

mimecast™

[Your Company]’s Monthly Human Risk Insights Report

Sep 2025



Table of Contents

- 1 Executive Summary
- 2 Prevented Threats
- 3 Detections Benchmarking
- 4 Human Risk
- 5 Risks Insights

Did you know?

Mimecast has been ranked the #1 email security solution for two consecutive years by At-Bay Cyber Insurance.

According to their analysis of real cyber claims data, Mimecast customers experience 37% fewer email-related incidents compared to the industry average. [Read the complete At-Bay Cyber Insurance Report.](#)



1 Executive Summary

3.4 million inbound threats were blocked in September 2025. This is an increase of 5% compared to the previous month.

! Recommendations and Insights

- Your human risk score has increased by 1 since last month because your training behavior risk score has weakened.
- Based on the credential harvesting attacks you were targeted with; Microsoft was the most impersonated brand. This was identified by the fake login pages that were detected and blocked. Consider educating your end users on the increased risk of malicious messages impersonating this brand.
- A number of attempts to exploit vulnerabilities were detected through analysis of malicious files, including CVE-2017-0199, CVE-2022-42889 and CVE-2012-1858. Consider patching these vulnerabilities if relevant to your environment.

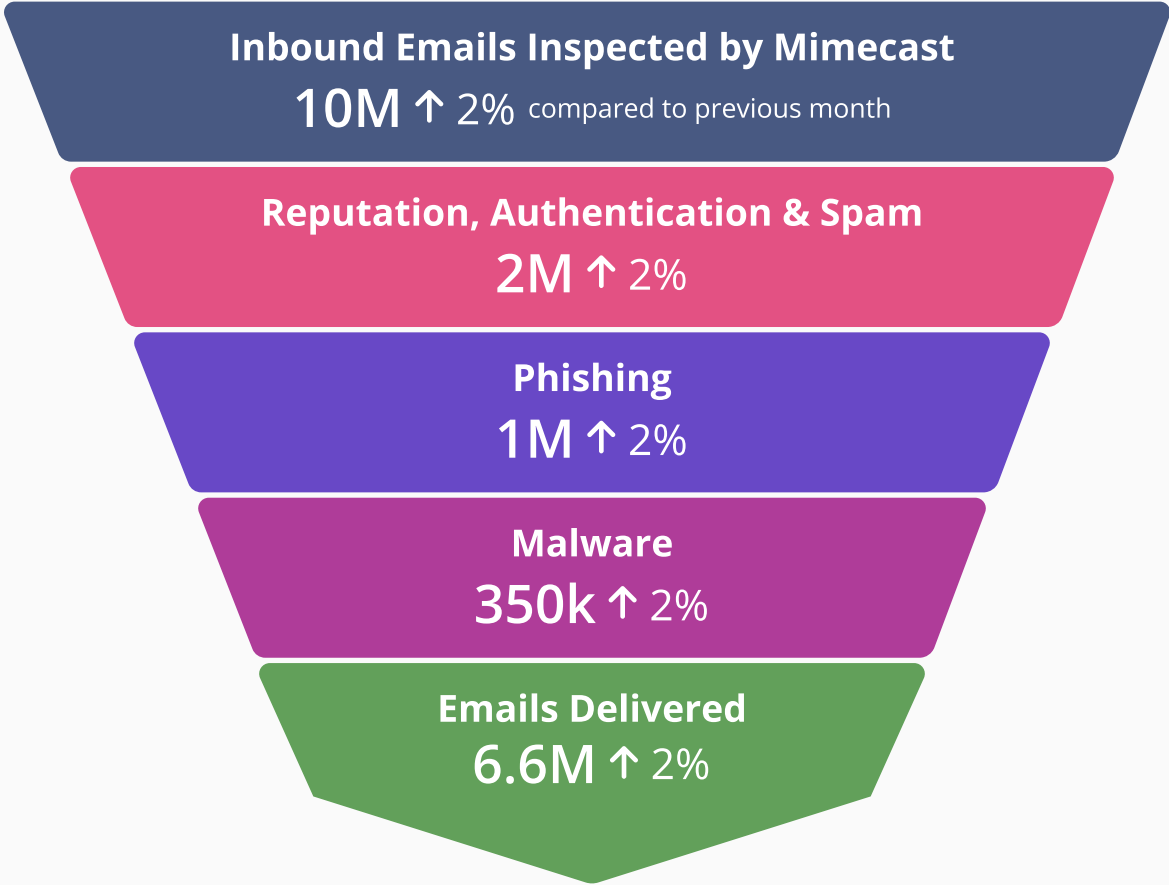
Your organization's human risk score is based on your end users' behaviors.



