

# SLASHNEXT CLOUD EMAIL SECURITY

EXECUTIVE SUMMARY REPORT

Company: Acme

Reporting period: July 1, 2024, to September 30, 2024

Date: October 1, 2024

Generated by: Jonathan Smith

# TABLE OF CONTENTS

<a href="#">Introduction</a>	2
<a href="#">Report Summary</a>	2
<a href="#">Phishing Threats</a>	3
Overview	4
Phishing Threats Timeline	4
Top Phishing Threats	5
Top 10 Phishing Recipients	7
Top 10 Phishing Senders	8
BEC & Social Engineering Threats	9
Impersonation Attacks	10
Impersonation Attacks Breakdown	10
Impersonation Attacks Timeline	10
Top 10 Impersonated Users	11
Impersonated VIP Users	11
Phishing Links & Quishing Threats	12
Phishing Attachments Threats	12
<a href="#">Spam &amp; Bulk Mail</a>	13
Summary	14
Spam Timeline	14
Top 10 Spam Recipients	15
Top 10 Spam Senders	15
<a href="#">Business Impact Summary and ROI</a>	16
BEC and Advanced Phishing	16
Spam & Bulk Mail	17
<a href="#">References</a>	18
<a href="#">Threat Cyclopedia</a>	19

## Introduction

In today's digital landscape characterized by connectivity and remote collaboration, email is the lifeline for communication and the prime vector for malicious actors seeking to exploit user vulnerabilities. This report provides a detailed and insightful analysis of Acme's email security posture. It aims to provide data-driven insights that empower you to make informed decisions, fortify your cybersecurity measures, and safeguard your organization effectively.

## Report Summary

During the reporting period, SlashNext blocked 29,594 phishing threats targeting 1,124 users, demonstrating the service's effectiveness in identifying sophisticated phishing attacks that could lead to financial losses, reputation damage, and legal consequences for your organization.

Furthermore, the SlashNext Spam & Bulk Mail filtration service blocked 46,373 unsolicited emails sent to 1,310 users. By blocking 46,373 unsolicited emails, SlashNext's spam filtration service has increased productivity levels for your IT team and end users by 168 hours.

The report concludes with an in-depth ROI analysis that showcases the security and productivity improvements you can achieve with SlashNext Email Security.

2,278

Mailbox Monitored  
Blocking Mode

29,594

Phishing Threats Detected

46,373

Spam & Bulk Mail Detected

168

Hours of productivity gain  
potential

## Phishing Threats

---



Though spear phishing campaigns account for only 0.1% of all email-based phishing attacks, they are responsible for 66% of all breaches.

*Top Phishing Statistics for 2024, StationX*



 1,265%

increase in phishing emails since the launch of ChatGPT, signaling a new era of cybercrime fueled by generative AI.

[SlashNext State of Phishing Report](#)

# Phishing Threats

## Overview

SlashNext identified 29,594 phishing threats at “Company” during the reporting period, marking a 21% decrease from the previous period. The predominant categories of phishing threats targeting “Company” were Phishing Links & Quishing (QR Code Phishing) and Social Engineering.

Below is a breakdown of phishing threats across four primary categories.

**16,740** Phishing Links & Quishing

Emails with malicious links or QR codes, intended to steal sensitive information or execute social engineering scams.

**1,123** BEC Threats

Financial frauds such as invoice scams, payroll theft, and fraudulent funds transfers, among others, typically using impersonation to mislead victims.

**1,378** Phishing Attachments

Email attachments embedded with malware, QR & phishing links, or carrying messages designed for social engineering.

