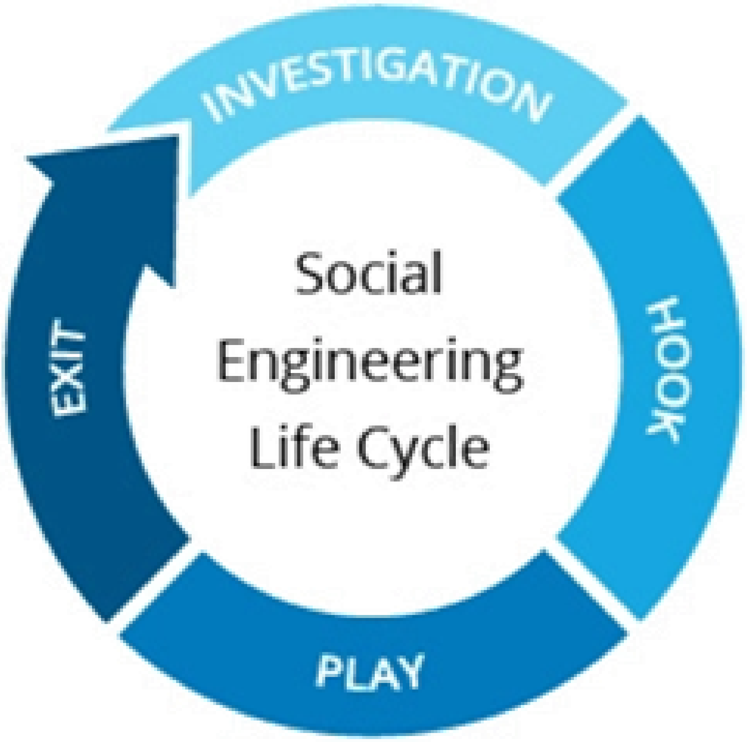
Phishing : diseño y detección de campañas de ingeniería social

1) Preparar el terreno

- Identificar a la víctima
- Recolectar su información
- Seleccionar la técnica

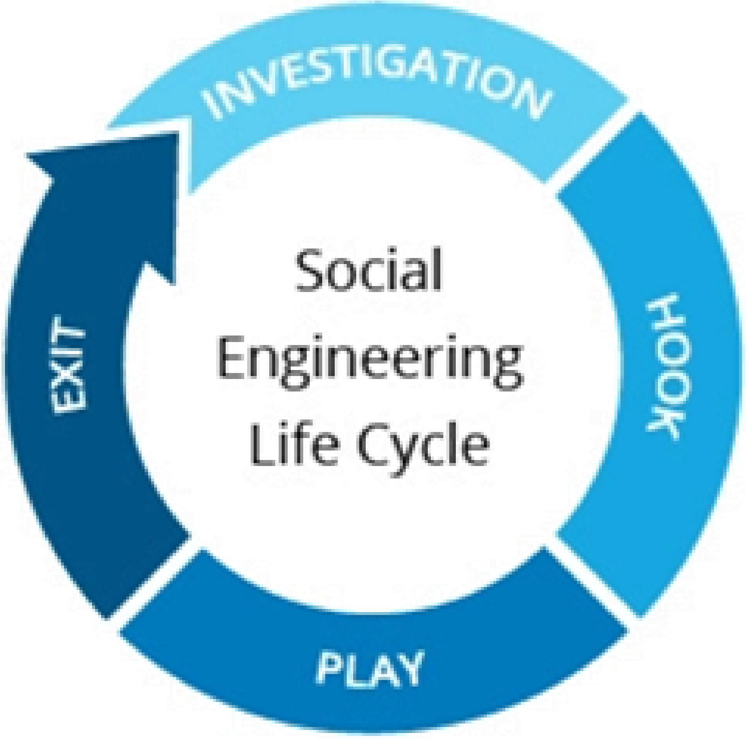


- Enganchar al objetivo
- Hilar la historia
- Tomar el control de la interacción

2) Enganchar a la víctima

4) Cerrar la interacción

- Remover trazas
- Cubrir rastros
- Realizar un cierre natural



- Expandir la confianza
- Ejecutar el ataque
- Recuperar los datos

3) Iniciar el ataque

Phishing attacks:
Defending your organisation

National Cyber Security Centre
a part of GCHQ

A multi-layered approach – such as the one summarised below – can improve your resilience against phishing whilst minimising disruption to user productivity. This approach provides multiple opportunities to detect a phishing attack and stop it before it causes major harm. The mitigations included are also useful against other types of cyber attack.

