Università degli studi di Camerino

SCUOLA DI SCIENZE E TECNOLOGIE

Corso di Laurea in Informatica (Classe L-31)

Analisi di alcuni tra i Phishing Tool più conosciuti e come le aziende possono difendersi da essi

Laureando
Stefano Sammarco

Relatore
Fausto Marcantoni

Indice

1. Introduzione

Fra le diverse tipologie di attacchi informatici, ne esiste una chiamata Phishing. Con questa particolare tipologia di attacchi, l'obiettivo principale è quello di indurre le persone a condividere informazioni sensibili, trasferire somme di denaro, ed altro ancora. Gli attacchi pshishing sono, quindi, solitamente mascherati da interazioni innocue che portano la vittima a fidarsi.

1.1 Tipologie di attacchi phishing

La tipologia di attacchi phishing più conosciuta sono le *e-mail* di phishing, con cui un'utente apparentemente legittimo, cerca di indurre il destinatario a cliccare su un link malevolo o a scaricare un file infetto.

Altra tipologia sono gli *SMS* di phishing, dove in sostanza gli aggressori cercano di indurre la vittima a fornire informazioni personali, come ad esempio i dati delle carte di credito, attraverso degli SMS che sembrano provenire magari dal proprio istituto bancario.

Ulteriore tipologia sono i *Voice* phishing, che hanno sostanzialmente lo stesso scopo degli SMS, quindi anche in questo caso si cerca di indurre vittima a fornire informazioni personali, come carte di credito. La differenza sostanziale con gli SMS di phishing è che la vittima viene contattata con una chiamata. [2]

1.2 Obiettivo Tesi

Ci sono malintenzionati molto interessati ad ottenere credenziali di accesso per i più disparati servizi online.
Esistono diversi strumenti che facilitano gli attacchi necessari a carpire queste informazioni. L'obiettivo di questa tesi è quello di analizzarne qualcuno, infatti nel secondo capitolo vengono analizzati: SEToolkit, Zphisher, Gophish. Vedremo poi, nel terzo capitolo, come le aziende possono difendersi da questi tipi di attacchi.

2. Phishing tool

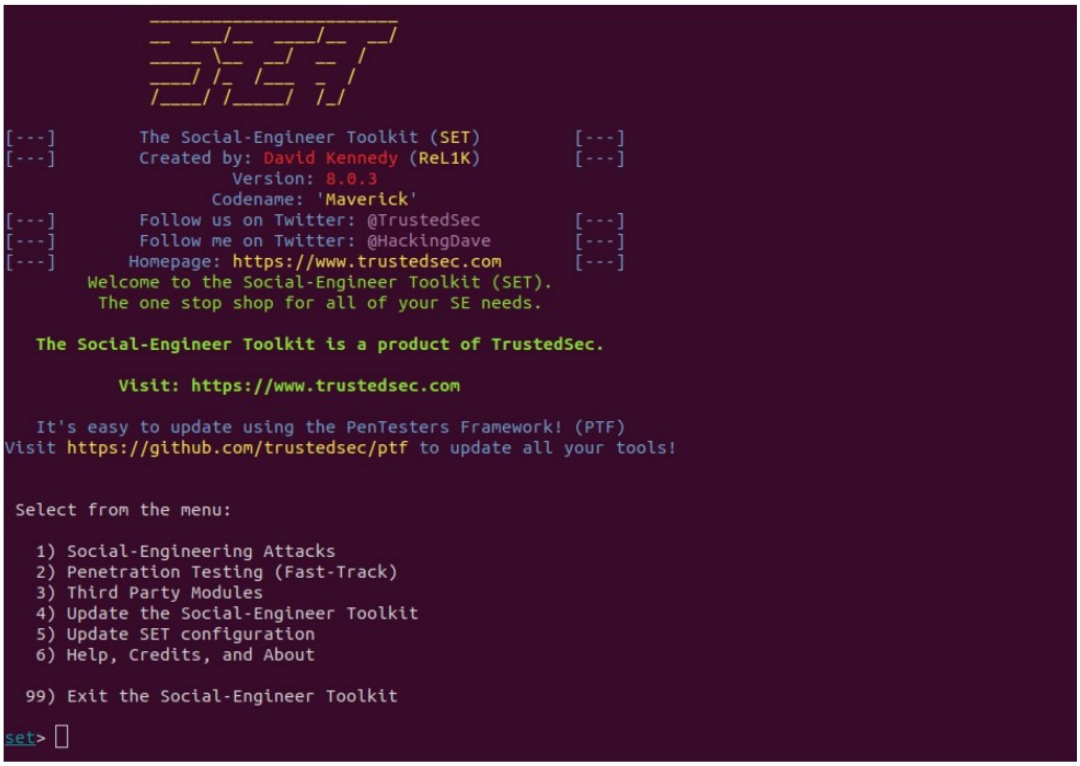
In questo capitolo vengono analizzati alcuni strumenti realizzati e utilizzati dagli "smanettoni" per effettuare attacchi di phishing volti a carpire credenziali di accesso per diversi servizi online.
Ci concentreremo su tre tool: SEToolkit, Zphisher, Gophish.