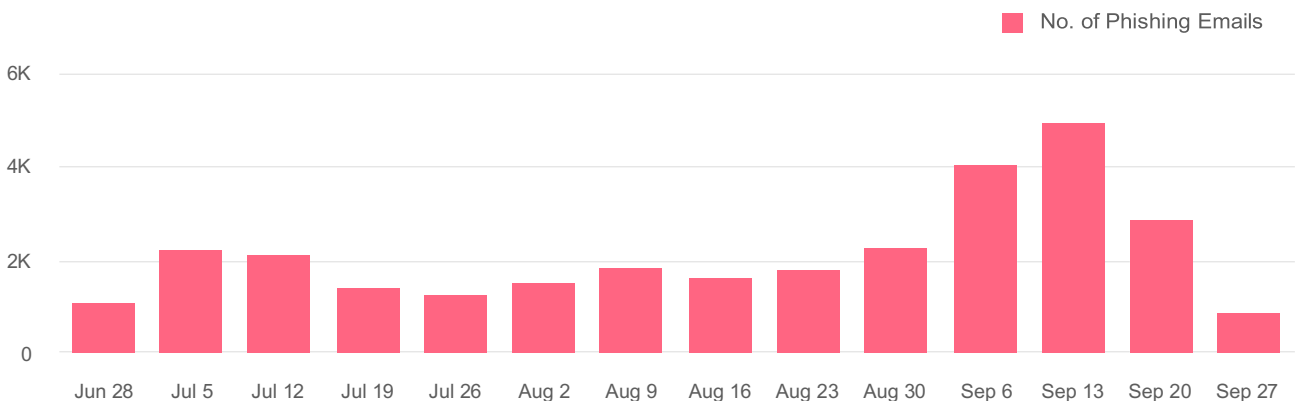
**9,338** Social Engineering

Scams aimed at individuals, including phony job offers, buying scams, and deceptive investment opportunities, among others.



## Phishing Threats Timeline

The bar chart highlights the change in phishing volume over time, showing the number of phishing emails blocked throughout the reporting period.



# Phishing Threats

## Top Phishing Threats

Below are the top phishing threats identified within each threat category, along with the frequency of each attack and its percentage representation.

Phishing Threats Threat Count

### BEC Threats

BEC: RFQ Scam 443 (1.65%)

RFQ scams involve attackers posing as genuine entities and requesting to purchase goods on credit terms without the intention of payment.

---

BEC: Reconnaissance 368 (1.37%)

A BEC reconnaissance email aims to start a conversation with the victim in an urgent tone to build trust and carry out various scams later on.

---

BEC: Assistance Scam 156 (0.58%)

In BEC Assistant Scams, attackers pretend to be executives or colleagues, asking for assistance or a favor to prompt a response.

### Phishing Links & Quishing

Fraudulent Website 13,616 (50.65%)

Email links designed to conduct social engineering scams such as gift, shipment, and Bitcoin scams.

---

Credential Stealing 3,078 (11.45%)

Email links that are designed to steal credentials or request sensitive information.

---

Technical Support Scam 24 (0.09%)

Email links that falsely flag users' computers as infected with viruses, prompting them to call a scammer for remote support.

# Phishing Threats

## Phishing Threats

## Threat Count

### Phishing Attachments

#### Credential Stealing

1,376 (5.12%)

Email links that are designed to steal credentials or request sensitive information.

---

#### Fraudulent Website

1 (-%)

Email links that are designed to conduct social engineering scams such as gift, shipment, and Bitcoin scams.

---

#### QR Phishing

1 (-%)

Emails containing QR codes that redirect to websites stealing credentials or personal information.

### Social Engineering

#### Social Engineering: Scam

4,712 (17.53%)

Scam emails to perform online frauds, ranging from fake jobs, lottery winnings, phony investment opportunities, etc.

---

#### Social Engineering: Investment Scam

2,095 (7.79%)

Investment scams involve fraudsters posing as legitimate investors offering lucrative investment opportunities for a nominal fee.

---

#### Spam: Generic

1,011 (3.76%)

BEC Generic attacks usually aim to execute commercial scams, such as fictitious partnerships and investment opportunities.

# Phishing Threats

## Top 10 Phishing Recipients

This table contains the top 10 recipients of phishing emails within your organization. By pinpointing which individuals are most frequently targeted, you can tailor your training and awareness programs to these high-risk users, fortifying their ability to recognize and respond to phishing attempts. This targeted approach not only helps in reducing the susceptibility of these key areas but also bolsters the overall resilience of your organization against cyber threats.

Display Name	Email	Department	Title	Threat Count
Regina Smith	rsmith@acme.com	Construction Servi...	-	629
Andy Panda	apanda@acme.com	Construction Servi...	-	498
Jeffrey Doe	adoe@acme.com	Civil/Highway	-	451
Jessica Rarebit	jrarebit@acme.com	Azure AD - Proofpo...	Corporate Director of M...	422
Lewis Barry	lbarry@acme.com	Azure AD - Proofpo...	Branch Manager	380
Dan Manning	dmanning@acme.com	Environmental	-	370
Rob Baron	rbaron@acme.com	Underwater	-	353
Pat Hattie	phattie@acme.com	Azure AD - Proofpo...	Chief Executive Officer	299
Russ Kittle	rkittle@acme.com	Mechanical	-	272
Herb Hancock	hhancock@acme.com	Marketing	-	272



# Phishing Threats

## Top 10 Phishing Senders

This table contains the top 10 malicious email senders against your organization. By identifying and understanding the common sources of these threats, your IT security team can develop more targeted defense strategies, such as reining your email filtering protocols and raising awareness among employees about specific phishing tactics. This proactive approach not only mitigates the risk of successful phishing attacks but also strengthens your overall security posture against evolving cyber threats.