LAYER 1
Make it difficult for attackers to reach users.

- Implement anti-spoofing controls to stop your email addresses being a resource for attackers.
- Consider what information is available to attackers on your website and social media and help your users do the same
- Filter or block incoming phishing emails.

LAYER 2
Help users identify and report suspected phishing emails.

- Relevant training can help users spot phishing emails, but no amount of training can help them spot every email.
- Help users to recognise fraudulent requests by reviewing processes that could be mimicked and exploited.
- Create an environment that lets users seek help through a clear reporting method, useful feedback and a no-blame culture.

LAYER 3
Protect your organisation from the effects of undetected phishing emails.

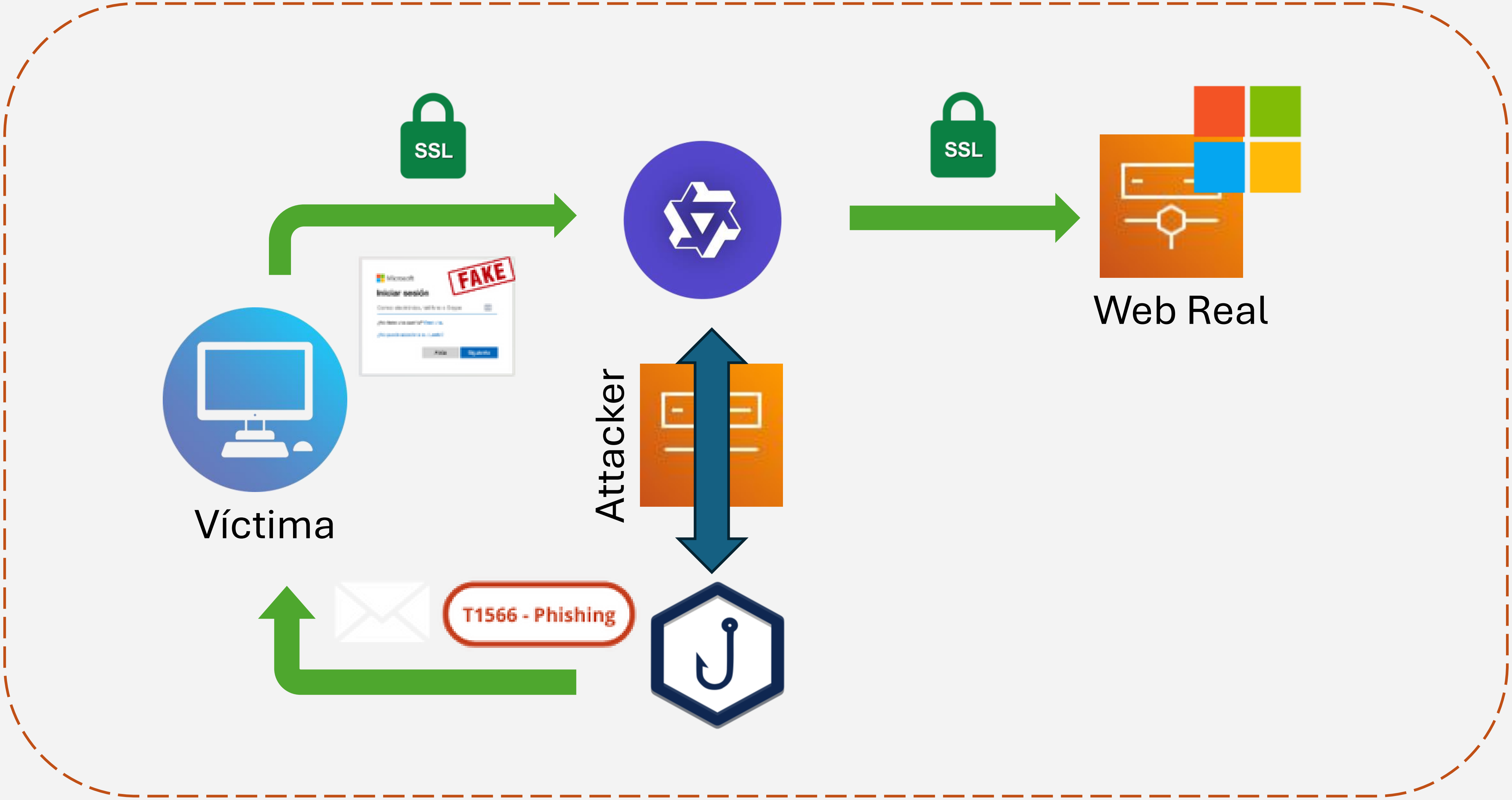
- Protect your accounts: make authentication more resistant to phishing (such as setting up MFA) and ensure authorisation only gives privileges to people who need them.
- Protect users from malicious websites by using a proxy services and an up-to-date browser.
- Protect your devices from malware.