2.1 SEToolkit

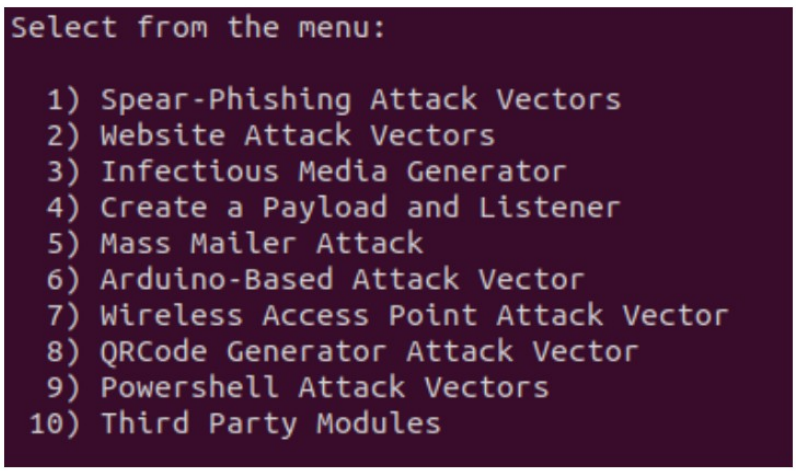
SEToolkit è uno strumento per sistemi Linux, pubblicato nel 2013 da David Kennedy. Offre diverse funzioni, come la possibilità di usare e clonare pagine web per gli attacchi di pshishing, inviare e-mail o SMS da emittenti fasulli, oppure ottenere file all'apparenza innocui, ma che hanno all'interno payload dannosi. Il tool offre inoltre servizi di pentesting. L'analisi si concentrerà esclusivamente sulle funzionalità utili a clonare o utilizzare siti web per il phishing di credenziali di accesso.

Negli anni passati alcuni hacker giovanissimi sono stati perseguiti penalmente per aver eseguito diversi tipi di attacchi e realizzato delle truffe avvalendosi di SEToolkit. [1]

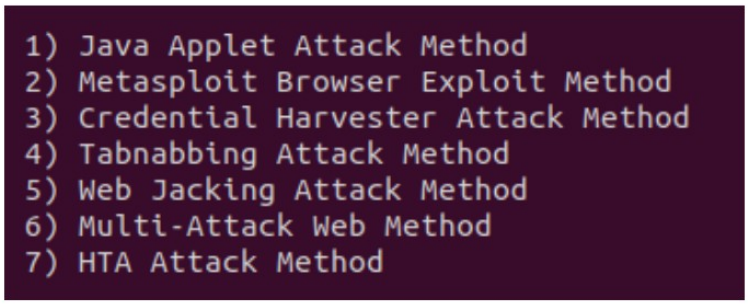
All'avvio lo strumento appare così come si vede nell'immagine seguente. Noi analizzeremo esclusivamente il primo punto del menu, cioè *Social-Engineering Attacks.*



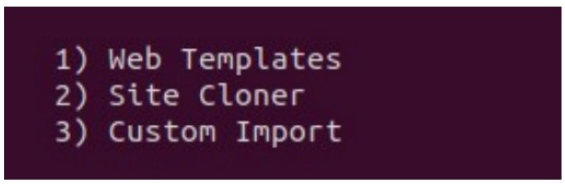
Dopo aver selezionato il primo punto, lo strumento ci mostra un ulteriore menu, visibile nell'immagine successiva; selezioniamo *Website Attack Vectors*.



Proseguiamo ancora selezionando *Credential Harvester Attack Method*.

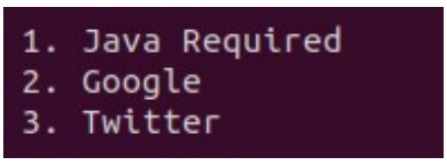


A questo punto lo strumento permette di sfruttare tre particolari funzionalità. La prima ci permette di utilizzare web templates già inclusi in SEToolkit, la seconda ci consente di clonare e utilizzare qualsiasi sito web dando "in pasto" allo strumento un URL. La terza ed ultima opzione permette di utilizzare un file HTML presente sulla macchina su cui è in esecuzione il tool.