Display Name	Email	Domain	Threat Count
Cooking Curiosity	update@cookingcuriosity.com	cookingcuriosity.com	713
Miller Steve	miller.biddingestimating@gmail.c...	gmail.com	622
YETI Tundra 45 Hard	alerts@hotmail.ca	hotmail.ca	174
AnyTrivia	trivia@anytriviamail.com	anytriviamail.com	167
Igloo Trailmate Cooler Confirma...	team@hotmail.ca	hotmail.ca	166
AAA Car Rewards!	thebrick@hotmail.ca	hotmail.ca	159
AA Rewards Team	thebrick@hotmail.ca	hotmail.ca	159
Milwaukee Winner Centre	thebrick@hotmail.ca	hotmail.ca	158
Tommy Bahama Beach Chairs	noreply@hotmail.fr	hotmail.fr	158
AAA Car Emergency Kit	noreply@hotmail.fr	hotmail.fr	158

# Phishing Threats

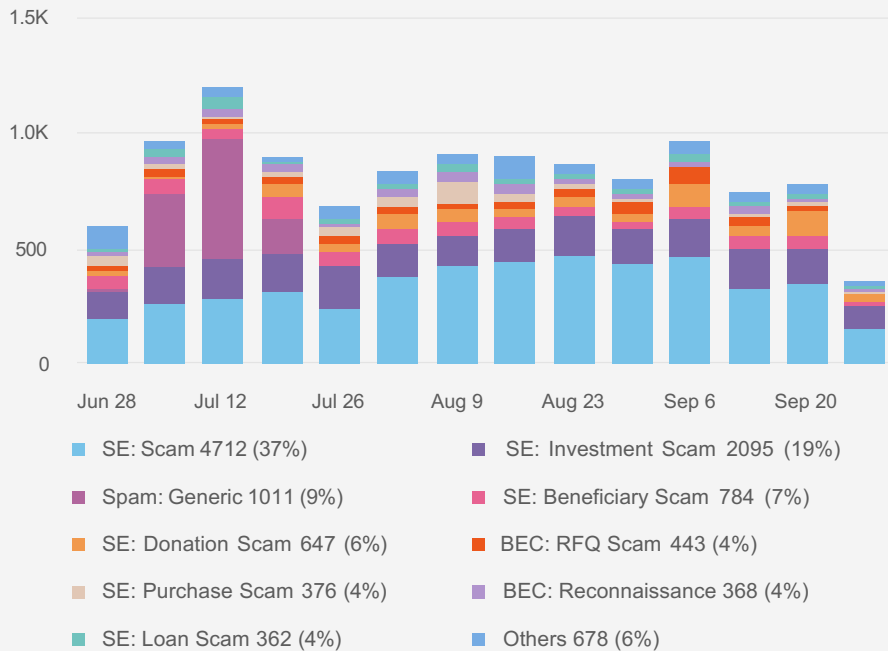
## BEC & Social Engineering Threats

BEC and social engineering attack emails typically don't contain malicious links or attachments. Instead, they employ sophisticated tactics, such as deceptive language, convincing narratives, and impersonating genuine users, to manipulate and deceive their targets.

Below is a breakdown of BEC and social engineering attacks identified during the reporting period.