2.1

Detection Overview

Inbound threats detected



Detection Highlights

Detection	Impact
<div> Phishing 12 ↑ 11%*</div> <div>Email remains the number one attack vector for cybercriminals, and phishing attacks remain the top threat to email users.</div>	
<div> Business Email Compromise 17 ↑ 2%*</div> <div>The average cost of a successful BEC attack is \$137,132. (1)</div>	
<div> Credential Harvesting 21 ↓ 11%*</div> <div>Use of stolen credentials is the top initial access technique observed across all incidents. (2)</div>	
<div> Ransomware 25 ↓ 6%*</div> <div>The typical ransomware event costs \$1.4 Million. (3)</div>	
<div> Malicious QR code 33 ↓ 11%*</div> <div>Mimecast analysts have found that over 90% of malicious QR codes are phishing attacks that lead to credential harvesting sites.</div>	

(1) 2023 FBI Internet Crime Report www.ic3.gov.

(2) Cyentia IRIS 2022. (3) Cyentia Institue Information Risk Insights Study: Ransomware.

2.2

Detection Overview

Comprehensive insights into threat activity and resolution status

Malware

30 Detections

5 Delivered

10 Resolved

Phishing

30 Detections

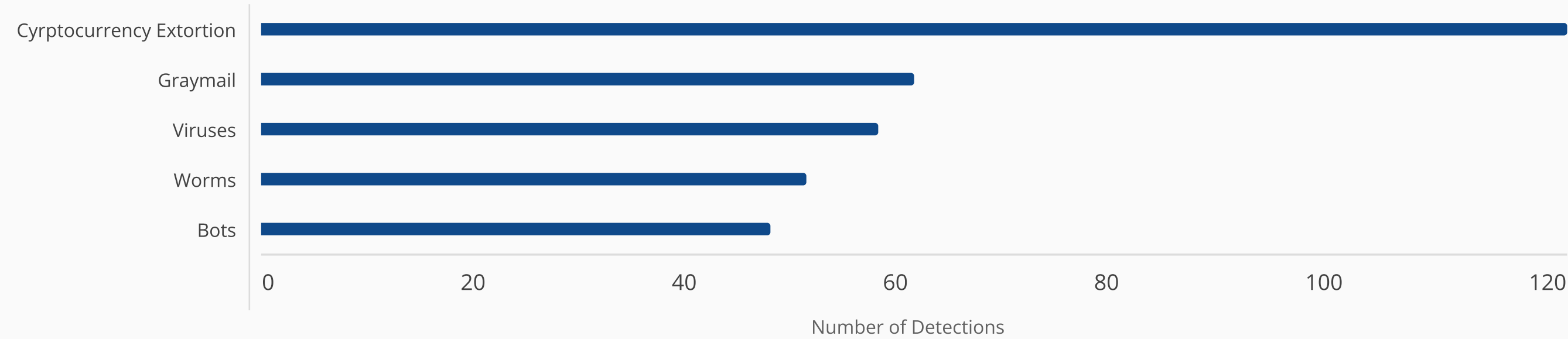
5 Delivered

10 Resolved

Spam

No Detections

Threat Details



3.1

Detections Benchmarking - UK

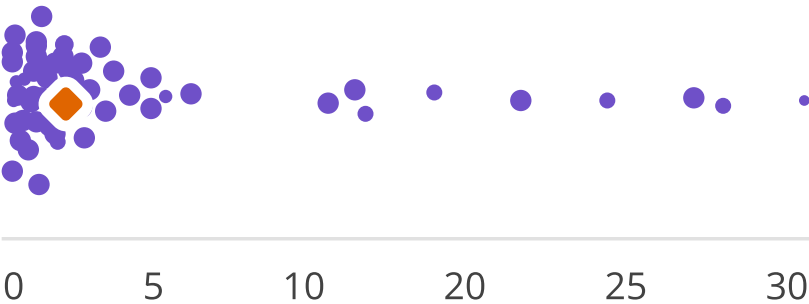
