales Engineering	338
Hari Srinivasan	hari@company.com	Finance	Chief Finance Officer	302
James Parry	james@company.com	Finance	Finance Manager	235
Cesar Cruz	cesar@company.com	Sales	Sales Operations Manager	185
Divya Devendran	divya@company.com	Sales	Marketing Manager	169

Top 10 Senders

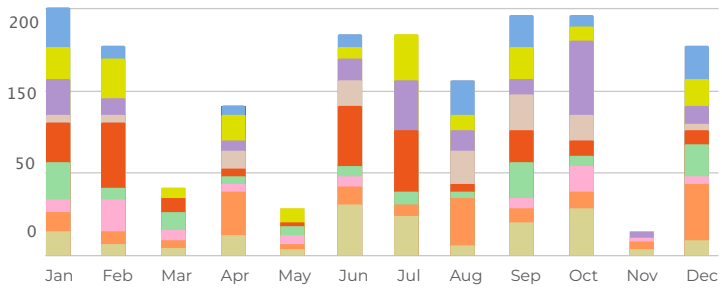
The information in this table are the senders responsible for the highest volume of attacks.

Display Name	Email	Domain	Threat Count
Jene Gordina	jene@dr.com	dr.com	432
Jack Bosma	jack@post.com	post.com	421
Ross Smith	ross@workmail.com	workmail.com	395
Colleen Hawk	colleen@contractor.com	contractor.com	364
Jenny Wang	jenny@consultant.com	consultant.com	345
Herbert Byerly	herbert@europe.com	europe.com	338
Robert Dum	robert@iname.com	iname.com	302
Joel Soderberg	joel@engineer.com	engineer.com	235
Christine Lopes	christine@planetmail.com	planetmail.com	185
Larry Felt	larry@workmail.com	workmail.com	169

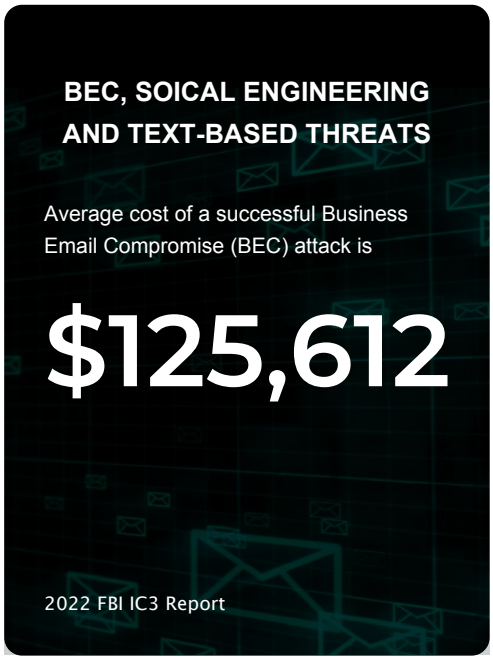
BEC, Social Engineering and Text-based Threats

598 Total BEC Attacks

198 Total SE Attacks

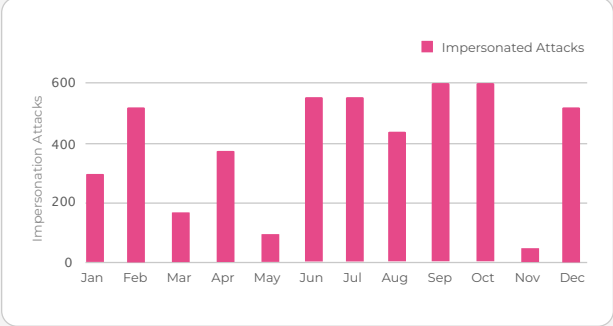


- BEC: Request of Payment 124 (74%)
- BEC: Data Exfiltration 104 (68%)
- SE: Intimidation 101 (62%)
- BEC: Invoice Fraud 94 (58%)
- BEC: Legal Support 84 (52%)
- SE: Flirtation 78 (48%)
- SE: Lottery Scam 72 (46%)
- SE: Intimidation 68 (42%)
- SE: Loan Offer 62 (40%)
- SE: Reward 52 (36%)



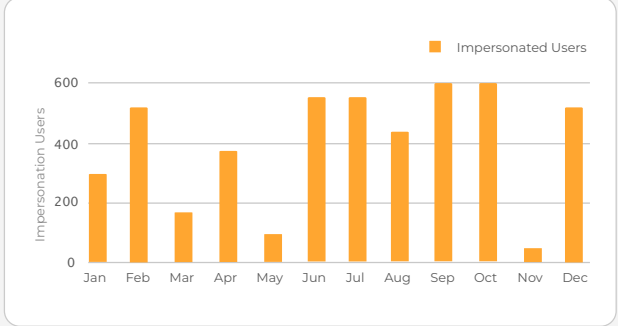
Impersonation Attacks

Impersonated attacks refer to attacks in which the sending display name is manipulated to appear as one of your employees. This table will be blank if impersonation attacks did not occur in the reporting period.



Impersonated Users

The information in this chart hows the number of employee names used in impersonation attacks. This table will be blank if impersonation attacks did not occur in the reporting period.



Top 10 Impersonated Users

The information in this table are the employees that are most frequently impersonated.