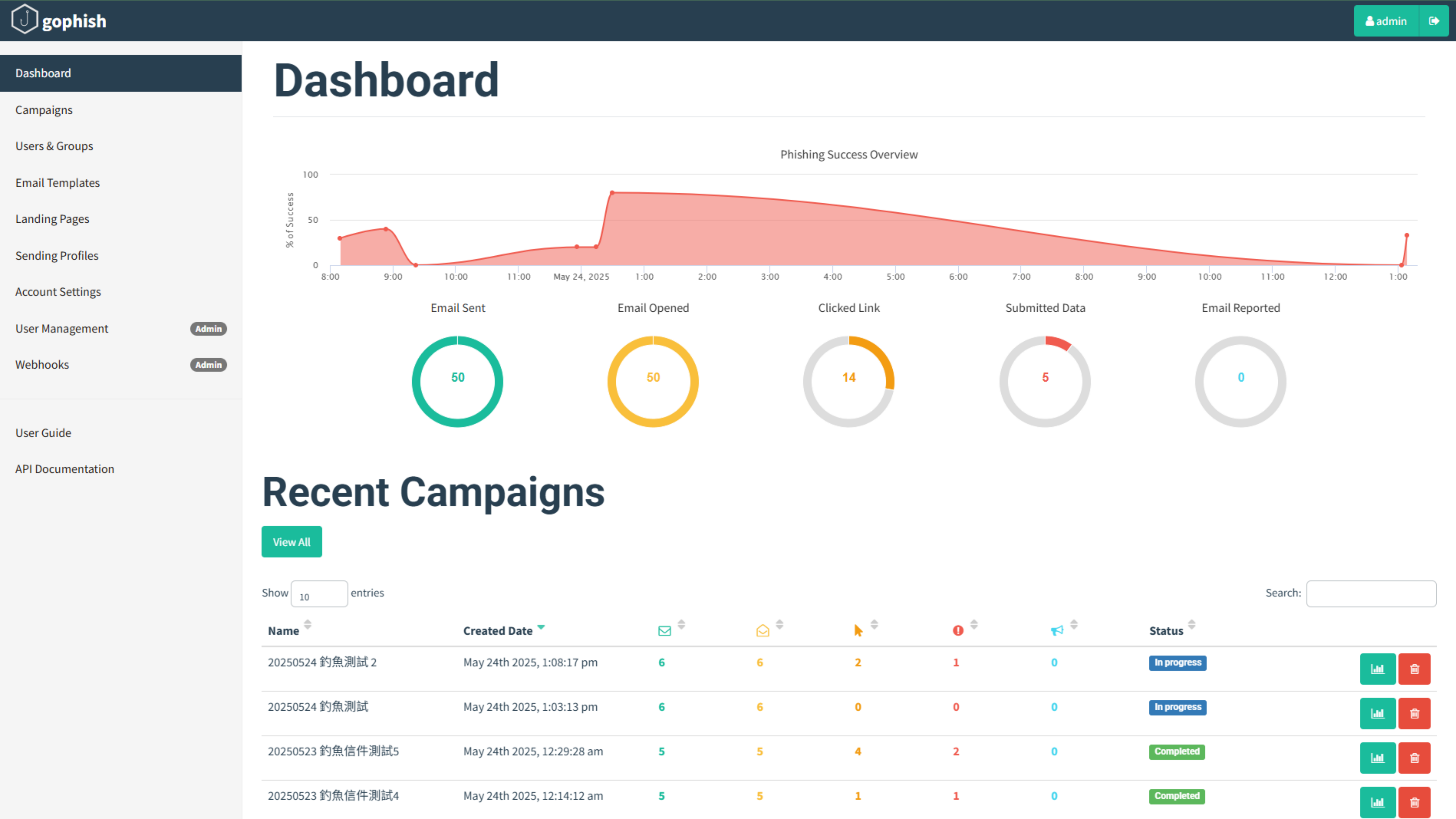
LAYER 4
Respond to incidents quickly.