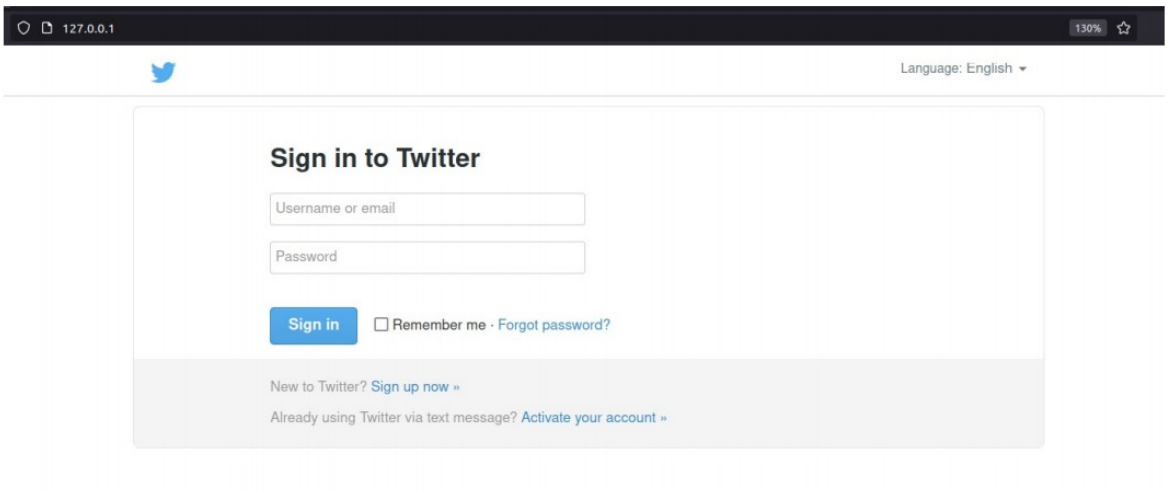


2.1.1 Phishing con web templates già inclusi in SEToolkit

Selezioniamo la prima opzione tra le tre visibili nell'immagine precedente, cioè *Web Templates*. Il tool, subito dopo, ci chiederà di digitare l'indirizzo IP su cui vogliamo ospitare la pagina web, inseriamo l'indirizzo di Localhost, `127.0.0.1` .
Infine SEToolkit ci propone tre diversi web templates, che possono essere scelti in base alle necessità. Scegliamo l'opzione tre, Twitter.



Utilizzando un qualsiasi browser, abbiamo modo di vedere la pagina di login di Twitter. Su nostra macchina basta utilizzare indirizzo di localhost, mentre gli altri dispositivi connessi alla stessa rete locale, potranno visualizzare la pagina attraverso l'indirizzo IP della macchina su cui è in esecuzione la pagina web.



Con l'utilizzo di servizi terzi, è possibile poi rendere disponibile su rete internet globale, ciò che è in esecuzione su localhost.
Si tratta meglio questo aspetto nel prossimo paragrafo dedicato Zphsher.

La vittima, convinta che si tratti della pagina originale per il Login su Twitter, inserirà i suoi dati. Questi dati però finiranno nelle mani dell'attaccante, e la vittima verrà poi reindirizzata su vera pagina Twitter.

Sul terminale vengono mostrati i dati catturati, scritti in rosso. Abbiamo username *"0ste1"* e password *"ciaociao"* .
Si può premere CTRL + C per generare un report con i dati ottenuti.

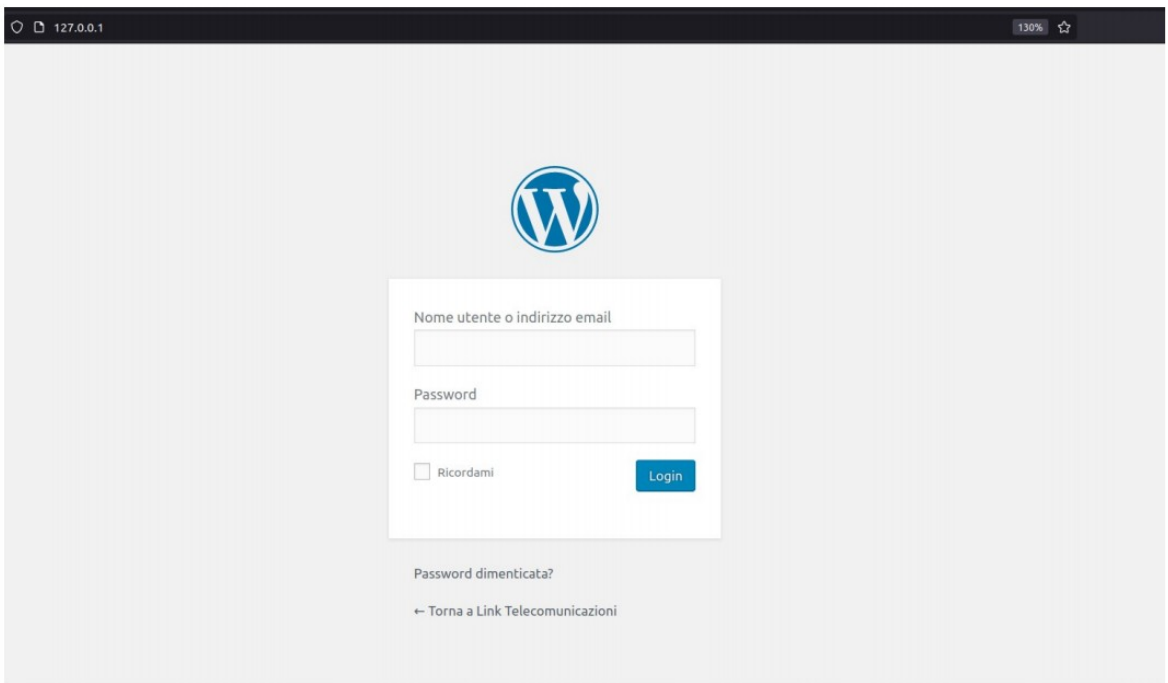
```
[*] Information will be displayed to you as it arrives below:
127.0.0.1 - - [18/Dec/2022 17:00:33] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [18/Dec/2022 17:00:33] "GET /opensearch.xml HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=0ste1
POSSIBLE PASSWORD FIELD FOUND: session[password]=ciaociao
```

Il terminale mostrerà poi il percorso in cui è stato memorizzato il report richiesto. Il report in questione conterrà i medesimi dati mostrati su terminale.