**1,123** Total  
BEC  
Threats

**9,338** Total  
Social Engineering  
Threats



## BEC & SOCIAL ENGINEERING THREATS

Average cost of a successful  
Business Email Compromise  
(BEC) attack is

**\$137,132**

2023 FBI IC3 Report

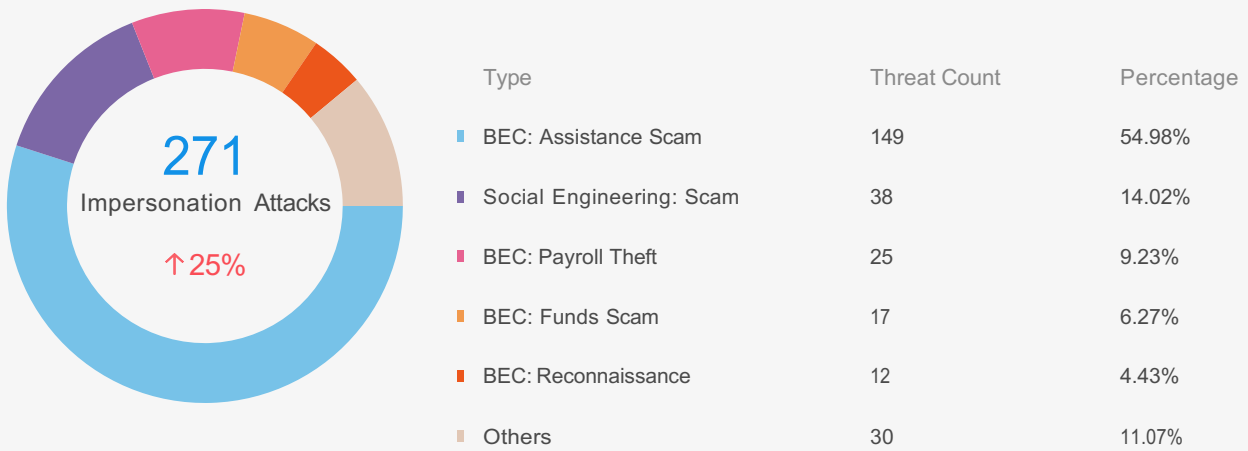
# Phishing Threats

## Impersonation Attacks

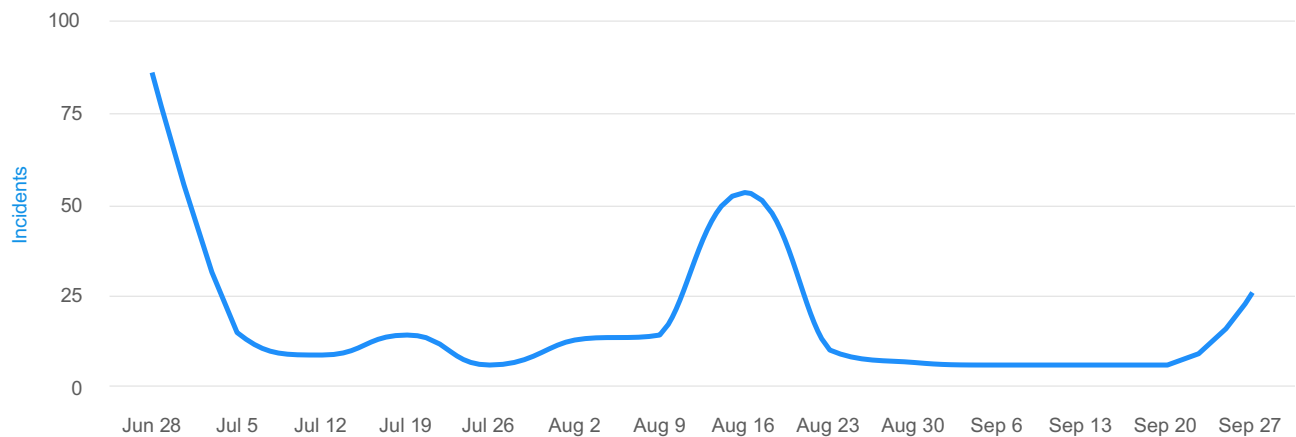
Impersonation attacks occur when attackers disguise themselves as someone you trust, like a coworker, a company leader, or a service provider. Below is a breakdown of impersonation attacks blocked and their timeline.

## Impersonation Attacks Breakdown

The system has blocked 6 types of threats leveraging impersonation techniques, with BEC: Assistance Scam and Social Engineering: Scam attacks being the most prominent categories.













## Impersonation Attacks Timeline



# Phishing Threats

## Top 10 Impersonated Users

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

Display Name	Email	Department	Title	Threat Count
Patrick Neil	pneil@acme.com	Azure AD - Proofpoint	Chief Executive Officer	 184
David Ghoul	dghoul@acme.com	-	-	 10
Andrew Candy	acandy@acme.com	Construction Services	-	 9
David Jermaine	djermaine@acme.com	Corrosion Protection	-	 8
Steve Bluebird	sbluebird@acme.com	Azure AD - Proofpoint	Chairman of The Board	 6
Fiona Apple II	fapple@acme.com	Group Undefined	-	 5
Paul Barry	pbarry@acme.com	Azure AD - Proofpoint	Geospatial Division	 4
Nathan Olivera	nolivera@acme.com	-	-	 4
Mary Lamb	mlamb@acme.com	Survey	-	 3
Doug Myer	dmyer@acme.com	-	-	 2

## Impersonated 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	Title	Threat Count
Patrick Kittle	pkittle@acme.com	Azure AD - Proofpoint	Chief Executive Officer	184
Steve Bluebird	sbluebird@acme.com	Azure AD - Proofpoint	Chairman of The Board	6
Paul Barry	pbarry@acme.com	Azure AD - Proofpoint	Geospatial Division	4
Ken State	kstate@acme.com	Azure AD - Proofpoint	Chief Executive Officer	2
Louis Alcinder	lalcinder@acme.com	Azure AD - Proofpoint	Branch Manager	1
Tim Leary	tleary@acme.com	Azure AD - Proofpoint	Branch Manager	1

