Email Link Isolation

Isolate email links to reduce attack surface and simplify operations

Reduce phishing risks by applying browser isolation protections and controls

Challenge: Sophisticated multi-channel phishing

Multi-channel phishing spans email and web delivery in ways that can adeptly evade filtering rules. Such common types include:

- **Deferred phishing**: An initially benign link within an email is later weaponized with a malicious destination after delivery.
- **Cloud service phishing:** Dangerous HTTPS links closely resemble common cloud services (e.g. Google Drive, Box)

To stop threats like these, modern email protection must be equipped to apply Zero Trust 'never trust, always verify' scrutiny to all links.

Solution: Email link isolation

Integrating remote browser isolation (RBI) capabilities with cloud email security (CES) applies that scrutiny to bolster phishing protection. Soon, Cloudflare Area 1 customers will be able to turn on Cloudflare Browser Isolation to neutralize these multi-channel threats.

Administrators can control user interactions on isolated webpages (such as restricting keyboard input and file uploads) to prevent phishing impacts like credential harvesting or confidential data theft.

Plus, opening up email links in an isolated browser neutralizes malware by running all code in the cloud, far away from local devices.

What analysts are saying:

"Email-based URLs that resolve externally are often used to phish employees. Isolating these can reduce successful phishing attacks."

"Most attacks are delivered via the public internet, through either web browsing or emailed links that trick the user into visiting malicious sites. Simply removing (or, more strongly, isolating) the browser from the end user's desktop significantly improves enterprise security posture, including protection from ransomware attacks."

"Evaluate and pilot a browser isolation solution for specific high-risk users (such as finance teams) or use cases (such as rendering email-based URLs), particularly if your organization is risk-averse." [1]

Gartner

Read more

Business benefits of integrating CES & RBI

Bolster phishing protection

Email isolation not only stops harmful code in a phishing link from executing locally, but also applies data protection controls to prevent sensitive information from falling into the wrong hands.

Unlock IT and security productivity

Turn on email isolation for any website with a few clicks.

IT and security teams avoid the hassle of configuring filtering policies that risk 'over-blocking' (and limiting user productivity) and 'under-blocking' (and letting threats in).

Sample use case: Stopping deferred phishing

Problem: Deferred phishing evades detection

With the right tactics and motivation, deferred phishing campaigns can bypass traditional protections.

Campaign setup: Attackers can start by sending an authentic-looking email from a newly created domain, using proper email authentication (SPF, DKIM, DMAR) and a benign web page.

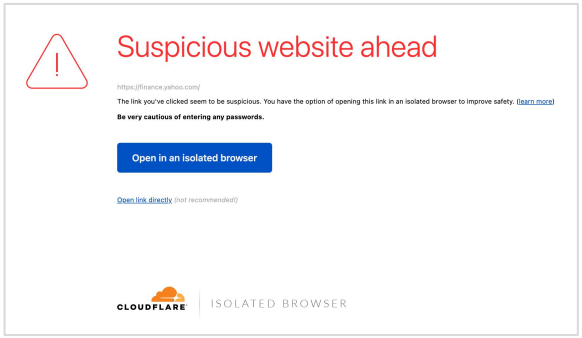
Successful delivery to inboxes: These emails can evade detection by secure email gateways, authentication-based filters, or other services that rely on reputation-based signals and other deterministic techniques.

Pivoting to a malicious link: With the email successfully delivered, the attacker can pivot the link to a malicious destination by changing the attacker-controlled webpage. For example, a common pivot is to a fake login page used to harvest credentials.

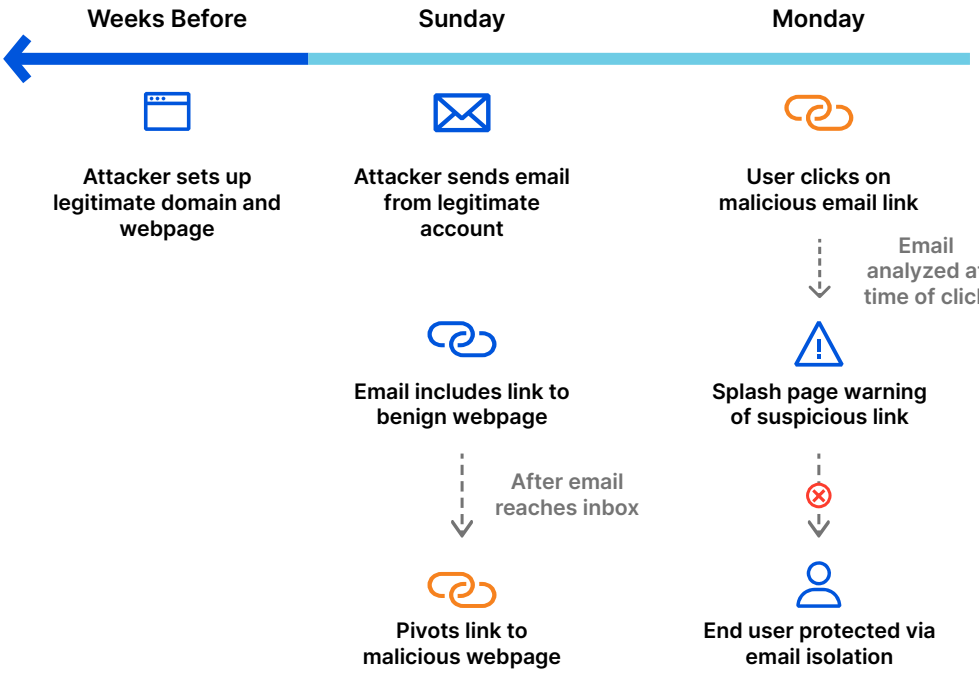
Solution: Isolate suspicious links post-delivery