- Define and rehearse an incident response plan for different types of incidents, including legal and regulatory responsibilities.
- Detect incidents quickly by encouraging users to report any suspicious activity.

NCSC.GOV.UK @NCSC @CYBERHQ @CYBERHQ National Cyber Security Centre

Laboratorio & Herramientas


SSL
SSL
Microsoft
Iniciar sesión
FAKE
Correo electrónico, teléfono o Skype
¿No tiene una cuenta? Cree una.
¿No puede acceder a su cuenta?
Atrás
Siguiente
Web Real
Víctima
Attacker
T1566 - Phishing

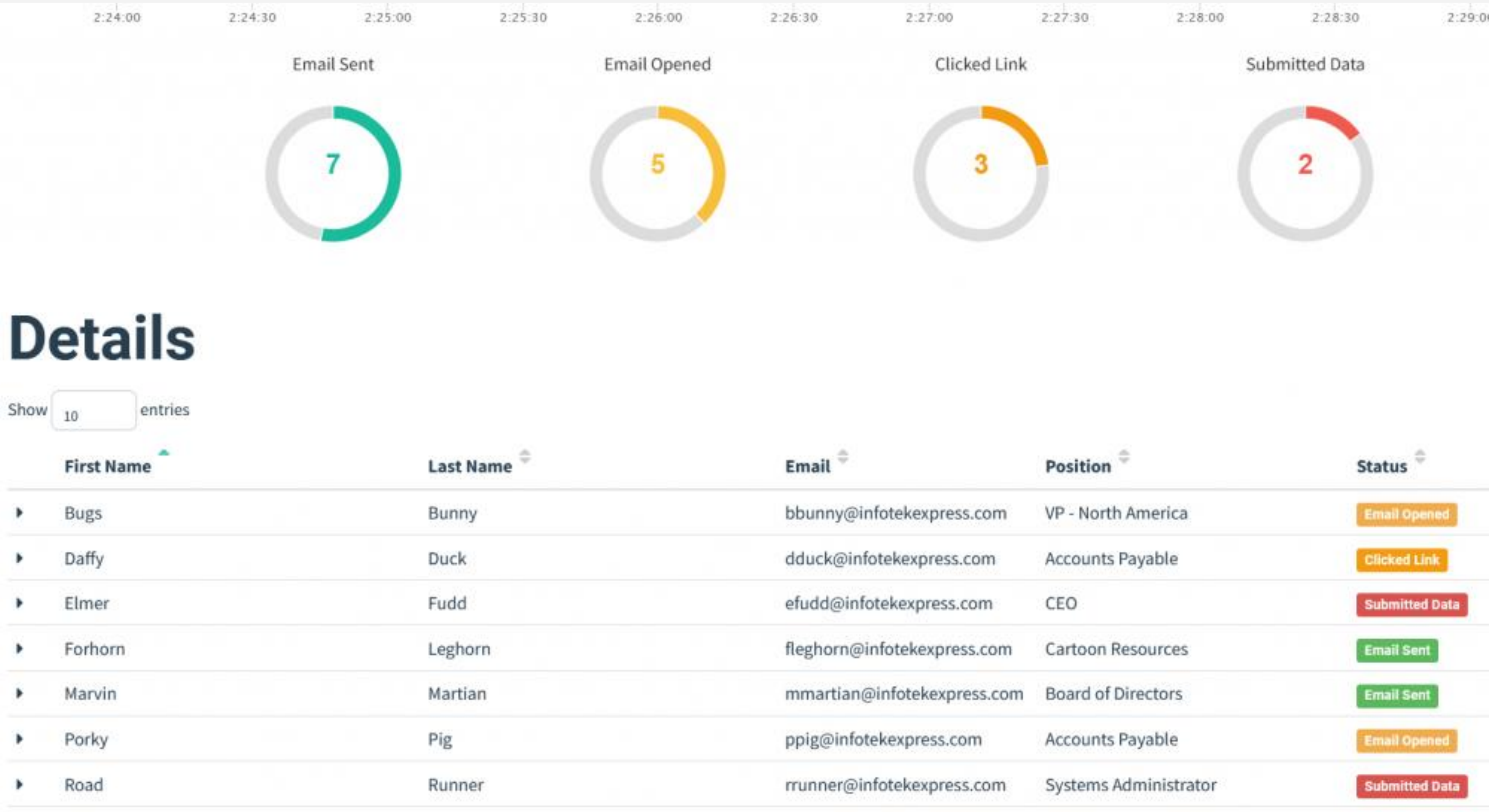


Dashboard

Email Sent	Email Opened	Clicked Link	Submitted Data	Email Reported
50	50	14	5	0

Recent Campaigns

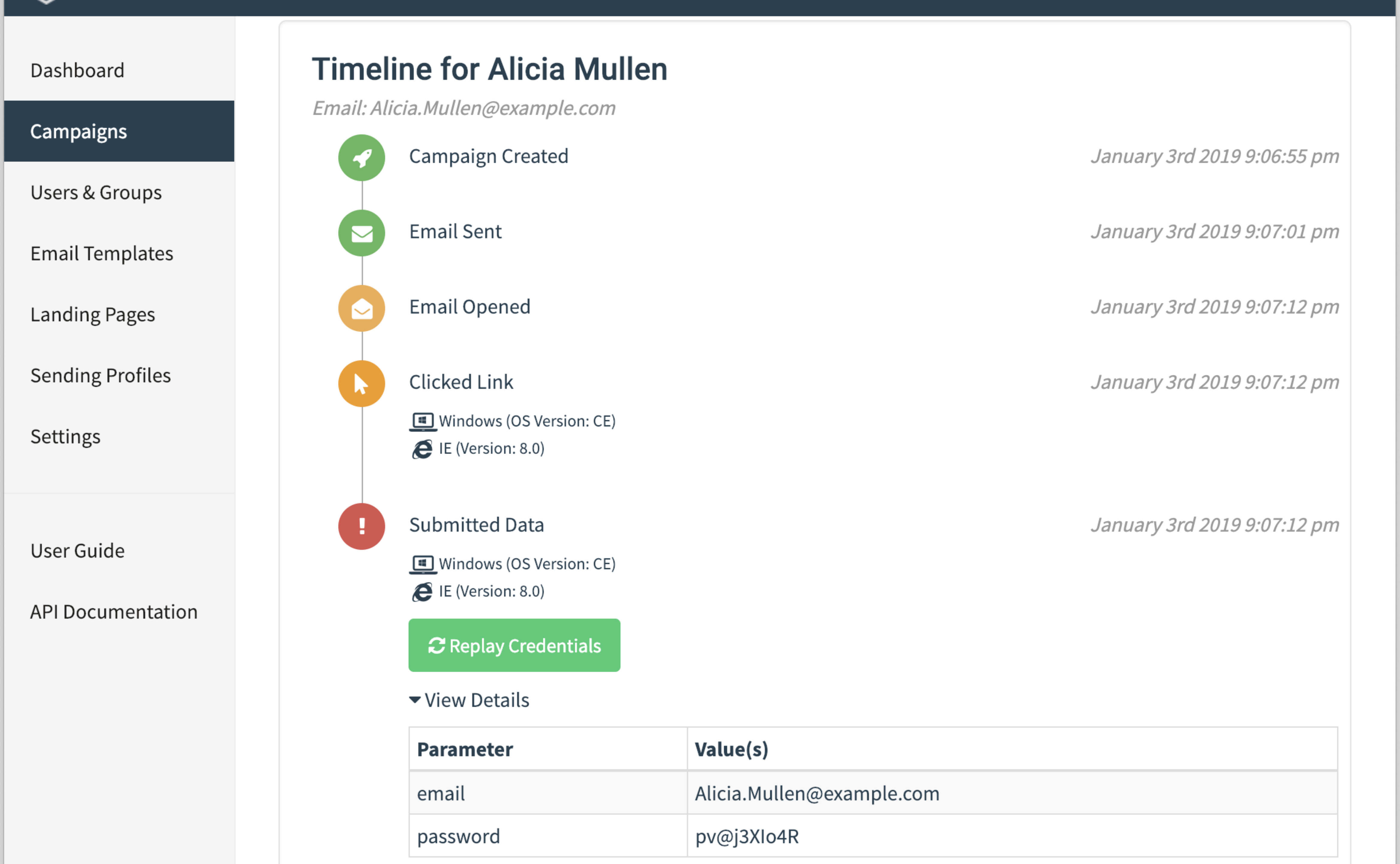
Name	Created Date	✉	✉	➤	!	📢	Status
20250524 釣魚測試 2	May 24th 2025, 1:08:17 pm	6	6	2	1	0	In progress
20250524 釣魚測試	May 24th 2025, 1:03:13 pm	6	6	0	0	0	In progress
20250523 釣魚信件測試5	May 24th 2025, 12:29:28 am	5	5	4	2	0	Completed
20250523 釣魚信件測試4	May 24th 2025, 12:14:12 am	5	5	1	1	0	Completed