Compare your organization to other Mimecast customers in your region



UK Region: Detections per user by threat type, for Mimecast customers in the UK Region during the past month. Each dot represents 2% of customers. The line shows the number detections per user, for your organization.

◆ Your Organization ◆ Mimecast Customers

Phishing detections per user



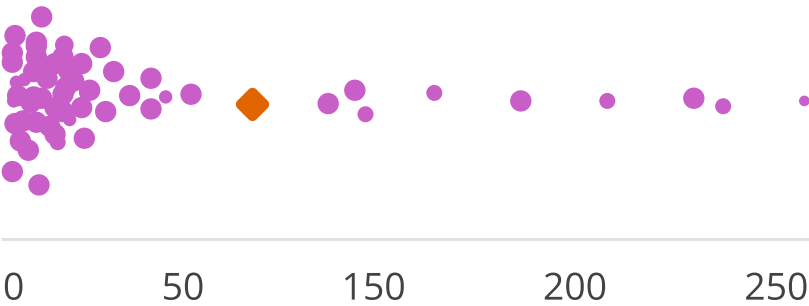
Your organization
◆ 0.05 Detections per user
This is **higher than ~58%** of Mimecast customers in the UK region.

Malware detections per user



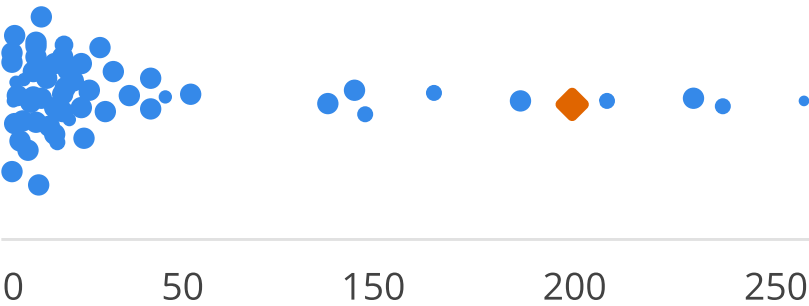
Your organization
◆ 1.1 Detections per user
This is **lower than ~60%** of Mimecast customers in the UK region.

Credential Harvesting detections per user



Your organization
◆ 100 Detections per user
This is **higher than ~79%** of Mimecast customers in the UK region.

Business Email Compromise detections per user



Your organization
◆ 124 Detections per user
This is **higher than ~65%** of Mimecast customers in the UK region.

3.2

Detections Benchmarking - Finance Industry

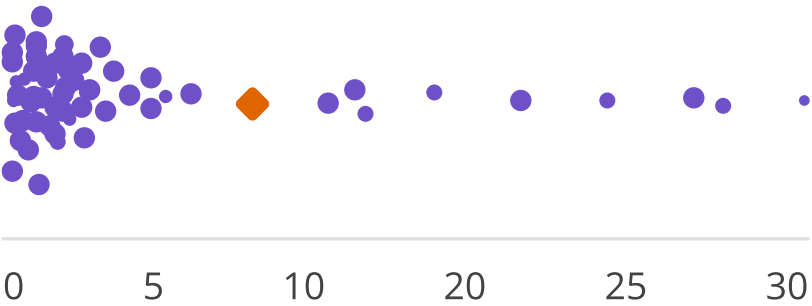
Compare your organization to other Mimecast customers in your industry



Finance Industry: Detections per user by threat type, for Mimecast customers in the Finance Industry during the past month.