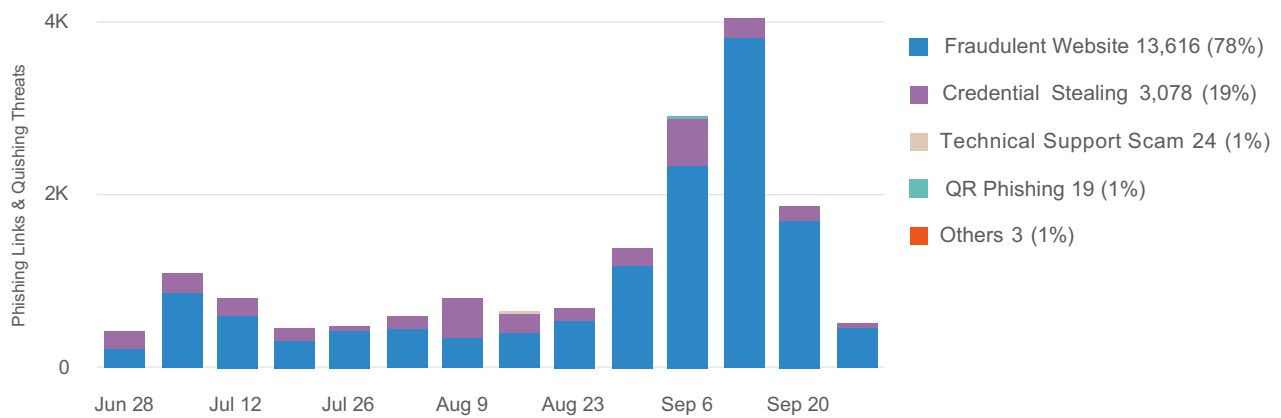
# Phishing Threats

## Phishing Links & Quishing Threats

Malicious emails with embedded URLs and QR codes, 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.

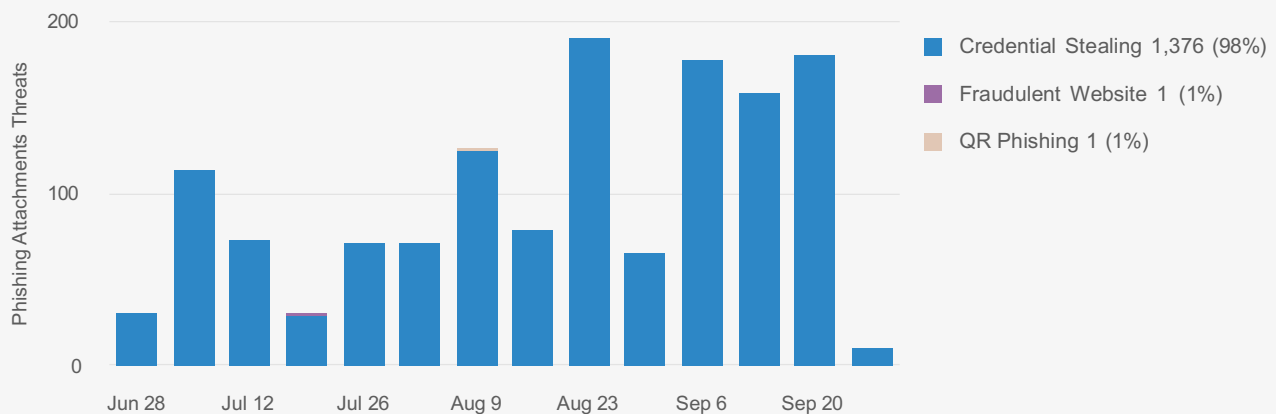
Below is a timeline of Phishing Links and Quishing attacks blocked during the reporting period.



## Phishing Attachments 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

Below is a timeline of threats containing Phishing attachments blocked during the reporting period.



## Spam & BulkMail

---



# 49%

162 billion spam emails are sent every day, with 49% of the 333 billion daily emails sent.

*Spam Statistics (2024) by Emailtooltester*



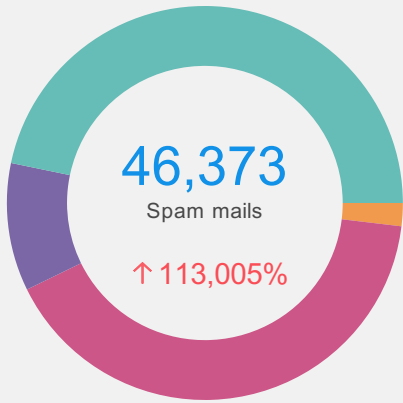
# 20 Billion

New York consulting firm Basex blamed unsolicited e-mail for nearly \$20 billion in lost time and expenses worldwide. Spam within the enterprise can cost between \$600 and \$1,000 per year for every user.

# Spam & BulkMail

## Overview

The SlashNext Spam & BulkMail filtration service blocked 46,373 unsolicited emails. This represents a 113,005% increase from the previous period. The most common categories of spam emails identified were Hybrid Spam and Sales Outreach.



