SafeToOpen®
& PhishingFree

PG. 2

Reduce Operational Expenses

PG. 3

Reduce Phishing Detection Time

PG. 4

Expand Customer Protection Coverage

https://safetoopen.com
https://phishingfree.com

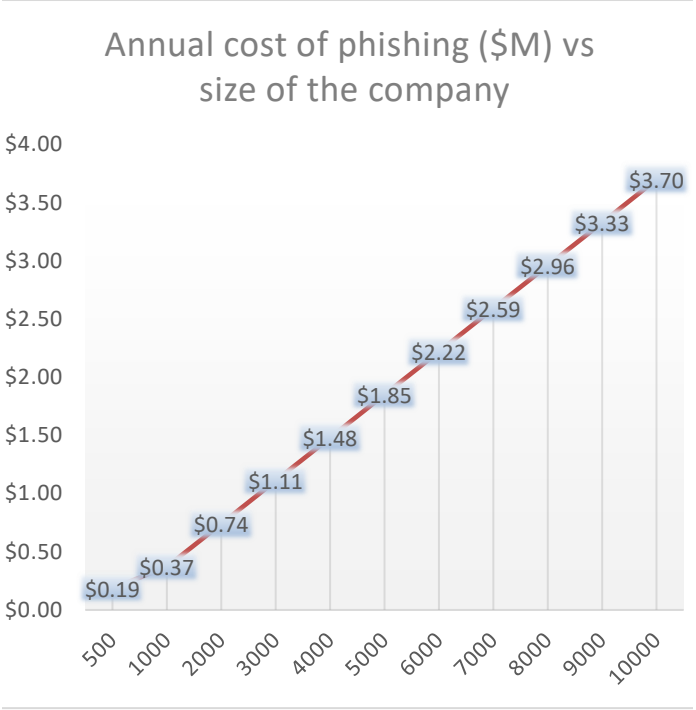
'THE AVERAGE 10,000 EMPLOYEE COMPANY SPENDS $3.7 MILLION A YEAR DEALING WITH PHISHING ATTACKS'

Ref: https://www.csoonline.com

> *Phishing scams are one of the most common, prolific and successful attacks we see. It's important to know how to protect your **business** and **customers** against them.*

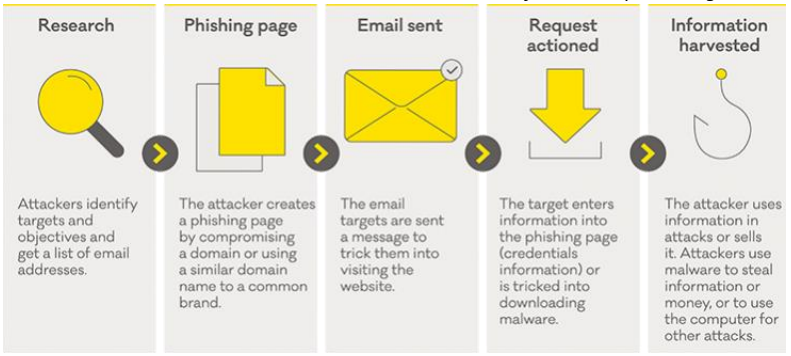
This money is spent on:

- IT department cost to resolve incident (includes staff and consultants)
- Legal cost: When a phishing scam is successful people often sue. Legal cost includes in-house counsel, outside counsel and settlement fees



- Call center
- Postal communications
- Lost revenue
- Reputation (or brand) damage
- Employee time wasted on phishing scams

PHISHING ATTACK PROCESS: *reference: https://cert.govt.nz*



"*The best way to reduce the cost of phishing scams is to reduce the detection and response times*" *–Maziar Janbeglou (Founder at SafeToOpen®)*

Why SafeToOpen?

SafeToOpen helps you reduce cost, reduce phishing detection/response time and protect your customers and brands.

1- OPEX AND ACCURACY IN VERIFYING REPORTED SUSPICIOUS EMAILS

Your security operation team is responsible to verify and respond to many suspicious emails reported by your staff as well as your customers every day. Manually going through and verifying a pile of reported emails can *take a lot of time* of your security team and may involve *human error*.

