proofpoint.

SOLUTION BRIEF

Proofpoint Collab Protection

Protect your people from messaging and collaboration threats

Key benefits

- **Extend phishing protection** beyond email
- **Block malicious URLs** in real time
- **Get visibility** of phishing threats across all digital channels
- **Lower your risk** of data breaches with extended phishing protection

In today's dynamic work environment, people communicate and collaborate beyond email. They also work in many other digital channels, such as messaging, collaboration and social media platforms. Threat actors have recognized this shift and now exploit those channels to launch attacks.

Messaging and collaboration platforms under siege

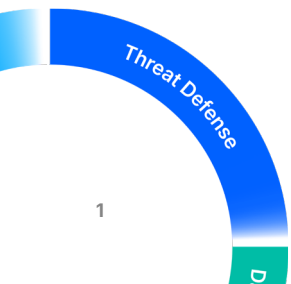
Attackers are making messaging and collaboration platforms the new launch pads for their phishing attacks. To do this, they are using social engineering tactics and malicious URLs. Malicious URLs are now the most common way that attackers deliver their payloads. Over the past three years, the Proofpoint Threat Research team has seen a whopping 2,524% increase in URL threats delivered through SMS-based phishing (smishing). Bad actors use messaging and collaboration applications to set up false accounts, establish sham relationships, and direct people to fake login pages. These pages are designed to harvest personal information and trick users into transferring money or revealing sensitive company information.

How attacks in messaging and collaboration applications happen

A phishing attack that targets a messaging or collaboration application such as Microsoft Teams, Slack or Zoom typically has the following stages:

Figure 1: Attacks on messaging and collaboration applications typically have multiple stages.

This solution set is part of Proofpoint's integrated Human-Centric Security platform, mitigating the four key areas of people-based risks.



Strengthen messaging and collaboration security

Messaging and collaboration applications don't have native security features to protect your people and business from phishing attacks. This is where Proofpoint can help.

Proofpoint Collab Protection protects against malicious URLs that are delivered in any messaging, collaboration or social media application. It performs URL reputation inspection and analysis in real time and blocks malicious URLs when users try to access them. With Collab Protection, Proofpoint protects your users from advanced phishing attacks anywhere, anytime.

Protect people from malicious messages

Collab Protection is powered by industry-leading threat intelligence from Proofpoint. When an employee tries to access a suspicious link in a messaging or collaboration application on their desktop or mobile device, Collab Protection analyzes the URL in real time. It does a URL reputation check and analyzes any URL rendered in the browser. If Collab Protection finds a malicious URL, it blocks it. In this way, your users are protected from malicious websites and content.

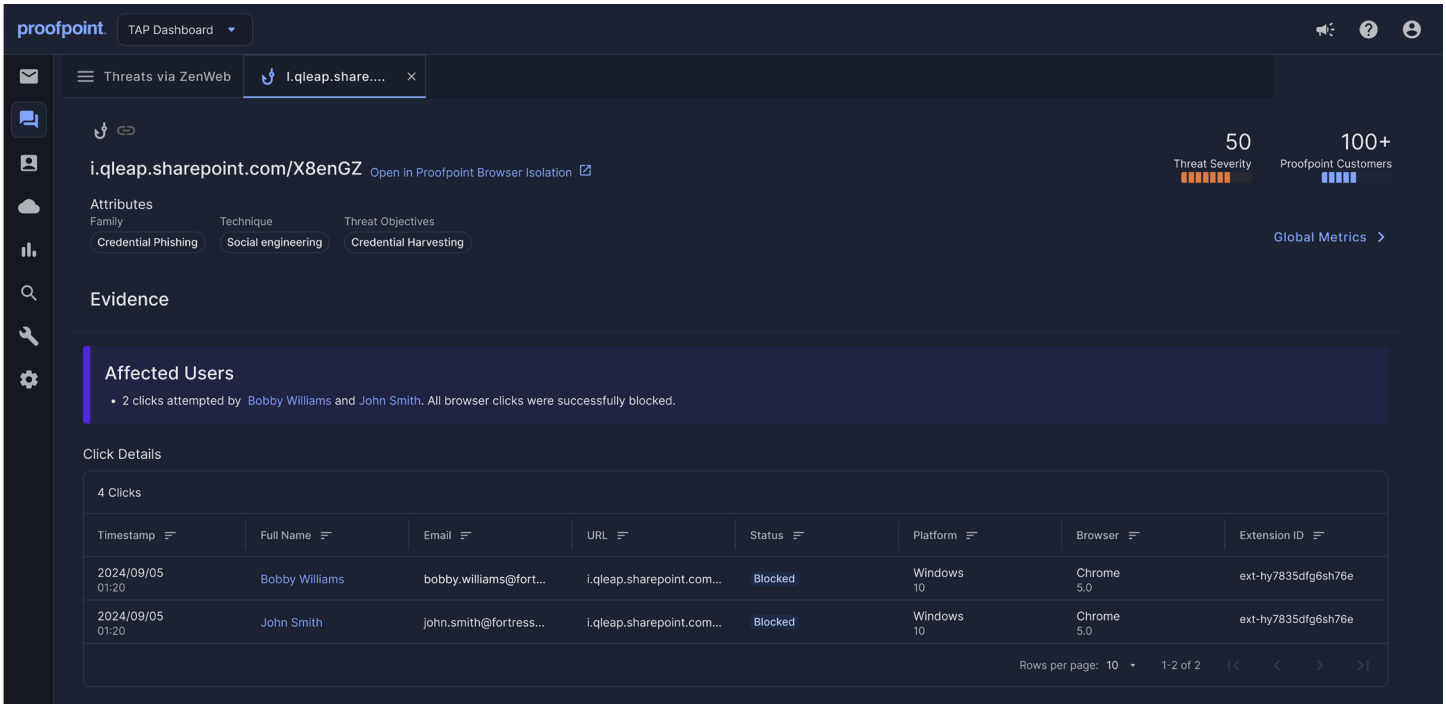


Figure 2: Collab Protection analyzes URLs accessed by your users in real time.