2.1.2 Clonare e utilizzare qualsiasi sito web

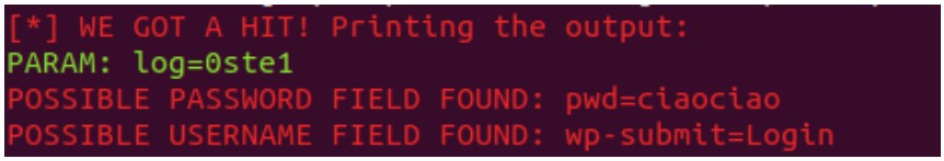
Selezioniamo la seconda opzione tra le tre visibili nel menu a pagina 5, cioè *Site Cloner*. Il tool, subito dopo, ci chiederà di digitare l'indirizzo IP su cui vogliamo ospitare la pagina web, inseriamo anche in questo caso l'indirizzo di localhost, **127.0.0.1** . Lo strumento ci chiede infine di digitare l'URL del sito web che vogliamo clonare.
Decidiamo di clonare la pagina che gli amministratori di un sito web, realizzato con Wordpress, utilizzano per autenticarsi.

Come prima, con un qualsiasi browser, abbiamo modo di visualizzare la pagina web che in questo caso abbiamo clonato.

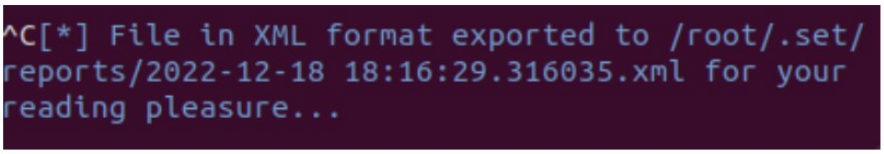


Anche in questo caso la vittima, convinta che questa sia la pagina originale di Login, inserirà i suoi dati. Questi dati finiranno poi nelle mani dell'attaccante, e la vittima verrà reindirizzata su vera pagina di Login.

Sul terminale otteniamo i dati inseriti dall'utente. In questo caso l'username è scritto in verde, cioè l'username è *"0ste1"* . La password viene mostrata nella prima riga scritta in rosso, ed essa è *"ciaociao".*



L'attaccante quando ha terminato, e quindi quando è a conoscenza di aver ottenuto i dati necessari, può premere contemporaneamente i tasti CTRL + C della tastiera, per generare un report con i dati già mostrati su terminale. Il terminale mostrerà quindi il percorso in cui è stato memorizzato il report richiesto.



2.2 Zphisher

Zphisher è un ulteriore strumento per il phishing. Al suo interno sono inclusi 35 templates di pagine web login che possono essere facilmente utilizzate per ingannare una potenziale vittima.
Lo strumento in questione ha una particolarità, cioè al suo interno troviamo integrate molteplici servizi di tunneling. Cioè, lo strumento rende possibile in modo facile e veloce la visualizzazione della pagina web con finto login anche al di fuori di una rete locale. La pagina web, quindi, diventa visibile da ogni dispositivo connesso alla rete Internet.

All'avvio lo strumento appare come visibile nell'immagine seguente:

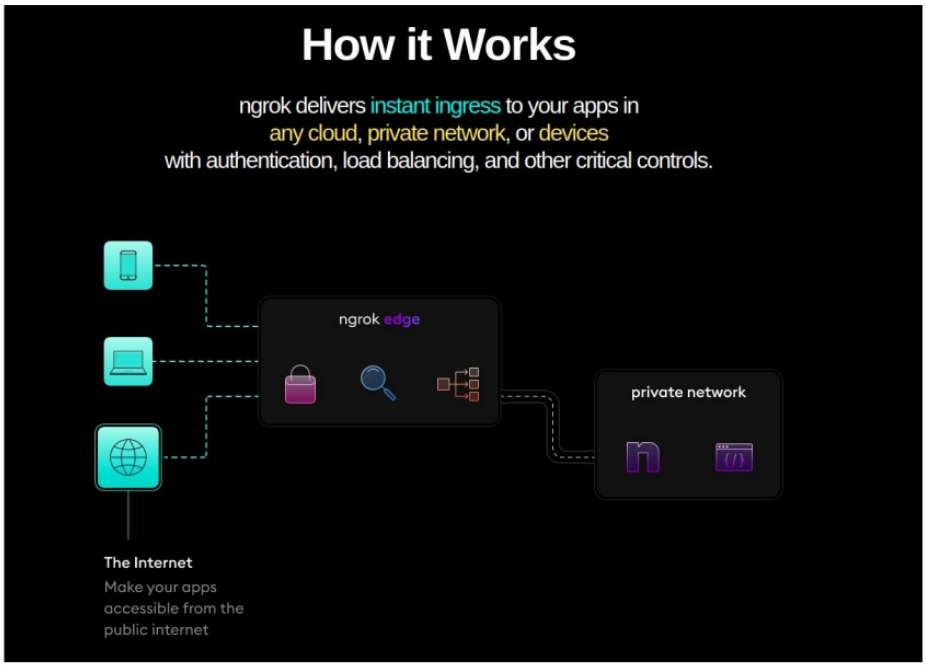
I template offerti sono molti. Selezioniamo numero 18, Spotify.

