caniphish

CanIPhish SaaS Platform

Phishing Simulation that Accelerates Business

CanIPhish trains your users by blending vulnerability discovery, exploitation and social engineering to deliver real-world phishing simulations.

Discovery

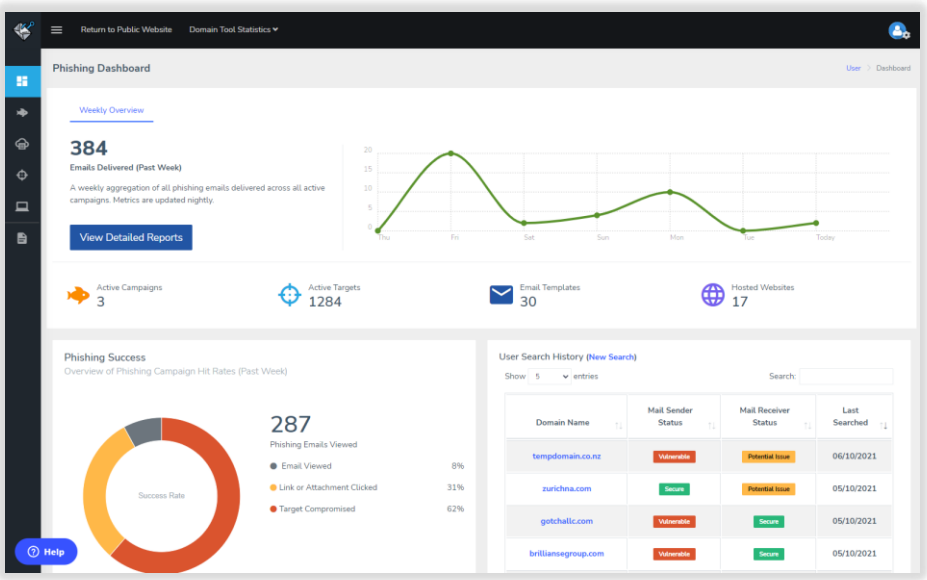
Discover vulnerabilities in your email sender and receiver supply chains.

Simulation

Blend vulnerability exploitation with tailor-made phishing material.

Training

Track, train and target vulnerable users for future simulations.



Key Use Cases

- Gain visibility into email sender vulnerabilities which enable domain spoofing.
- Gain visibility into email receiver vulnerabilities which enable filter bypass attacks.
- Simulate phishing attacks based off malicious activity detected in-the-wild.
- Deliver tailor-made phishing material targeted towards your users or industry vertical.
- Use managed or self-hosted infrastructure for email delivery and phishing websites.
- Incorporate email sender and receiver supply chain vulnerabilities into campaigns.
- Create recurring and dynamic campaigns to introduce operational efficiencies.

Connect With Us

CanIPhish SaaS Platform - Discovery

Discover vulnerabilities in your email sender and receiver supply chains.

1. Identify domains vulnerable to spoofing

Using a tailor-made analysis engine, identify vulnerable SPF & DMARC configurations on any given domain.

2. Identify domains with a vulnerable mail receiver supply chain

Using a variety of proprietary techniques, identify what mail gateways, spam filters and malware filters any given domain is leveraging – also identify whether the supply chain is vulnerable to attack.

3. Identify domains with a vulnerable mail sender supply chain

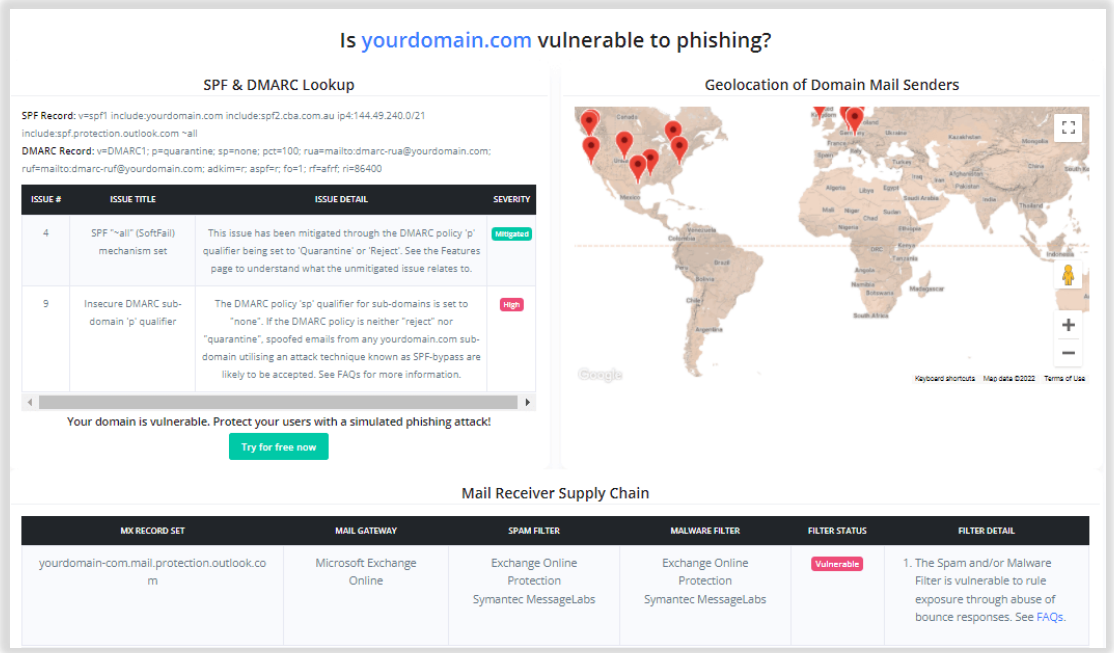
Using a tailor-made scanning engine, identify the full mail sender supply chain of any given domain.