◆ Your Organization ◆ Mimecast Customers

Phishing detections per user



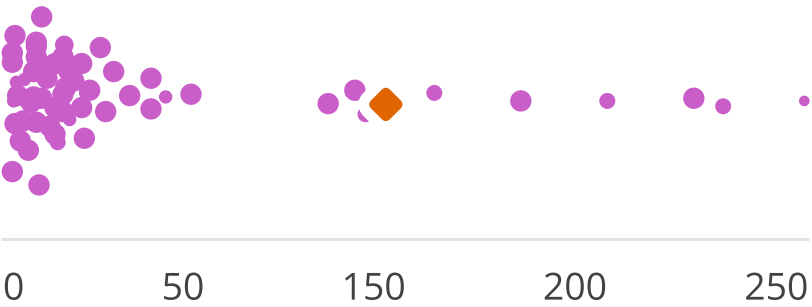
Your organization
◆ 0.05 Detections per user
This is **higher than ~58%** of Mimecast customers in the Finance industry.

Malware detections per user



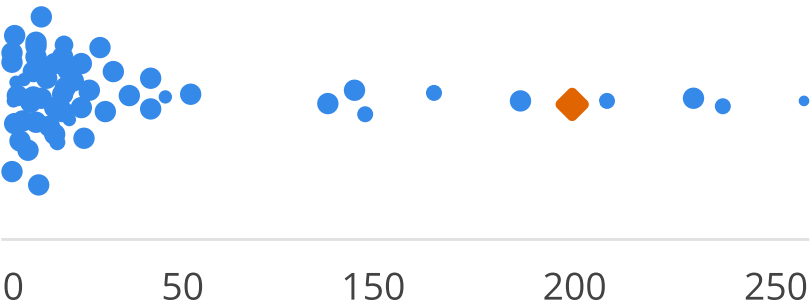
Your organization
◆ 1.1 Detections per user
This is **lower than ~60%** of Mimecast customers in the Finance industry.

Credential Harvesting detections per user



Your organization
◆ 100 Detections per user
This is **higher than ~79%** of Mimecast customers in the Finance industry.

Business Email Compromise detections per user



Your organization
◆ 124 Detections per user
This is **higher than ~65%** of Mimecast customers in the Finance industry.