### 877 Marketing Ads

Spam emails frequently promoting questionable products like electronics, diet pills and counterfeit items. They commonly feature vibrant banners and lack user personalization.

### 18,954 Sales Outreach

Sales outreach by companies or individuals to potential customers, presenting products and services with a professional tone and personalized content tailored to the recipients.

### 4,866 News & Announcements

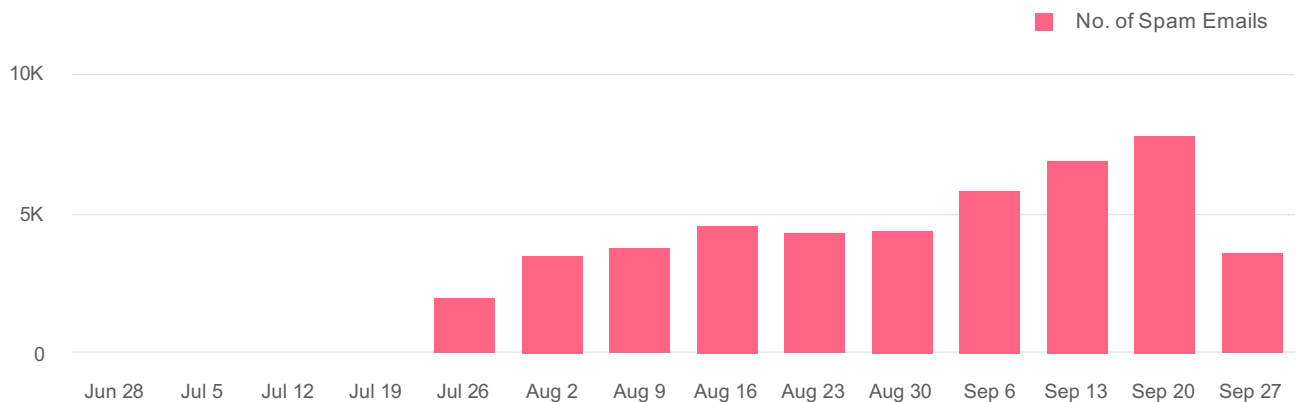
Spam emails containing invitations, polls, campaign donation requests, and other similar content, typically unrelated to the recipient's interests.

### 21,676 Hybrid Spam

Commercial spam emails blending traits from other specific types of spam, showcasing varied intents and formatting styles.

## Spam Timeline

The bar chart highlights the change in spam volume over time, showing the number of spam emails blocked throughout the reporting period.



# Spam & BulkMail

## Top 10 Spam Recipients

This table shows the top recipients who have experienced the highest number of spam emails.

Display Name	Email	Department	Role	Threat Count
Victoria Clueless	vclueless@acme.com	Human Resources	-	833
Steve Bluebird	sbluebird@acme.com	Azure AD - Proofpo...	Chairman of The Boa...	788
Chris Corning	ccorning@acme.com	Civil/Highway	-	683
Luis Alcinder	lalcinder@acme.com	Administration	-	606
Frank Stella	fstella@acme.com	Land Development	-	598
Pat Manning	pmanning@acme.com	Administration	-	568
Jeff Fisher	jfisher@acme.com	Civil/Highway	-	564
John Shore	jshore@acme.com	Administration	-	553
Stephan Knownly	sknownly@acme.com	Human Resources	-	545
Bernie Rohe	brohe@acme.com	Traffic	-	536

## Top 10 Spam Senders

This table shows the top senders responsible for sending the highest volume of spam emails.