4. Visualise mail sender geolocations

Enhance and visualise mail sender supply chains with near exact geolocation information. Providing insight into geolocation or politically motivated risks.

5. Identify malicious mail senders

Leveraging multiple IP-driven blacklists, identify malicious mail senders that exist in the mail sender supply chain of any given domain.



Vulnerability scanning automation

The CanIPhish SPF & DMARC analysis engine has been open-sourced to provide our users with the option to automate vulnerability scanning and reporting. Please see our GitHub project.

Historic search dashboard

Registered users can view their historical searches within the CanIPhish User Dashboard. The dashboard provides an overview of domains searched, vulnerabilities discovered and the last date of search by any user for a given domain.

CanIPhish SaaS Platform - Simulation

Blend vulnerability exploitation with tailor-made phishing simulations.

1. Simulate phishing attacks based off activity seen seen in-the-wild

Our content development team is constantly updating the email and web phishing template libraries based off malicious activity seen in-the-wild.

2. Deliver tailor-made phishing material

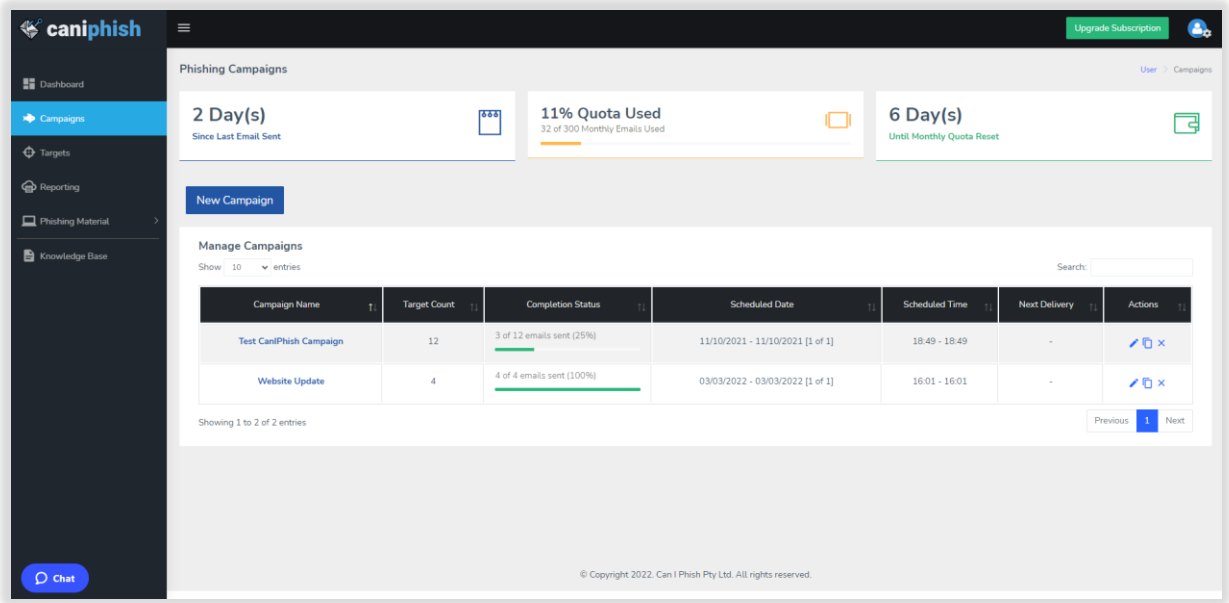
Using a highly configurable platform which supports the creation of new sender profiles, custom phishing emails and managed or self-hosted phishing websites.