Dopo aver selezionato il template desiderato, lo strumento ci chiede in che modo vogliamo rendere disponibile la pagina di login scelta.

La prima opzione ci consente, come per gli altri strumenti analizzati, di rendere disponibile la pagina di login, all'interno di una rete locale.

Le restanti opzioni sono decisamente più interessanti, infatti ci viene data la possibilità di rendere visibile la nostra pagina sulla rete internet globale, in modo comodo e veloce. Questo è possibile grazie a tre servizi che troviamo già inclusi in Zphisher, che sono: Ngrok, Cloudflared, LocalXpose.

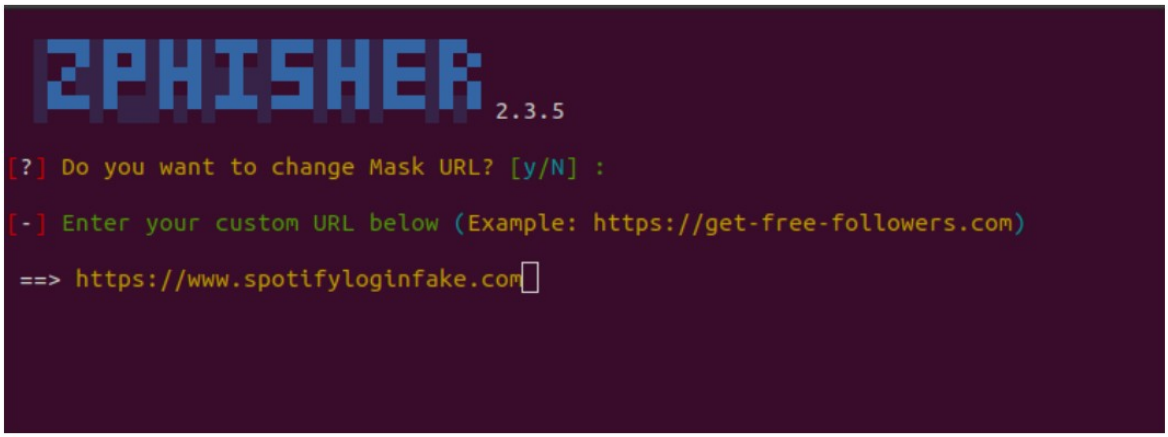
I tre servizi in questione funzionano in maniera simile, e consentono sostanzialmente di rendere visibile su rete internet globale ciò che è in esecuzione su localhost della nostra macchina. Nell'immagine seguente è mostrato, in breve, il funzionamento generale di questa tipologia di servizi.



A destra è rappresentata la rete locale a cui è connessa la macchina su cui è in esecuzione la pagina web fasulla, al centro il servizio che rende visibile su rete internet globale la nostra pagina web, e infine a sinistra, appunto, i dispositivi collegati alla rete internet globale che possono visualizzare la pagina web in esecuzione su nostra macchina.

Decidiamo, quindi, di rendere visibile su rete internet la pagina di login fasulla che abbiamo scelto in precedenza. Scegliamo l'opzione più comoda, cioè la numero `03`, Cloudflared. Infatti, questo servizio, a differenza degli altri due, non richiede registrazione account.