Display Name	Email	Department	Role	Threat Count
Ruiqi Chen	ruiqi@company.com	Finance	Manager Accounts	432
Melissa Cantor	melissa@company.com	Finance	Assistant Manager Accounts	421
Franklin Tavarez	franklin@company.com	Sales	Sales Manager	395
Ryan Roslansky	ryan@company.com	Finance	Senior Manager Accounts	364
Daniel Shapero	daniel@company.com	Sales	Sales Specialist	345
Taylor Borden	taylor@company.com	Sales	Sales Engineering	338
Hari Srinivasan	hari@company.com	Finance	Chief Finance Officer	302
James Parry	james@company.com	Finance	Finance Manager	235
Cesar Cruz	cesar@company.com	Sales	Sales Operations Manager	185
Divya Devendran	divya@company.com	Sales	Marketing Manager	169

Impersonated Custom VIP Users

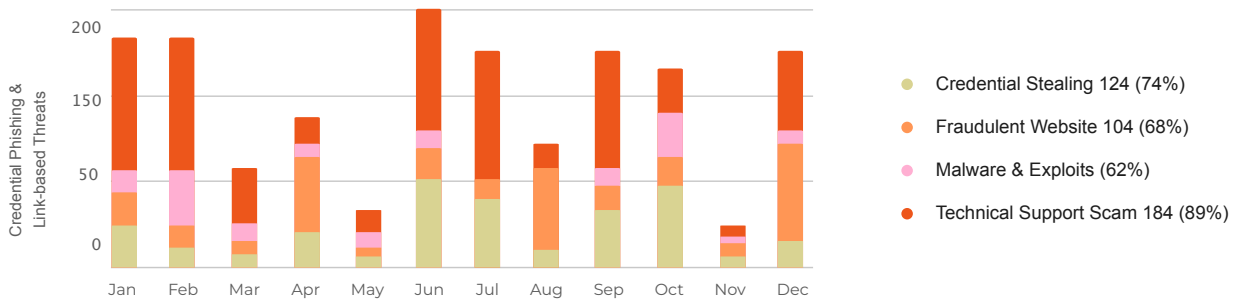
The information in this table are the employees, from your customer VIP list, that are most frequently impersonated. This table will be blank if the feature is not enabled or impersonation attacks did not occur in the reporting period.

Display Name	Email	Department	Role	Threat Count
Ruiqi Chen	ruiqi@company.com	Finance	Manager Accounts	432
Melissa Cantor	melissa@company.com	Finance	Assistant Manager Accounts	421
Franklin Tavarez	franklin@company.com	Sales	Sales Manager	395
Ryan Roslansky	ryan@company.com	Finance	Senior Manager Accounts	364
Daniel Shapero	daniel@company.com	Sales	Sales Specialist	345
Taylor Borden	taylor@company.com	Sales	Sales Engineering	338
Hari Srinivasan	hari@company.com	Finance	Chief Finance Officer	302
James Parry	james@company.com	Finance	Finance Manager	235
Cesar Cruz	cesar@company.com	Sales	Sales Operations Manager	185
Divya Devendran	divya@company.com	Sales	Marketing Manager	169

Credential Phishing and Link-Based Threats

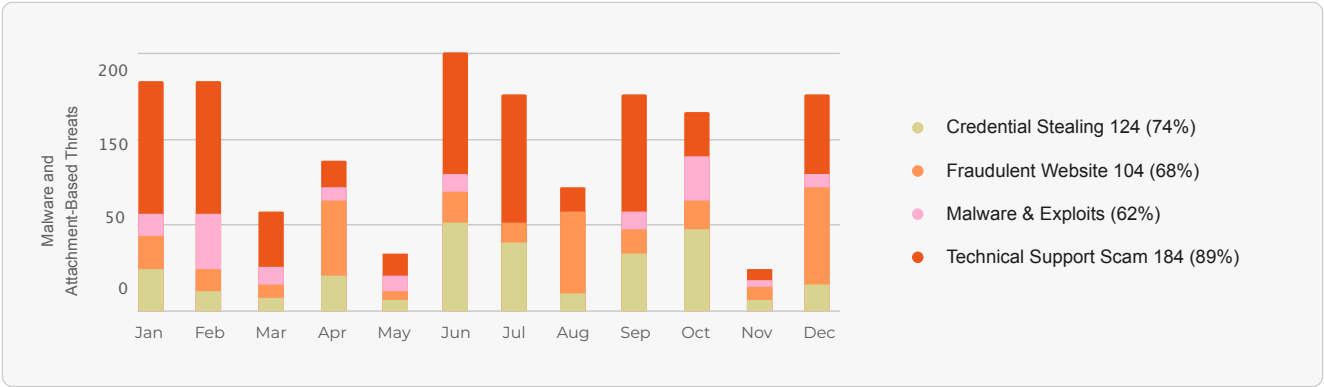
Malicious emails with embedded URLs, especially those associated with credential phishing, are a prominent threat in our cybersecurity landscape. These emails often employ social engineering tactics, leveraging various methods to appear benign and trustworthy.

The email hyperlinks redirect recipients to fraudulent websites crafted meticulously to imitate genuine platforms. This includes duplicating the look and feel of login pages with the ultimate goal of tricking individuals into providing their login credentials or downloading malicious files.



Malware and Attachment-based Threats

Emails with malicious attachments represent a significant cybersecurity risk. These emails often use social engineering tactics to appear legitimate and trustworthy. The email files contain ransomware, malware or other malicious code that can compromise a recipient's system when opened.



Business Impact Summary and ROI

111 /3245

Number of users targeted out of total inboxes protected

2101 /9087

Number of malicious emails out of total number of emails scanned

780

Number of BEC Emails Mitigated

$125,612

Avg Cost of Successful BEC attack

$4,500,000

Avg Cost of a Successful Ransomware attack

SOC OpEX Saved per Investigation **16-30 mins**