Email link isolation provides a critical layer of post-delivery protection. Cloudflare analyzes any link within an email that a user clicks. If the link is deemed suspicious or risky, Cloudflare displays a warning splash page *(see below)* and then isolates the webpage if the user navigates through.

Admins keep malicious code from executing on local devices and can apply data protection controls, such as restricting file uploads and downloads, preventing user keyboard input, or opening the page in read-only mode.



Timeline of a deferred phishing campaign



Cloudflare analyzes each link at the time of click

Safe link: Users will be redirected to this site transparently.

Malicious link: Users are blocked from navigating.

Suspicious link: Users are heavily discouraged from navigating and are presented with a splash warning page encouraging them to view in the link in an isolated browser.

Integrating Cloud Email Security with Cloudflare Zero Trust

Modern security with Zero Trust

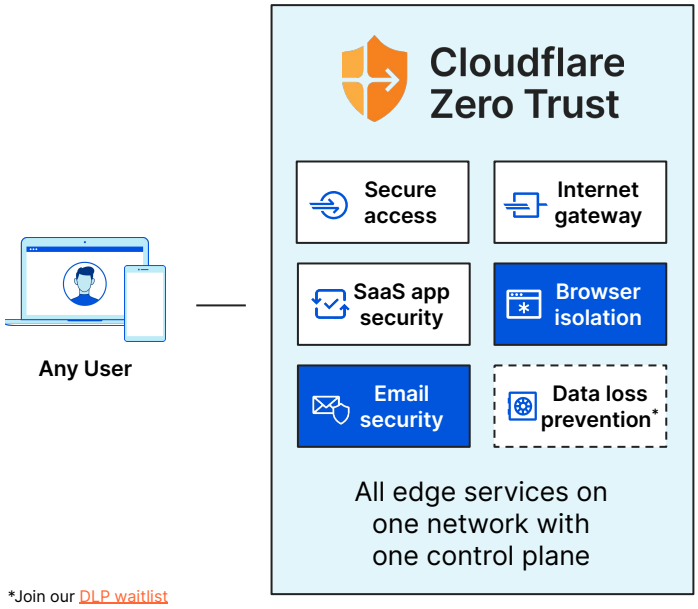
Cloudflare Zero Trust increases visibility, eliminates complexity, and reduces risks as remote and office users connect to corporate applications and the public Internet.

On April 1 2022, Cloudflare completed the acquisition of Area 1 Security with a vision of augmenting how our Zero Trust platform will protect users from phishing attacks in email, web, and network environments. Read more here.

Email Security: Core to Zero Trust

Cloudflare Area 1 email security enhances Zero Trust by removing implicit trust from email to preemptively stop phishing and business email compromise (BEC) attacks.

Never trust any sender, even if internal. Instead, ensure all user traffic including email is verified, filtered, inspected, and isolated from Internet threats. Email security will be integrated across Cloudflare's Zero Trust services, in powerful combination with RBI, CASB, and more.



*Join our DLP waitlist

VPN replacement
simplify and secure connecting any user to any resource

Internet protection
keep your data safe from threats over any port and protocol

Streamline SaaS security
visibility and control of applications including email

Security modernization
improved productivity, simpler operations, reduced attack surface

Cloud Email Security (CES)

- Reduce phishing incident response times by 90%.
- Identify attacker infrastructure and delivery mechanisms ahead of time to stop phishing at the earliest stages of the attack cycle.
- Remove implicit trust from email by analyzing content, context, and social graphs of communications.
- Leverage integrations with Microsoft, Google, and other environments to enhance built-in security

Remote Browser Isolation (RBI)

- Stop credential compromise by opening risky sites in 'read-only mode' by controlling user interactions (e.g. keyboard input, copy & paste, up/download).
- Run all browser code on Cloudflare's network, insulating local devices from malicious code.
- Deliver a frictionless, fast end-user experience. Instead of typical pixel streaming, we draw an exact replica of the page from a remote browser just <50ms away from 95% of Internet users globally.

Request a phishing risk assessment today **Contact us**

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

REV: PMM-2022JUN

[1] *Gartner Hype Cycle for Network Security, 2021* | GARTNER and HYPE CYCLE are registered trademarks and service marks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.