IRONSCALES
SAFER TOGETHER

IRONSCALES THREAT INDEX

Q4'22/Q1'23 Edition

8 Million

The number of phishing incidents IRONSCALES caught that slipped past traditional email defenses*

88%

of those messages were **unknown threats** - advanced phishing attacks that use social engineering tactics to create a false sense of trust and urgency to get the victim to act fast. These threats evade traditional security measures, but can be detected by a combination of machine learning technologies (AI) and human insights.

***Disclaimer:** This IRONSCALES Threat Index encompasses email data across all of IRONSCALES Microsoft 365 and Google Workspace protected customers from October 2022 through March 2023, and compared to the previous six months (April 2022 to September 2022) to identify trends.

Known phishing scams increased slightly (>2%)

72% → 10.5%

of all known phishing scams were credential theft attempts

spike from the previous six months

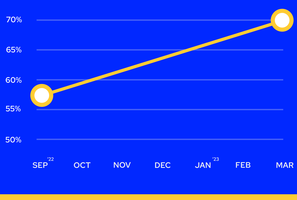
35% increase in BEC attempts from previous six months

~10%

of all phishing scams were BEC attempts

57% to 70%

Payment scams increased sharply over six months



Top 3 Industries Impacted by Phishing and BEC

- Financial services
- Industrials (manufacturing, construction, etc.)
- Computer hardware or software

Threat Dictionary

Definitions of various email scams referenced in the Threat Index

Advance-fee Scam

A scam that promises a large sum of money, often harvesting sensitive information and requesting a smaller up-front payment to obtain the promised money.

BEC Payment

A scam that involves a payment or wire-transfer inquiry or request.

Credential Theft

A type of phishing attempt that tries to manipulate the recipient to get their credentials. Examples include: vendor impersonation messages about password status changes, terms of service changes, payment information updates, account or subscription pending deletion or cancellation, confirmation of document receipt that can only be viewed by logging in using a malicious link, or addition to a team or group at work that requires confirmation using a malicious link or attachment.

Lottery Scam

A scam that involves fake notices of lottery wins, often harvesting sensitive information and requesting a small fee to obtain the lottery winnings.

Suspected VIP Impersonation

An email designed to look like it came from a known VIP, usually sent from a different email address or third-party service. These are often used in BEC attacks and don't have a malicious link or attachment, but an urgent call-to-action.

BEC Gift Card or Purchase Task

A BEC attack that requests the recipient to make a gift purchase, usually a gift card, on behalf of the impersonated sender.

BEC Task

A scam that involves a request for an urgent task. Sometimes the scammer checks for the availability of the recipient by asking for a return communication via phone call. Often, the type of task is not specified.

Extortion

A scam that typically involves fake claims about access to private information, which will be used as leverage to extort large sums of money.

Sextortion Email

An email that involves fake claims about having access to the recipient's videos that are sexual in nature which will be used as leverage to extort large sums of money.

Suspected Malicious Payload Email

Any email attack that has a link or attachment that might be malicious.

Stop Phishing. Dead in its Tracks.

IRONSCALES is the industry's only AI and human insights enterprise email security solution protecting 10,000 global customers.

Ready to experience the power of IRONSCALES for yourself?

Request a Demo