4.1

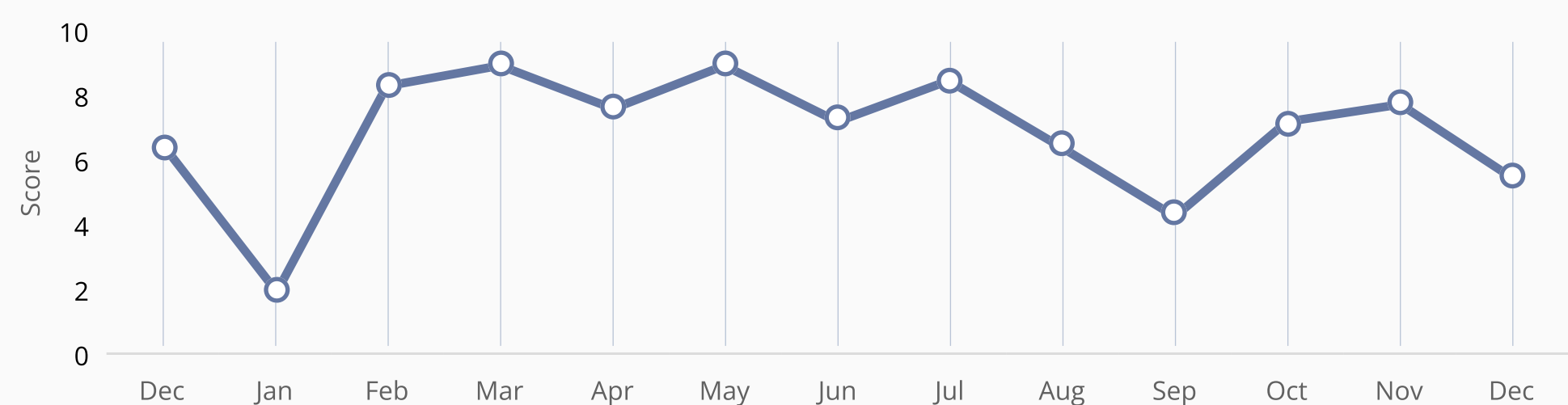
Human Risk

Your organization's overall level of human risk

Hunan Risk Score
Based on user behavior and actions



Human Risk Score Trends Over Time
Last 12 months



The Human Risk Score is based on the actions users take, both positive and negative (their behavior) which increase or decrease risk. The lower the score is, the lower the calculated risk. A low Risk Score is good and indicates less negative Human Risk Behaviors.

4.2

Human Risk Behaviors

How frequently your users engage in risky behaviors

0.1	Phishing	↓	Lower by 0.1 vs. past month	TBD
0.1	Real World Phishing	↓	Lower by 0.1 vs. past month	Actual Phishing refers to actions in response to phishing attempts generated by attackers outside the organization as opposed to internal simulated phishing campaigns.
0.1	Simulated Phishing	=	Unchanged vs. past month	Simulated Phishing refers to actions in response to phishing campaigns that are generated internally as opposed to by external threat actors.
9.1	Training	↑	Higher by 0.1 vs. past month	Training identifies further areas for security improvement for individuals at your organization. Training is done to measure success in understanding of good security practices and to meet compliance requirements.
0.1	Malware	↑	Higher by 0.1 vs. past month	TBD
4.0	Sensitive Data Handling	=	Unchanged vs. past month	TBC

↓ Decreasing Risk ↑ Increasing Risk = Unchanged

The Human Risk Score considers behaviors in the following areas: Actual Phishing, Simulated Phishing and Training. Examples of risky actions that weaken Human Risk Behavior scores include: not reporting a simulated phishing email, clicking on a link in a phishing email, and delays completing training.

Riskiest Users

4.3 These are the riskiest users in your organization according to user behaviors and actions in the following areas: Actual Phishing, Simulated Phishing, and Training. The symbols next to each score indicate the trend compared to the previous month.

User	Risk Score	Phishing	Real World Phishing	Training	Malware	Sensitive Data Handling
Frank Gallagher	9.1 ↑	1.2 ∅	4.0 ↓	9.1 ↑	1.2 ∅	4.0 ↓
Anne Rogers	0.1 ↑	1.2 ∅	4.0 ↓	9.1 ↑	1.2 ∅	4.0 ↓
Louise Contreras	1.1 ↑	1.2 ∅	4.0 ↓	9.1 ↑	1.2 ∅	4.0 ↓
Juan Lopez	4.2 ↑	1.2 ∅	4.0 ↓	9.1 ↑	1.2 ∅	4.0 ↓
Ugun Arioum	6.1 ↑	1.2 ∅	4.0 ↓	9.1 ↑	1.2 ∅	4.0 ↓
Lorena Gallagher	9.1 ↑	1.2 ∅	4.0 ↓	9.1 ↑	1.2 ∅	4.0 ↓
Peter Barents	9.1 ↑	1.2 ∅	4.0 ↓	9.1 ↑	1.2 ∅	4.0 ↓
Frank Lloyd-Right	9.1 ↑	1.2 ∅	4.0 ↓	9.1 ↑	1.2 ∅	4.0 ↓
Roger Watters	9.1 ↑	1.2 =	4.0 ↓	9.1 ↑	1.2 =	4.0 ↓
Olivia Newton	9.1 ↑	No Data ∅	4.0 ↓	9.1 ↑	No Data ∅	4.0 ↓