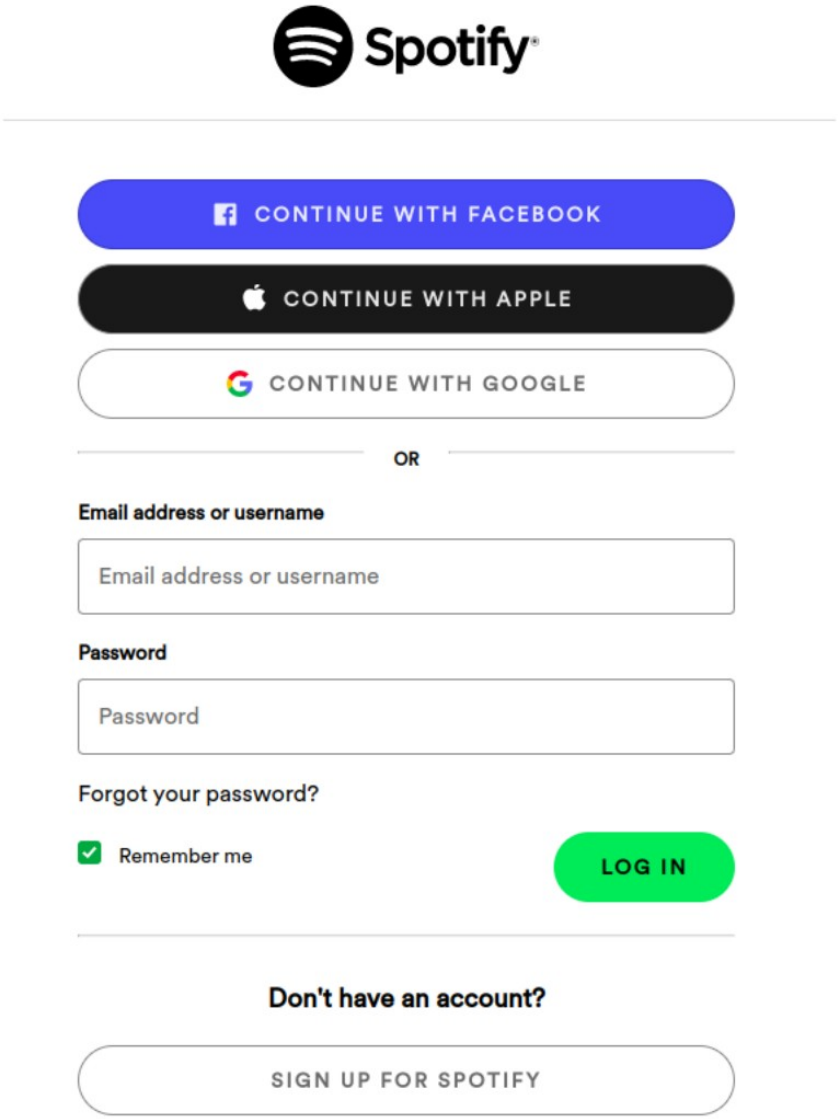
Dopo aver selezionato l'opzione desiderata, il servizio ci offre la possibilità di inserire un URL da usare poi per raggiungere la pagina. Decidiamo di usare un URL pensato sul momento, cioè www.spotifyloginfake.com



Zphisher, con il supporto del servizio di tunneling scelto (Cloudflared), mostra dei link che è possibile usare per raggiungere la pagina web con il falso login.

Cliccando su uno qualsiasi dei tre link generati, abbiamo modo di visualizzare la pagina con finto login.

Ecco la pagina di login scelta prima, Spotify.



La potenziale vittima può essere convinta a cliccare su uno dei tre link visti, magari attraverso l'utilizzo di e-mail in cui si chiede di ripristinare i dati di accesso per evitare blocco account. Quindi, dopo aver cliccato su uno dei tre link visti prima, la vittima si ritroverà sulla pagina mostrata nell'immagine precedente.
Se si inseriscono dei dati nei campi email e password, questi vengono immediatamente visualizzati su terminale dell'attaccante.

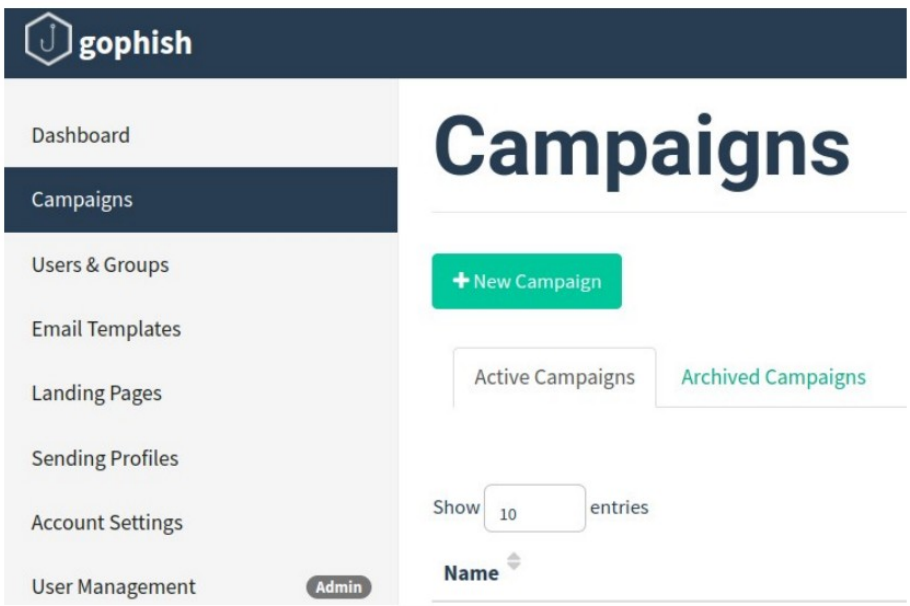
In questo caso la vittima ha indirizzo IP **5.171.244.122** , il suo username è *stefano.sammarco* e la password è *provapasswordprova .*

2.3 GoPhish

Gophish è uno strumento di phishing open source.
Permette di configurare ed eseguire, in modo rapido e semplice, attività di phishing. È disponibile per sistemi operativi Windows, Mac e Linux. Analizzeremo il tool in questione mostrando come si crea una campagna di pshishing, e come si può tenere d'occhio l'andamento di essa.

