CLOUDFLARE

ASSESSMENT BRIEF

Phishing Retro Scan

Identify the threats that have bypassed your current defenses to quickly remediate phishing exposure

Greater visibility into phishing exposure

Discover which phishing threats have already reached your end users

With phishing attacks on the rise and social engineering tactics becoming more convincing, it's no wonder why user exploitation poses the biggest security risk to organizations. While cloud email providers and secure email gateway (SEG) vendors offer various controls to limit unwanted emails, more targeted and deceptive phishing attacks can often bypass traditional security measures.

Cloudflare, a 2023 Forrester Wave™-recognized leader in Enterprise Email Security[1], offers a self-service tool that retroactively scans Office 365 inboxes in minutes to identify malicious and unwanted emails that have been delivered over the past 14 days. This includes identifying active phishing attacks that have evaded existing security controls and are already in the inbox, posing an immediate threat to your organization.

Running a retro scan

Steps	Benefits
1. Log in to existing Cloudflare dash account (or create a free account if one doesn't exist) 2. Access "Area 1" from left navigation bar 3. Run scan by clicking "Generate Retro Scan Report" button 4. Complete steps to authorize Microsoft 365 access and select email domain(s) to scan 5. Review report once scan has completed (email confirmation will be sent once scan is done)	• **Scan Office 365 inboxes in minutes** to immediately see malicious and unwanted emails delivered over the past 14 days • **View and download a customized report** that provides both an overview and detailed breakdown of emails flagged during the scan • **Connect with an email security expert** to better understand the types of threats detected and how to best remediate exposure

Run a free phishing retro scan to instantly see:

Who within your organization is most frequently targeted

How many malicious and unwanted emails are sitting in your inboxes

What specific threat types are evading your current defenses

Which attack groups and phishing tactics are targeting your users

Where malicious and unwanted emails are originating

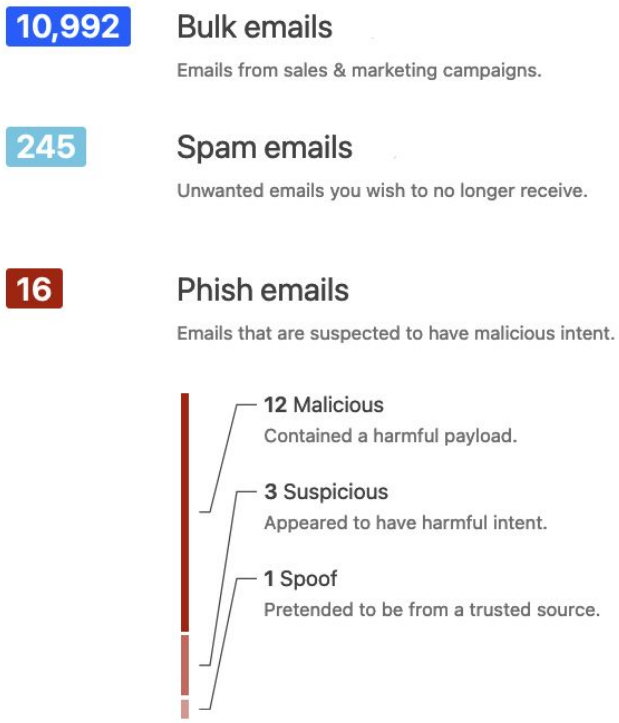
Example retro scan results

See a detailed breakdown of malicious and unwanted emails sitting in your inbox

Running a retro scan provides a full phishing assessment in minutes, detailing the frequency and type of threats that have reached your inboxes over the past 14 days, including active phishing attacks that have already bypassed Microsoft's built-in protections and any deployed email security solutions.

Once the scan is complete, a report is generated to provide both an overview of threat types discovered, as well as contextual data for each email identified. Emails flagged during the scan include:

- **Malicious:** Phishing emails that contain harmful payloads, links, or other deceptive elements. These emails seek to exploit users trust in an attempt to gain unauthorized access or commit financial fraud.
- **Suspicious:** Potentially harmful emails that appear to have malicious intent. These emails often require time and resources to investigate.
- **Spoof:** Phishing emails that attempt to trick users into thinking a message came from a person or entity they know and trust.
- **Bulk:** Emails from sales and marketing campaigns. While harmless, bulk emails are time-consuming and distracting.
- **Spam:** Unwanted emails that are harmless, but clog up inboxes and disrupt user workflows.



Sample phishing attack detected

QR codes are an increasingly popular phishing tactic for bypassing email security

While there are many clever and evasive phishing tactics in use today, QR codes are being leveraged more frequently by attackers to evade email security controls and pivot the user to a less secure attack channel, which in this case happens to be a mobile device. The goal of the attack is to bait the user into scanning the QR code and open the underlying malicious link that leads to a spoofed login page in an effort to steal the user's credentials.

Cloudflare uses an array of sophisticated techniques to identify QR code attacks, including optical character recognition (OCR) and ML-powered contextual analysis. Together, these techniques deconstruct and cross-validate the language and various elements within the message to determine the authenticity of the sender. The sample phish below shows how attackers utilize brand impersonation and malicious links to deceive users.

Why Cloudflare?

One unified platform

Secure access
by verifying and segmenting any user to any resource

Threat defense
by covering all channels with network-powered AI/ML & threat intel

Data protection
by increasing visibility and control of data in transit, at rest & in use

One programmable network

More effective
by simplifying connectivity and policy management

More productive
by ensuring fast, reliable, and consistent user experiences everywhere

More agile
by innovating rapidly to meet your evolving security requirements

Ready to see what's lurking in your inboxes?

Run a retro scan

1. Source: The Forrester Wave™: Enterprise Email Security, Q2, 2023