↓ Decreasing Risk ↑ Increasing Risk = Unchanged ∅ Not Present

5.1

Risk Insights - Threat Senders and Targets

Identifying key threat actors and vulnerable targets



Top malicious senders

Frequent sources of malicious emails

bob@email.com	61
charlie@email.com	59
david@email.com	15
elice@email.com	10
eve@email.com	9



This section highlights the email addresses identified as the most frequent sources of malicious activity. Monitoring these senders can help mitigate risks by blocking or flagging their communications before they reach users.



Top targeted users

Users most targeted by attackers

betty@emial.com	45
chet@emial.com	30
dirk@emial.com	45
elline@emial.com	30
frank@email.com	45




This section identifies the users within your organization who are most frequently targeted by malicious actors. Providing additional security training and monitoring for these users can help reduce the likelihood of successful attacks.

5.2

Risk Insights - URL Detections


Uncover risky URLs and their top targets




Top domains hosting malicious URLs

Key malicious sources

badlink.com	45
sobadlink.com	30
verylargeandlogbadlink.com	45
pirate.com	30
badrobot.com	45


 These domains were flagged for hosting malicious URLs. Consider adding them to your blocklist to prevent unauthorized access.



Top targets of malicious URLs

Users at risk

bob@email.com	20
charlie@email.com	20
david@email.com	20
elice@email.com	15
eve@email.com	15

 These users received the highest number of emails containing malicious URLs. Provide additional training and monitoring for improved security.