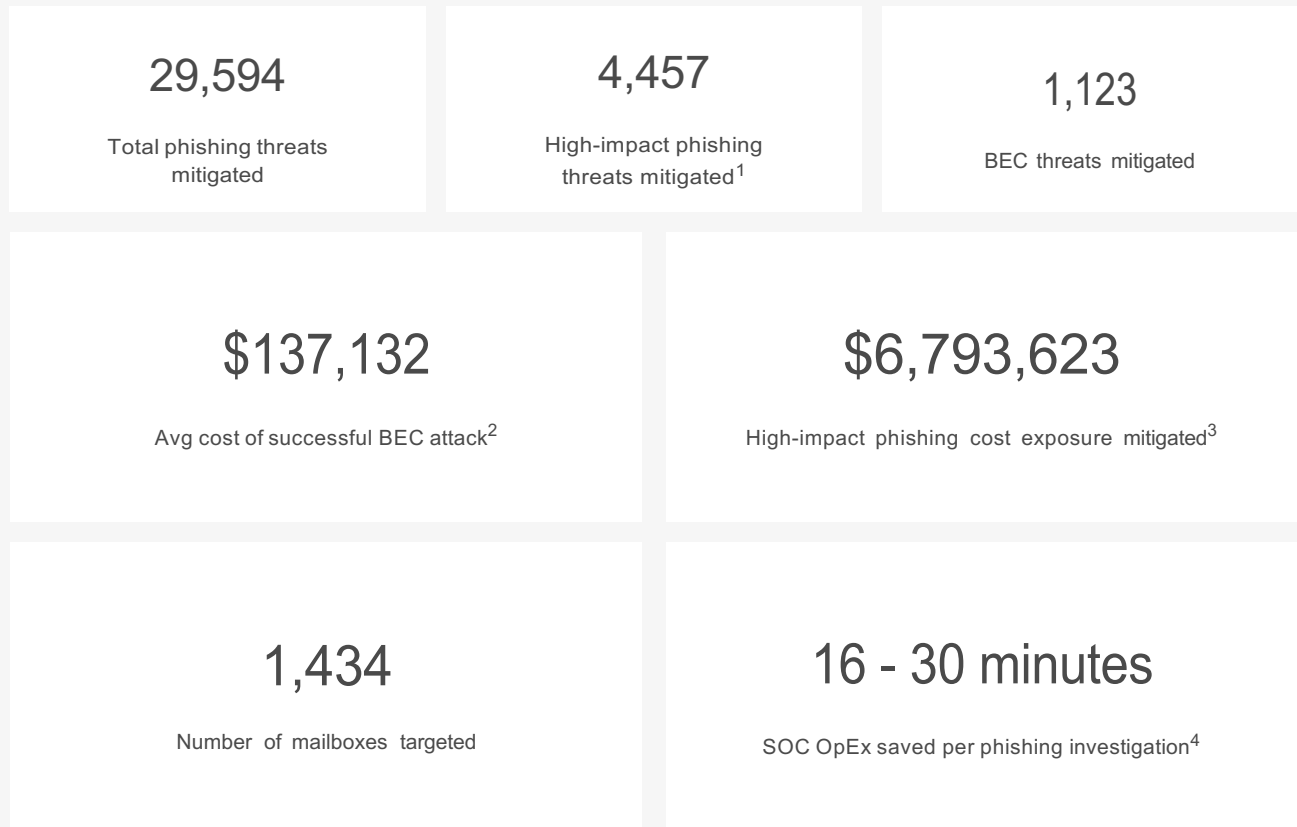
Display Name	Email	Domain	Threat Count
Cooking Curiosity	update@cookingcuriosity.com	cookingcuriosity.com	● 3,534
Recipe Zap	recipes@recipezap.com	recipezap.com	◆ 3,261
Cooking Corner Daily	today@cookingcornerdaily.com	cookingcornerdaily.com	1,034
USA Health	today@healthy-americans.com	healthy-americans.com	876
Stephen Miller	info@activistdonor.org	activistdonor.org	713
Hog Technologies	sales@thehog.com	thehog.com	498
AnyTrivia	trivia@anytriviainmail.com	anytriviainmail.com	449
Wild & Organic	hello@wildandorganic.com	wildandorganic.com	430
Indeed	no-reply@5mobilemailing.com	5mobilemailing.com	423
Voter Verification HQ	contact@email.nrsc.org	email.nrsc.org	374



# Business Impact Summary and ROI

## BEC and Advanced Phishing

This metric highlights BEC and advanced phishing as high risk threats among all identified attacks and quantities the typical financial damage linked with these attacks.



# Business Impact Summary and ROI

## Spam & BulkMail

### IT Productivity

**39 hrs**

saved in Abuse Inbox investigation

By blocking 46,373 spam emails, SlashNext has decreased the time your IT department spends on investigating user spam submissions by 39 hours.

### User Productivity

**129 hrs**

saved in User Productivity

Over the selected period, SlashNext blocked 46,373 spam emails, resulting in an estimated total savings of 129 hours in user productivity.

# References

- [1] High impact phishing threats is the sum of business email compromise, credential phishing, malware and exploits.
- [2] Average cost of a successful BEC attack – 2023 FBI IC3.
- [3] High-impact phishing cost exposure mitigated is calculated using the formula  $SUM = (\text{Number of BEC threats} * 1.45\% \text{ likelihood} * \$137,132) + (\text{Number of credential phishing, malware and exploits} * 1.42\% \text{ likelihood} * \$72,060)$ . 2021 Ponemon Institute “The Cost of Phishing Study”
- [4] SOC OpEx saved per phishing investigation – 2020 Osterman Research “Security Awareness Training as a Key Element in Changing the Security Culture Study”.