SafeToOpen email verification tool can hugely save time and reduce your Opex by:

- Quickly detecting and reporting Business Email Compromise (BEC) emails
- Using SafeToOpen's Microsoft Outlook add-in which enables your staff to easily report suspicious emails from within your organisation
- Quickly scanning all attachments and URLs and replying to your staff indicating whether the email is safe or not

- Analysing all reported emails from *your customers* and giving your security team detailed information allowing them to respond appropriately
- Using SafeToOpen's dashboard which helps your security team quickly identify phishing campaigns and respond to them
- Quickly generating website-takedown email templates

2- REDUCE PHISHING DETECTION TIME

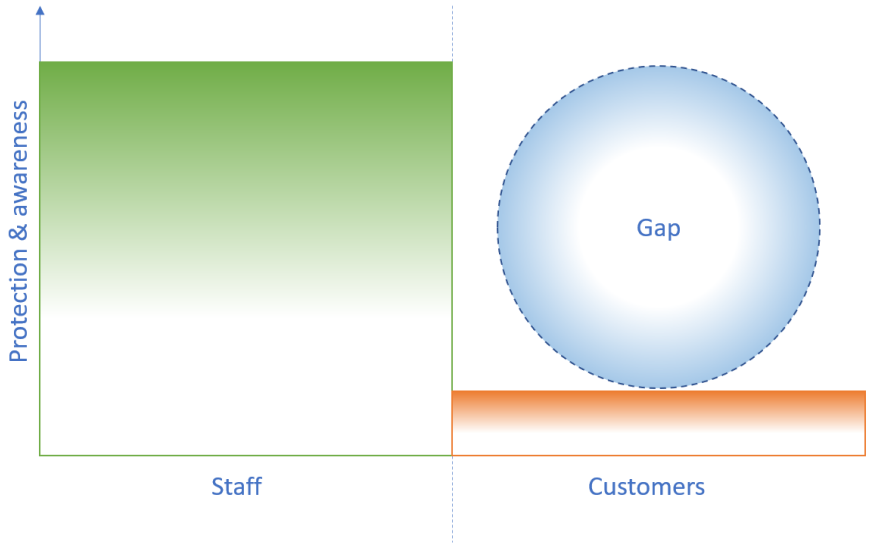
The traditional way of detecting phishing website is to *manually* verify emails reported by your customers or staff. Unfortunately, it is sometimes too late, and your customers and staff might have already given away their credentials.

SafeToOpen has taken a **unique approach** in detecting phishing websites by **examining your web servers' logs**, monitoring your brand in social media and reported text messages. *Our new technique can successfully detect phishing websites before Internet attackers send their malicious emails to your customers* (step 2 in phishing attack process). Our findings will be quickly reported to your security operation team to respond or we can eliminate those websites on your behalf. There is almost no setup cost for using our phishing detection service.

SafeToOpen uses **your business information** to *detect new phishing websites*. This information includes your business name, logo, geolocation, type of industry, etc.

3- EXPAND CUSTOMER PROTECTION COVERAGE

Your business may have invested in great security tools and subscribed to high-quality awareness improvement programs. *But none of those can **protect your customers** from being victims of a successful phishing attack.*