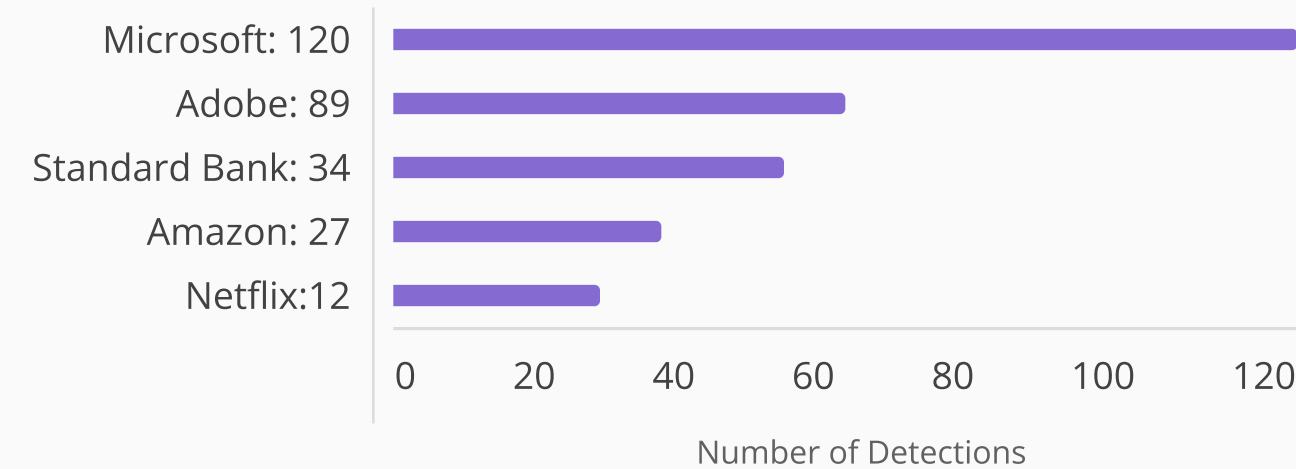
5.3

Risk Insights - Credential Harvesting Detections

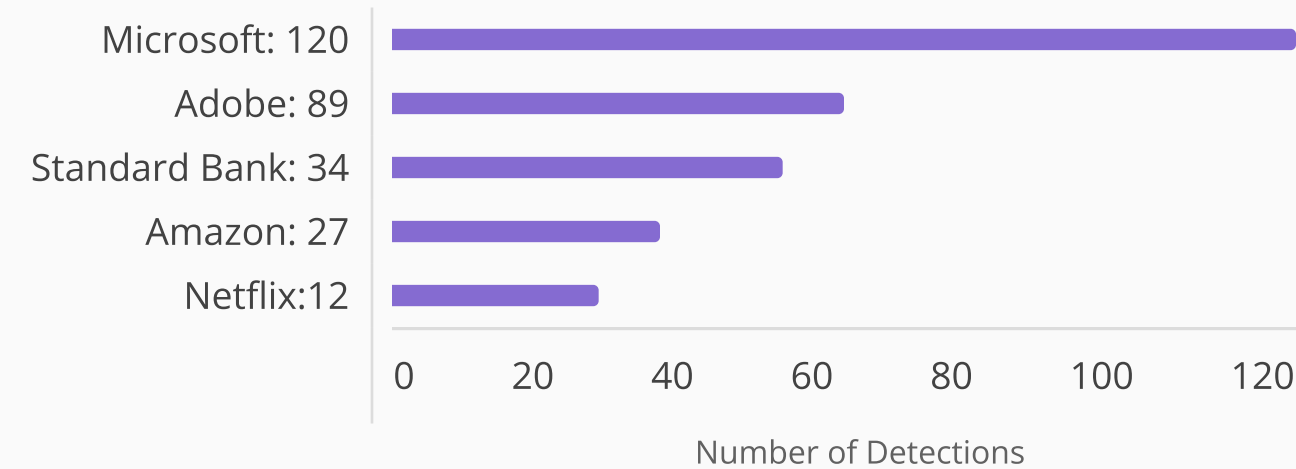
Most impersonated brands used in fake login pages that were detected and blocked by Mimecast Credential Theft Protection

The following brands were detected in credential harvesting attacks against your organization (left) and for Mimecast customers in your industry (right). These attacks use a fake login page that spoofs the brand to harvest credentials that would provide threat actors access to associated services.

Top Impersonated Brands – Your Organization



Top Impersonated Brands – Finance



Consider educating your end users on the increased risk of malicious messages impersonating these brands, particularly if your organization uses related services.

5.4

Risk Insights - CVE Detection Insights

Understand specific vulnerabilities that attackers are attempting to exploit



Your Organization

CVE Detections

CVE-2746-939568	500
CVE-2746-939568	467
CVE-2746-939568	433
CVE-2746-939568	367
CVE-2746-939568	343
CVE-2746-939568	221
CVE-2746-939568	211
CVE-2746-939568	187
CVE-2746-939568	123
CVE-2746-939568	99



Finance Sector

CVE Detections

CVE-2746-939568	500
CVE-2746-939568	467
CVE-2746-939568	433
CVE-2746-939568	367
CVE-2746-939568	343
CVE-2746-939568	221



United States

CVE Detections

CVE-2746-939568	500
CVE-2746-939568	467
CVE-2746-939568	433
CVE-2746-939568	367
CVE-2746-939568	343
CVE-2746-939568	221
CVE-2746-939568	211
CVE-2746-939568	187
CVE-2746-939568	123



These are the top Common Vulnerabilities and Exposures (CVEs) that attackers attempted to exploit, based on analysis of blocked malicious files. Mimecast recommends that you identify which CVEs are relevant to your organization and consider prioritizing the patching of those vulnerabilities.



Thank you!

mimecast

[Your Company] | [Account Code] | Monthly Human Risk Insights Report
01 Sep 2025 to 30 Sep 2025