3. Automate the phishing process through recurring and dynamic campaigns

Using our campaign scheduling engine to setup recurring campaigns monthly, quarterly or yearly. Recurring campaigns can be set to automatically update with the latest phishing library material

4. Exploit email sender or receiver supply chain vulnerabilities during campaigns

Exploit vulnerabilities which enable you to spoof an email domain. Adding an extra layer of realism to campaigns by abusing misconfigurations which threat actors frequently utilise.



Fully managed or self-hosted

The CanIPhish platform by default allows you to leverage our own email and web-hosting infrastructure for the delivery of phishing material. This is however fully configurable, with the option to use your own infrastructure for both email delivery and web-hosting.

Highly flexible campaign scheduling

Phishing campaigns are scheduled to operate between particular days and at certain times based off a time zone that you configure. This enables you to schedule campaigns at a time that best suits your organisational needs and has the biggest impact on security awareness.

CanIPhish SaaS Platform - Training

Track, train and target vulnerable users for future simulations.

1. Track every stage of the phishing simulation kill-chain

Leveraging a variety of techniques, track which users fell for, or partially fell for a phishing campaign:

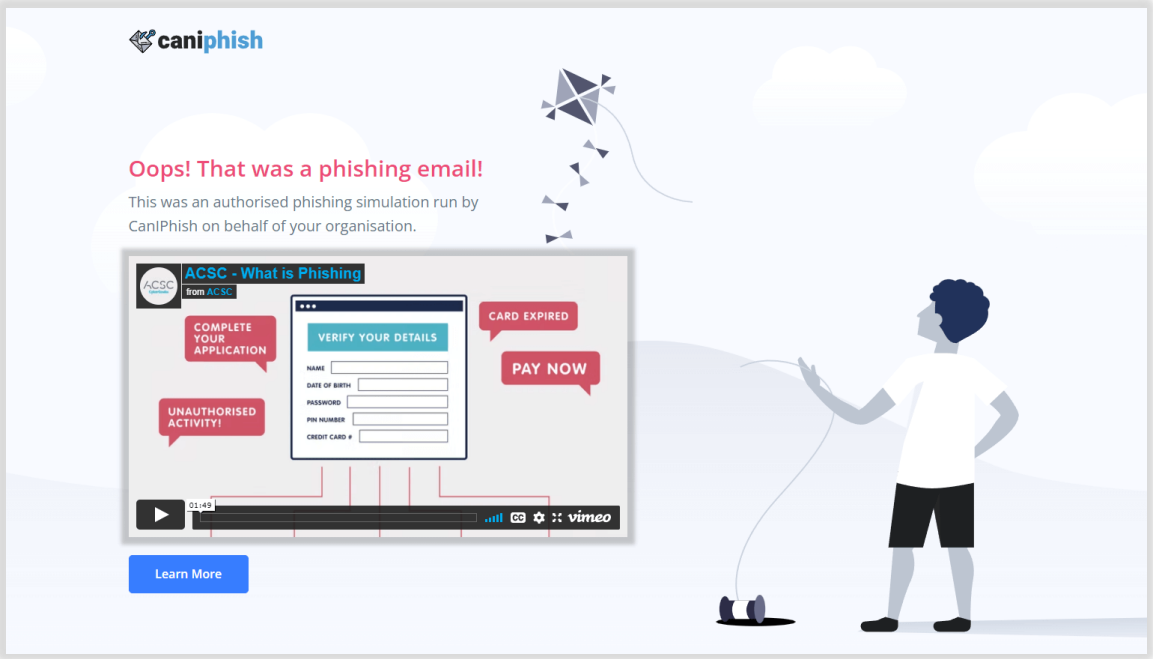
a. See users who viewed a phishing email
b. See users who clicked the link in a phishing email
c. See users who entered credentials into a phishing website

2. Train users immediately or on-demand

Once a user falls for a phishing email and/or inputs their credentials into a phishing website, CanIPhish presents the user with immediate security awareness guidance on what phishing is and how to avoid phishing attempts in the future.

3. Target known vulnerable users for future simulations

CanIPhish leverages campaign tracking to provide the option of creating custom target groups with users who fell for previous phishing campaigns. Using this feature, you can target security awareness training at the users who need it most.



Executive Reporting

The CanIPhish platform includes verbose reporting to provide you with the information necessary to show gradual improvements in your organisations security posture. This is typically represented through a gradual decline in month-on-month phishing click-rates.