## Business Impact Summary and ROI External References

2023 FBI Internet Crime Complaint Center (IC3) Report

2020 Osterman Research Security Awareness Training as a Key Element in Changing the Security Culture Study

## BEC Threats

### Assistance Scam

In BEC Assistant Scams, attackers pretend to be executives or colleagues, asking for assistance or a favor to prompt a response.

### Funds Scam

Funds scams involve attackers posing as trusted entities to deceive recipients into transferring money to fraudulent accounts.

### Gift Card Scam

In BEC Gift Card scams, scammers pretend to be executives or colleagues, persuading the victim to buy them gift cards for false reasons.

### Payroll Theft

Fraud incidents where attackers impersonate employees, aiming to mislead HR into rerouting paychecks to fraudulent accounts.

### W-form

BEC W-form scams involve attackers posing as colleagues or legal representatives to obtain employees' tax-related documents.

### Attorney Scam

In BEC Attorney Scams, attackers impersonate executives and urge the target to engage with a phony law firm to execute forged contracts.

### Generic

BEC Generic attacks usually aim to execute commercial scams, such as fictitious partnerships and investment opportunities.

### Invoice Fraud

Invoice fraud involves attackers posing as executives or suppliers to deceive recipients into paying bogus invoices.

### Reconnaissance

A BEC reconnaissance email aims to start a conversation with the victim in an urgent tone to build trust and carry out various scams later on.

## Social Engineering

### 419 Scam

A 419 scam, also known as an advance-fee fraud or Nigerian scam, involves soliciting a target through an email or letter.

### Donation Scam

Donation scams involve fraudsters convincing recipients that they qualify for a donation or charity based on fabricated reasons.

### Beneficiary Scam

Beneficiary scams involve fraudsters convincing recipients they're entitled to an inheritance from a wealthy individual or entity, citing fabricated reasons.

### Investment Scam

Investment scams involve fraudsters posing as legitimate investors offering lucrative investment opportunities for a nominal fee.

## Job Scam

Job scams involve fraudsters posing as legitimate employers and tricking job seekers in various ways for personal information or payments.

## Lottery Scam

Lottery scams deceive victims by convincing them they've won a lottery and then requesting personal information to claim the funds.

## Romance Scam

Romance scams exploit emotional manipulation to target individuals seeking companionship for monetary gain.

## RFQ Scam

RFQ scams involve attackers posing as genuine entities and requesting to purchase goods on credit terms without the intention of payment.

## Threat Scam

In Threat scam, sender attempts to intimidate the recipient into sending money or providing sensitive information by threatening them with negative consequences.

## Phishing Links & Quishing

### Credential Stealing

Email links that are designed to steal credentials or request sensitive information.

### QR Phishing

Emails containing QR codes that redirect to websites stealing credentials or personal information.

### Rogue Software

Email links downloading malware or software exploits aimed at compromising the user's device.

## Loan Scam

Loan scams involve fraudsters posing as legitimate lenders offering loans with generous terms in exchange for a nominal fee.

## Purchase Scam

Purchase scams involve fraudsters emailing fake purchase confirmations and asking to call their numbers to cancel the transaction.

## Scam

Scam emails to perform online frauds, ranging from fake jobs, lottery winnings, phony investment opportunities, etc.

## Sextortion

Sextortion is a form of cyber extortion scam where the sender threatens to release explicit or compromising images or videos of the recipient unless they pay a ransom.

### Fraudulent Website

Email links that are designed to conduct social engineering scams such as gift, shipment, and Bitcoin scams.

### Technical Support Scam

Email links that falsely flag users' computers as infected with viruses, prompting them to call a scammer for remote support.

## Phishing Attachments

### Rogue Software

Binary or document attachments embedding malware or software exploits aimed at compromising the user's device.

### Credential Stealing

HTML or PDF phishing attachments that are designed to steal credentials or request sensitive information.

### Technical Support Scam

HTML attachments that falsely flag users' computers as infected with viruses, prompting them to call a scammer for remote support.

### Fraudulent Website

HTML or PDF attachments that are designed to conduct social engineering scams such as gift, shipment, and Bitcoin scams.

### QR Phishing

HTML or PDF attachments containing QR codes that redirect to websites stealing credentials or personal information.

## Spam & BulkMail

### Hybrid Spam

Commercial spam emails blending traits from other specific types of spam, showcasing varied intents and formatting styles.

### Marketing Ads

Spam emails frequently promoting questionable products like electronics, diet pills and counterfeit items. They commonly feature vibrant banners and lack user personalization.

### Sales Outreach

Sales outreach by companies or individuals to potential customers, presenting products and services with a professional tone and personalized content tailored to the recipients.

### News & Announcements

Spam emails containing invitations, polls, campaign donation requests, and other similar content, typically unrelated to the recipient's interests.