White Paper

Common Tips for Preventing Email Spoofing

IRONSCALES
SAFER TOGETHER

Contents

There are several common methods typically discussed as barriers to email spoofing.

Let's look at their benefits and limitations more closely:

Sender Policy Framework (SPF)

Definition

- Sender Policy Framework (SPF) checks the IP addresses of incoming emails against a company's Domain Name System (DNS).
- If sender addresses don't meet DNS conditions, emails are rejected, keeping malicious emails from ever entering employees' inboxes.
- Works at the SMTP level.

Limitation

SPF is limited to 10 lookups. Many companies have multiple cloud-based services that can send messages, causing companies to bump up against this restriction almost immediately.

Records only apply to specific Return-Path domains and not those found in the 'from' address. This leaves a window for scammers to create messages that will authenticate, allowing scammers to spoof the visible "From" field.

Example:

From: Bank of America <billpay@billpay.bankofamerica.com>
Return-Path: <recepcionfacturas@grupo-emsa.com.mx>
Subject: Your eBill Due Date Is Approaching

DomainKeys Identified Mail (DKIM)

Definition

- DomainKeys Identified Mail (DKIM) acts as a second layer of protection after SPF.
- DKIM confirms sender domains and verifies that emails are sent from valid sources.
- DKIM assigns a public key to each sender's DNS record and creates a private key for outgoing email. If the keys match in an email exchange, it means that the messages weren't interfered with in transit.

Limitation

DKIM is famously challenging to implement. Perhaps for this reason, and the fact that a missing DKIM signature does not always mean a message is fraudulent, do if it is missing, the email will always get delivered. However, as with SPF, DKIM does not prevent a scammer from spoofing the visible 'from' field.

Example:

From: Billpay <billpay@billpay.bankofamerica.com>

Return-Path: <tua02@tribunalesagrarios.gob.mx>

Subject: Your eBill for Alex H. Lehocky

Domain-based Message Authentication, Reporting, and Conformance (DMARC)

Definition

- Domain-based Message Authentication, Reporting, and Conformance (DMARC) notifies domain owners when a spoofed email is detected and allows them to decide what should happen to that email.
- Admins can send spoofed emails to a spam folder or reject them outright.

Limitation

- Only works if SPF and DKIM are applied properly by the sender and receiver.
- Cannot protect against display name spoofing or domain impersonations.

Awareness Training

Definition

- Teaches employees common security practices like, being wary of emails that seem extra urgent, paying close attention to sender addresses, never sharing passwords or clicking into a website they've never been to, and changing their passwords often.
- Phishing tests are a good way to assess your employees' security knowledge and keep them on their toes.

Limitation

Training only goes so far-employees aren't actively looking for phishing emails like security teams might be, and they don't always abide by your company's security regulations. Employees don't recognize the nuance of every threat, so education can only be one step in a robust cybersecurity process.

Phishing tests can help, but scammers are constantly developing new techniques and leveraging social engineering, making it tough to test for every possibility and all it takes is one lapse of concentration.