2.3.1 Creare nuova campagna phishing

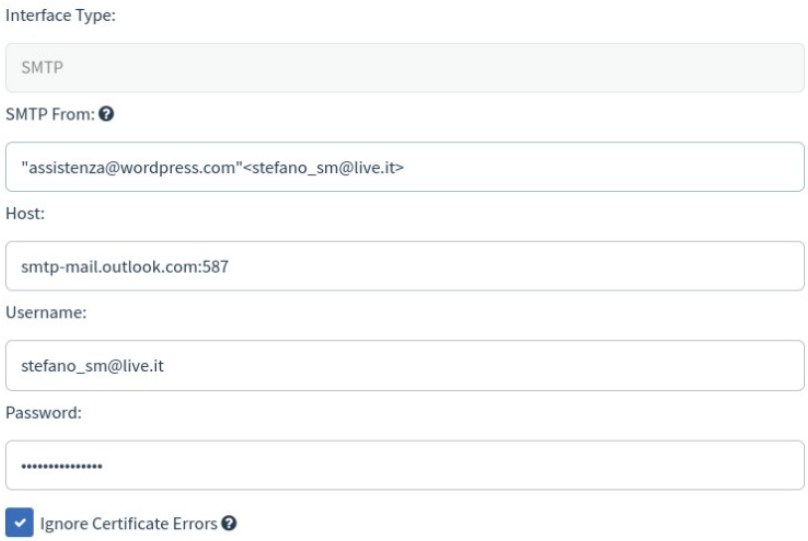
Creiamo una nuova campagna di phishing cliccando su *Campaigns* nel menu a sinistra, e poi su *New Campaign*.



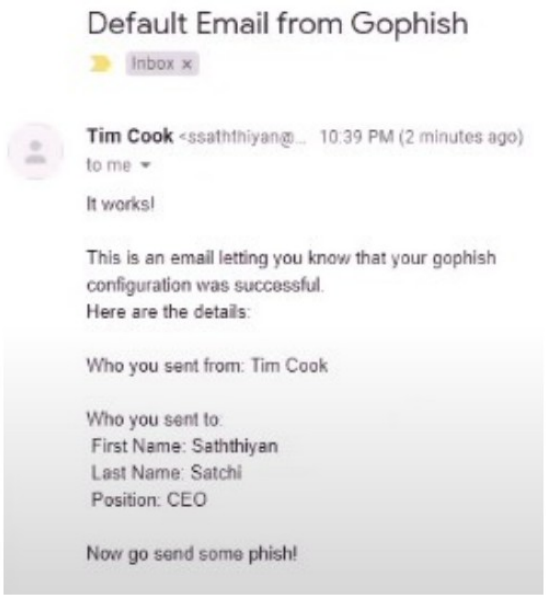
Prima di poter creare campagne phishing è fondamentale, però, impostare un *Sending Profiles*, cioè configurare un profilo con cui inviare le email. Importante, poi, definire un gruppo di utenti verso la quale si vuole indirizzare l'attacco.

Impostiamo quindi un nuovo profilo.
Per la configurazione del profilo è necessario indicare l'indirizzo del server SMTP; nell'esempio usiamo *outlook*. Serve poi indicare indirizzo e-mail e relativa password per l'invio delle email di pshishing.

Per aumentare le probabilità di una buona riuscita dell'attacco, è importante specificare all'interno del campo *SMTP From,* un nome o un indirizzo e-mail fasullo. In questo caso abbiamo inserito l'indirizzo "assistenza@wordpress.com", seguito poi dal nostro indirizzo reale.
La potenziale vittima, quando aprirà l'email vedrà in primo piano l'indirizzo wordpress, e ciò farà risultare l'email più credibile, aumentando le possibilità che la vittima caschi nel tranello.