Details

Show 10 entries

	First Name	Last Name	Email	Position	Status
▸	Bugs	Bunny	bbunny@infotekexpress.com	VP - North America	Email Opened
▸	Daffy	Duck	dduck@infotekexpress.com	Accounts Payable	Clicked Link
▸	Elmer	Fudd	efudd@infotekexpress.com	CEO	Submitted Data
▸	Forhorn	Leghorn	fleghorn@infotekexpress.com	Cartoon Resources	Email Sent
▸	Marvin	Martian	mmartian@infotekexpress.com	Board of Directors	Email Sent
▸	Porky	Pig	ppig@infotekexpress.com	Accounts Payable	Email Opened
▸	Road	Runner	rrunner@infotekexpress.com	Systems Administrator	Submitted Data



Timeline for Alicia Mullen

Email: Alicia.Mullen@example.com

Campaign Created *January 3rd 2019 9:06:55 pm*

Email Sent *January 3rd 2019 9:07:01 pm*

Email Opened *January 3rd 2019 9:07:12 pm*

Clicked Link *January 3rd 2019 9:07:12 pm*

Windows (OS Version: CE)
IE (Version: 8.0)

Submitted Data *January 3rd 2019 9:07:12 pm*

Windows (OS Version: CE)
IE (Version: 8.0)

Parameter	Value(s)
email	Alicia.Mullen@example.com
password	pv@j3XIo4R

Recomendaciones para remediación o prevención

- Hacer difícil que los correos electrónicos de sus dominios sean falsificados empleando DMARC, SPF y DKIM
-Capacitar a los usuarios, especialmente en forma de simulaciones de phishing
- Crear una cultura en la que los usuarios puedan denunciar correos electrónicos de phishing
- Evitar que los atacantes aprovechen vulnerabilidades conocidas utilizando únicamente software y dispositivos compatibles.