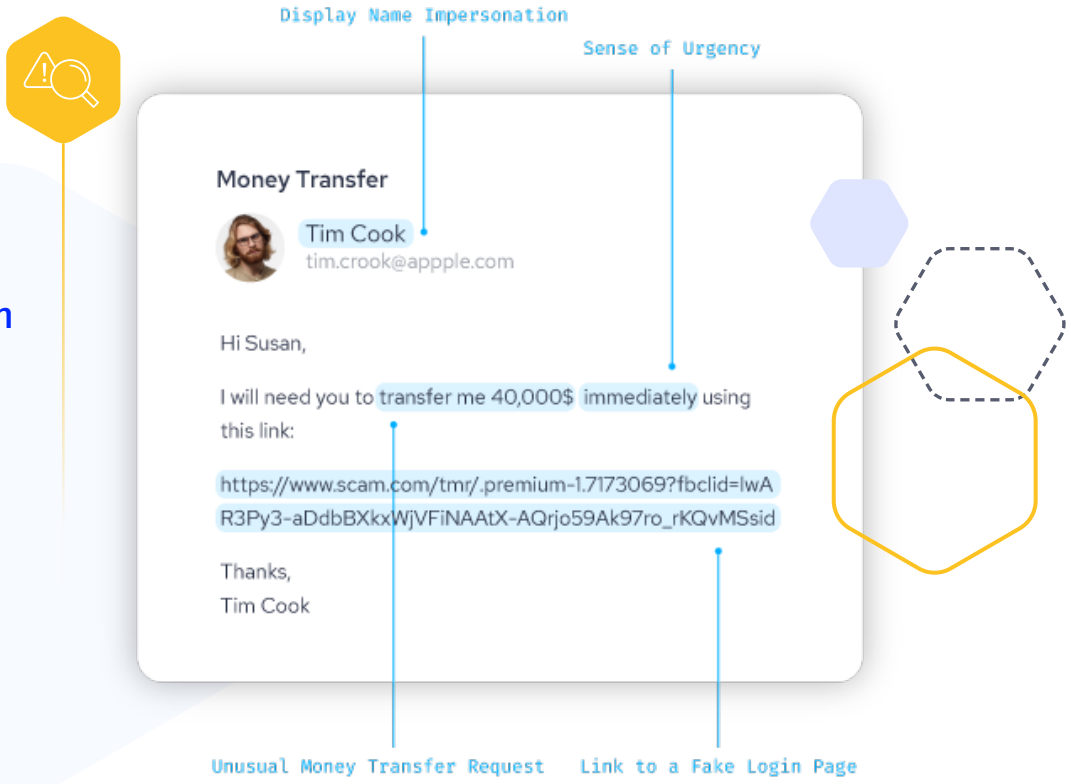
How to Successfully Prevent Email Spoofing

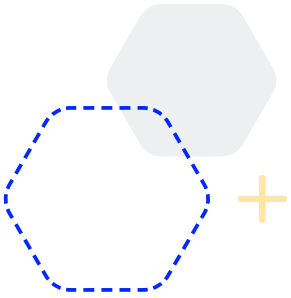
Email is now completely enmeshed with work, making spoofing prevention a baseline requirement in any organization. Commonly used strategies like SPF, DKIM, and DMARC have severe limitations, even when employed simultaneously. In fact, as more companies adopt those tactics, attackers launch more domain impersonation attacks that SPDF, DKIM, and DMARC cannot protect against.

Read our 3 part blog series
Understanding-DMARC: What's Driving All the Hype?

Modern spoofing prevention requires a blended approach of human and machine collaboration. Wading through thousands of emails a day and picking up on new abnormalities is an impossible task for humans alone, but not for computers.

AI systems flag possible attacks so that humans can review them for accuracy. Attacks that SPDF, DKIM, and DMARC cannot protect against.





AI-powered anomaly detection tools analyze both user behavior patterns and email metadata, helping the algorithms and platform better identify and respond to new spoofing techniques.

To react to spoofed emails quickly and effectively, organizations must layer advanced mailbox anomaly detection on top of SPF, DKIM, DMARC, and training.

Learn more about
Advanced Mailbox-level Anomaly Detection

Admins then provide feedback to the algorithm to make it stronger, creating an even more robust layer of protection.

Stop Spoofing With An Advanced Email Security Platform

IRONSCALES is a pioneer in the cybersecurity space, detecting email spoofing and other advanced threats better than any other platform on the market.

The IRONSCALES platform includes mailbox-level anomaly detection, anti-phishing tools, and protection against business email compromise (BEC). And with intelligent automation, IRONSCALES can stop phishing emails before they even hit your employees' inboxes.

Not only that, IRONSCALES is easy to use and deploy, allowing your security administrators to help your employees stay safer together.

IRONSCALES
SAFER TOGETHER

IRONSCALES is a self-learning email security platform that can predict, detect and respond to email threats within seconds.

Email threats are growing exponentially and morphing at scale. Each day, billions of new, increasingly sophisticated phishing attacks and launched globally. Legacy technologies like security email gateways (SEGs) have been shown to allow up to 25% of incoming phishing attacks through to their intended targets.

With IRONSCALES, you and your organization are Safer Together because of the following:

- Advanced malware/URL protection
- Mailbox-level Business Email Compromise (BEC) protection
- AI-powered Incident Response
- Democratized real-time threat detection
- A virtual security analyst
- Gamified, personalized simulation and training

To learn more, please visit **www.ironscales.com** today!