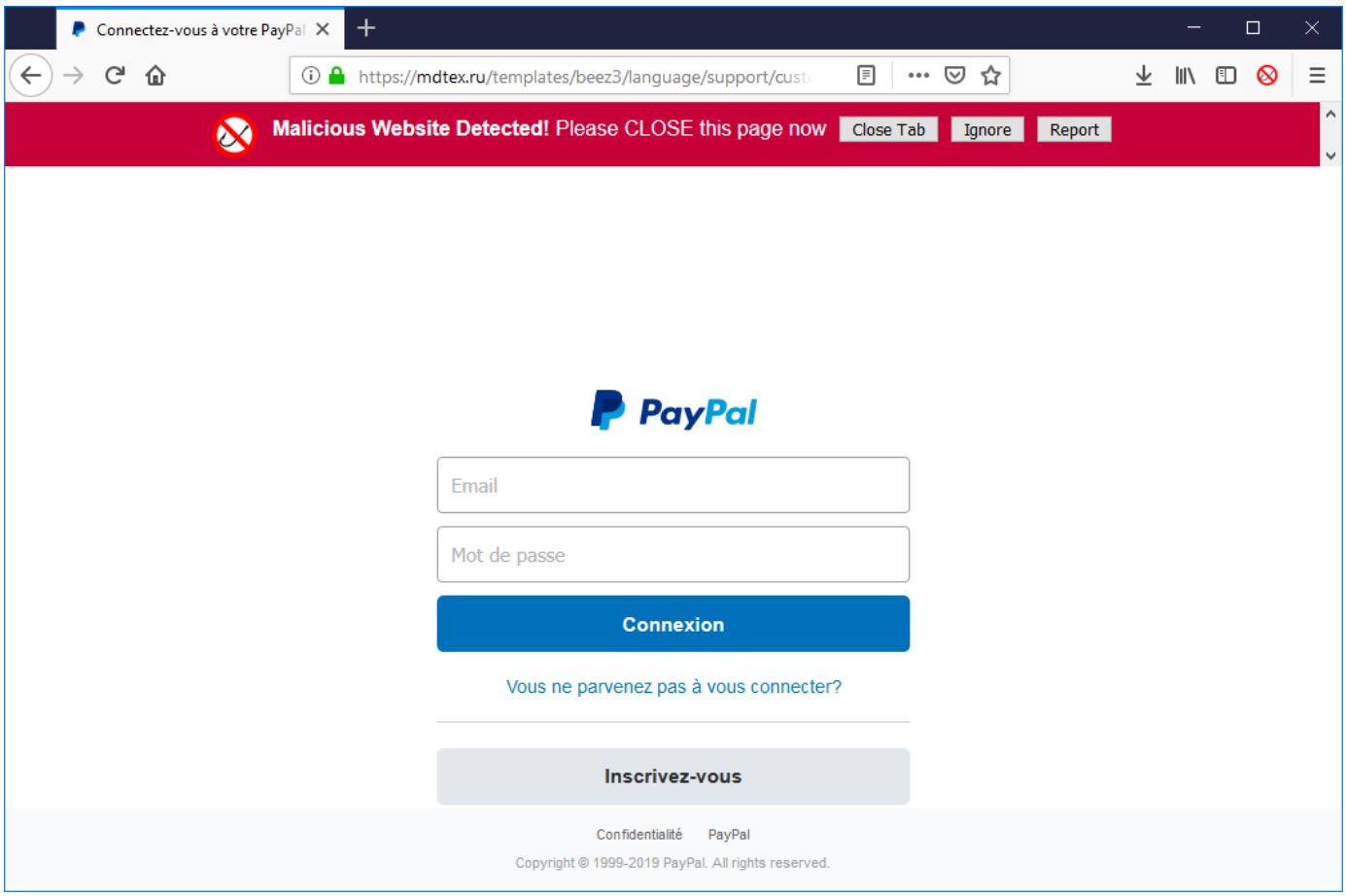


How do you protect your customers from targeted phishing scams impersonating your business?

As the above figure shows, your business can protect your staff from being a victim of successful phishing attacks with the implementation of email security gateways such as Microsoft Office 365 and Proofpoint with enabled phishing protection plugin, web proxies, endpoint protections and using phishing awareness programs such as Cofense, Wombat and Knowb4. However, the biggest gap here is the protection of your customers from phishing scams impersonating your business login page. In fact, your security team will find out phishing websites only after the attack is launched and a victim has reported it. The other problem is that how can you notify and protect your customers regarding the new phishing websites until it is taken down?

SafeToOpen's PhishingFree browser-based extension is a bridge between businesses and individuals that enables them to work hand in hand to fight phishing attacks.

Businesses can quickly report newly detected phishing websites to PhishingFree extensions installed on Internet browsers. The extension notifies users while visiting reported phishing websites and asks them to close the page.



The PhishingFree extension detects suspicious website with insecure or less secure authentication form and warns users not to trust the website. Once reported, PhishingFree will analyze the website and notify your security team if the URL was a new phishing website impersonating your business login webpage. The use of extension is free for individual and commercial use.

Contact us for more information: contact@safetoopen.com

https://safetoopen.com | https://phishingfree.com