

Solution Brief

# Contextual Email Banners

Just-in-time end user notifications of potential email attacks



No matter how good your email security solution is, reality is that your end users are the absolute last line of defense. Alert them against potentially malicious attacks with just-in-time warning banners directly in a suspicious email.

## Our contextual banners provide warnings for the following:

- First-time sender
- Business Email Compromise (BEC) Language
- Sender Address Spoofing
- Exact Display Name Impersonation
- Similar Display Name Impersonation
- Email Domain Look-Alike
- Company's Name Appears in Display Name
- Known Address in Display Name



“Companies need a solution that warns their end users of potential attacks in an intelligent, laser-focused manner so as not to cause banner fatigue.”

---

### The Challenge




Advanced phishing attacks are constantly evolving and even the most intelligent machine learning/AI-powered email solutions don't catch everything. Legacy email technologies are known to put banners into every email sent from outside the company, leading to end users ignoring the notifications.

Companies need a solution that warns their end users of potential attacks in an intelligent, laser-focused manner so as not to cause banner fatigue.

---

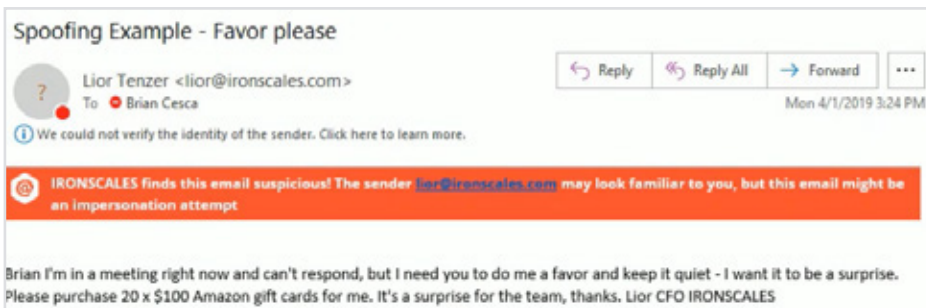
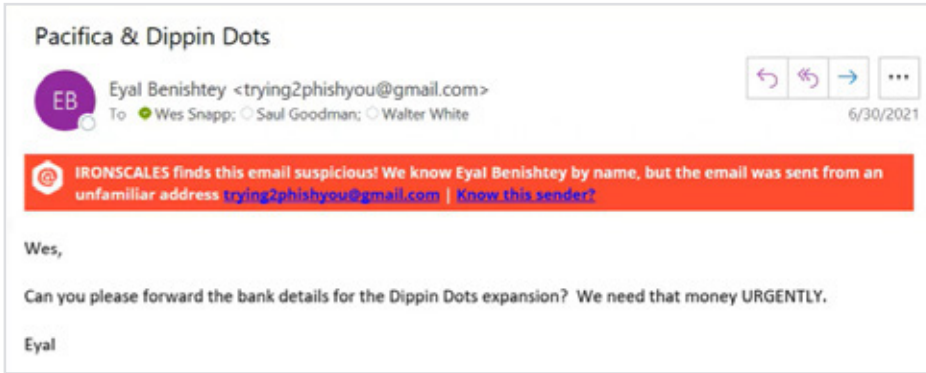
### The Solution

IRONSCALES' just-in-time contextual banners are automatically injected into emails flagged as suspicious by our Machine Learning (ML) models.

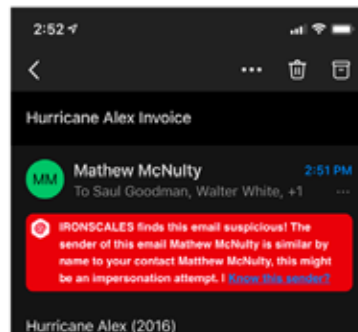
-  Each banner provides specific details about why our ML models have determined that the email is suspicious
-  Customize the banners however you like, including such things as adding your logo, escalation point of contact details and more.
-  The 90-day scan back that is done when you are onboarded will identify a baseline of external senders that each of your end users communicates with on a regular basis, eliminating the need for first-time sender banners for those identified external senders.

## The banners work seamlessly regardless of device or email client:

### Desktop View



### Mobile View



With banners, warnings and intuitive self-management, it's easy to prove that IRONSCALES is protecting our company. And it really is essential to have the visual tools that IRONSCALES provides to show our board and to easily demonstrate that our email security system is secure.

NEIL STEIN, SVP OF TECHNOLOGY SERVICES AT ORTHOCAROLINA

### Why choose IRONSCALES?

1. We are fast to deploy, simple to manage and highly effective in stopping all types of email attacks
2. We deliver email security in the mailbox and defend against modern email threats
3. We integrate both email security and awareness training into a single offering

[www.srccybersolutions.com](http://www.srccybersolutions.com) | +91 120 232 0960 / 1 | [sales@srccybersolutions.com](mailto:sales@srccybersolutions.com)



## ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