Get multi-channel phishing threat visibility

Bad actors now target your people across multiple digital channels. These channels include email, collaboration platforms such as Microsoft Teams, Slack and Zoom and even text messages. Your security and IT teams need to watch for threats in all of those channels. Collab Protection gives you this multi-channel visibility. If an employee accesses a suspicious link in a messaging or collaboration application, Collab Protection shows the user(s) that have accessed the link and which device (desktop or mobile) the link came from. It also shows whether it has blocked the associated URL. Because it gives you a unified view of threats across all of your channels, Collab Protection helps you to track and mitigate phishing threats faster. Your security and IT teams can detect and stop attacks before they harm your business.

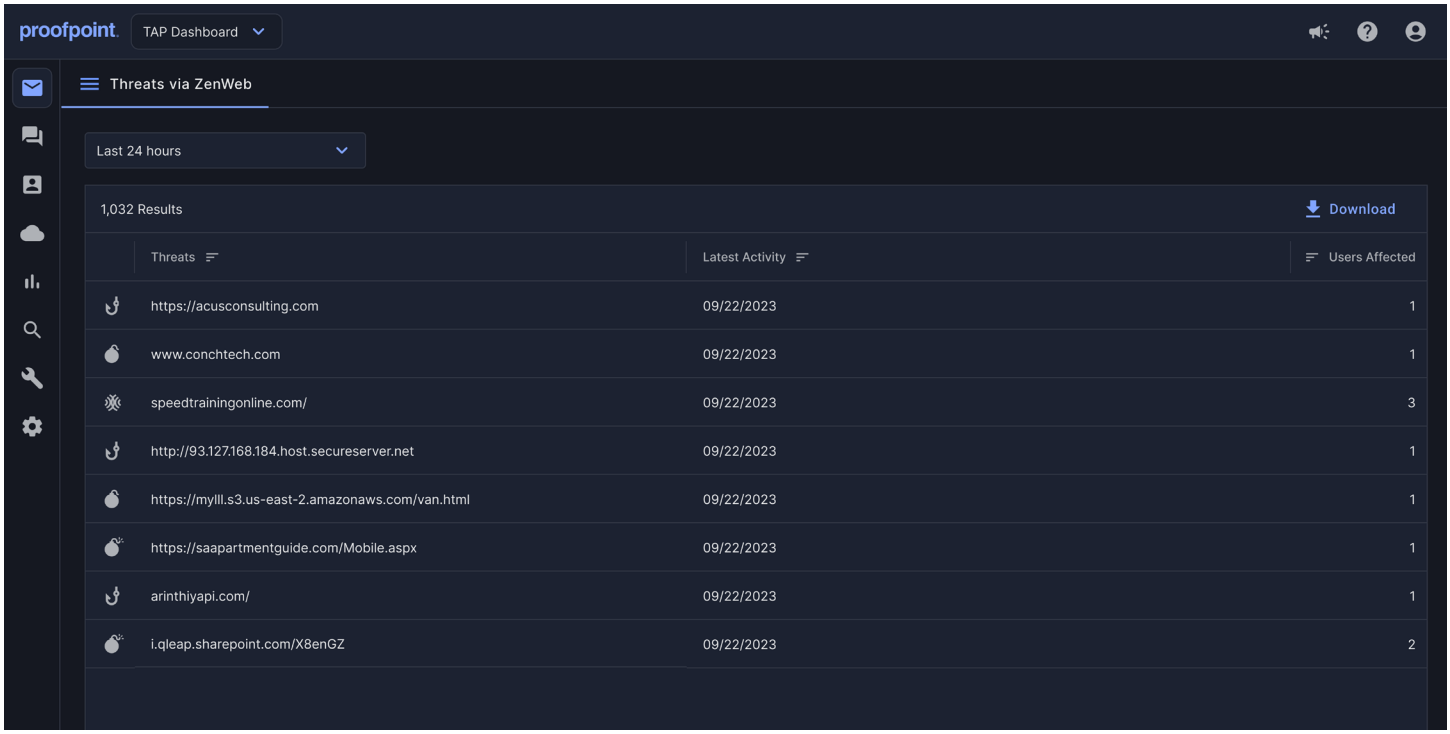


Figure 3: Collab Protection provides a unified view of threats in multiple channels.

The next evolution: human-centric security

Modern workers increasingly communicate and collaborate in channels other than email. Bad actors are exploiting this change to find new entry points for cyber attacks. These include phishing, malware and account takeover attacks. To stay ahead of these emerging threats, you need a solution that extends the same detection accuracy as your email protection to messaging and collaboration apps.

With Proofpoint Collab Protection, your organization can extend phishing protection beyond email. Collab Protection can stop malicious phishing messages in any messaging or collaboration application. Its URL reputation inspection and analysis detects and blocks these threats in real time. This means that you can protect your people from advanced phishing attacks anytime, anywhere.

proofpoint.

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 85% of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

Connect with Proofpoint: X | LinkedIn | Facebook | YouTube

DISCOVER THE PROOFPOINT PLATFORM →