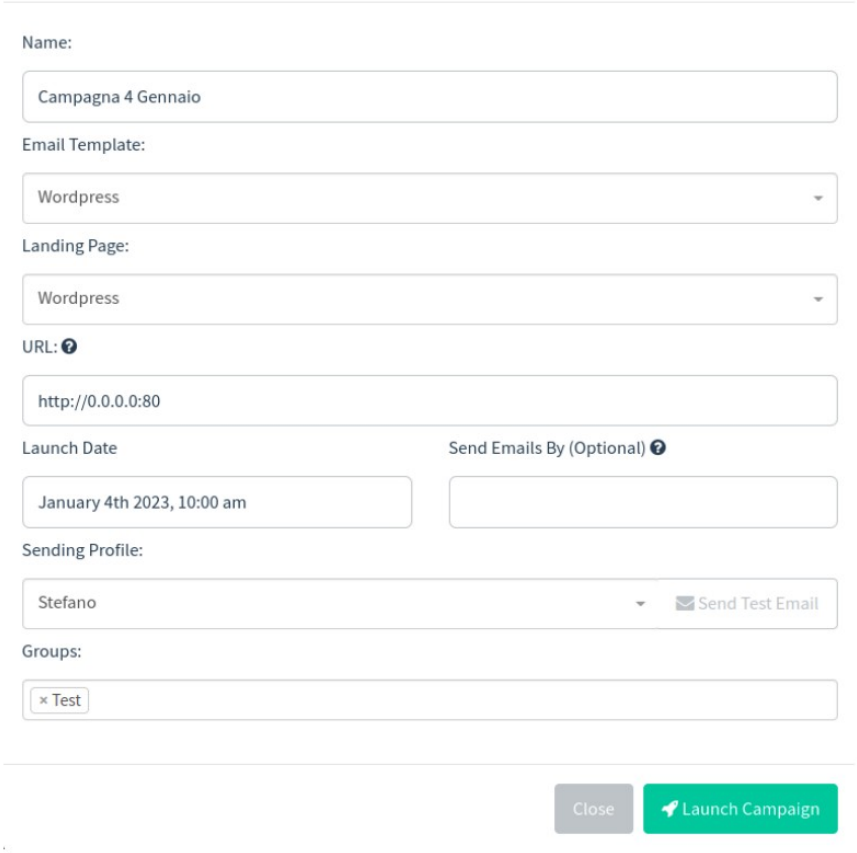


Nell'immagine successiva è presente un esempio di come la potenziale vittima visualizza l'email mandata dall'attaccante. Si può notare come il nome impostato dall'attaccante sia "Tim Cook", ed è proprio questo che spesso inganna la vittima. Il nome fasullo "Tim Cook" è seguito dal reale indirizzo e-mail del mittente.



Altra cosa importante, prima di avviare una nuova campagna, è la configurazione del gruppo di utenti verso la quale si vuole indirizzare l'attacco. Cliccando su *Users&Groups* presente nel menu a sinistra come prima e poi su *New Group* è possibile configurare un gruppo di utenti con relativi indirizzi e-mail. Durante la configurazione di una nuova campagna, sarà poi possibile selezionare i gruppi creati.

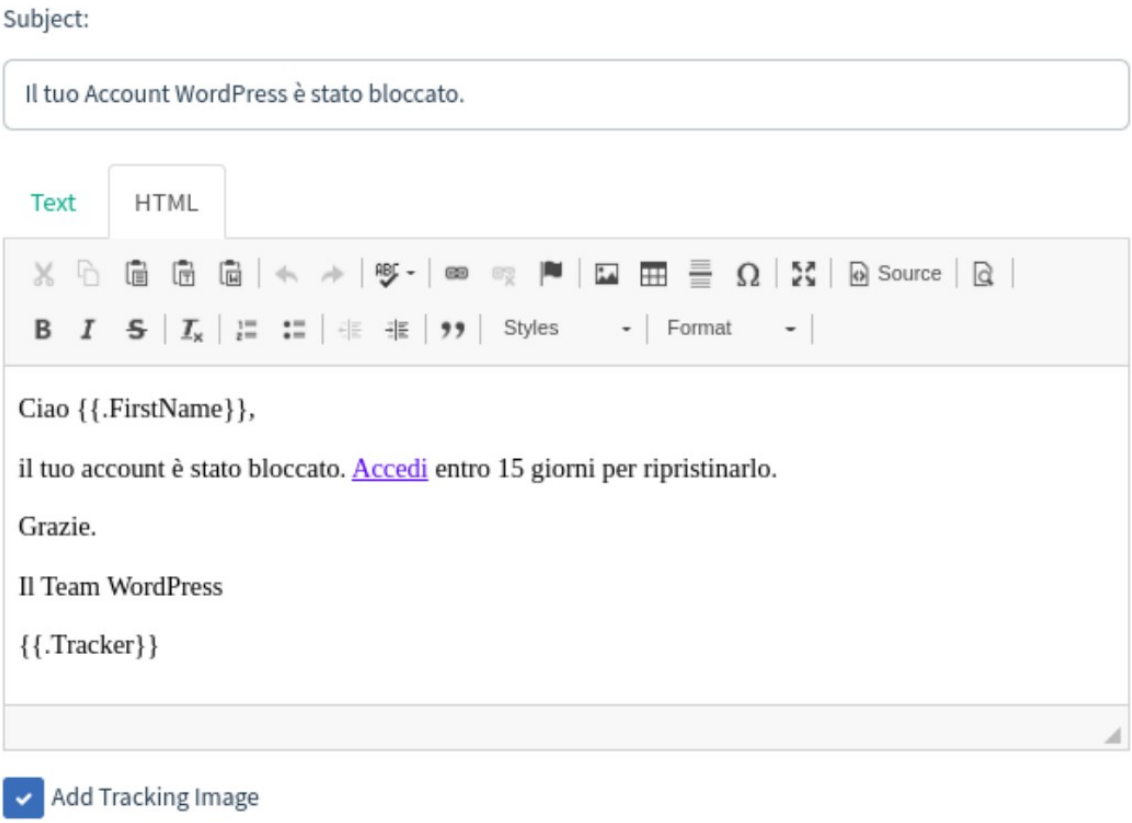
Creiamo quindi una nuova campagna.
È necessario selezionare un Email Template già creato (vedi **2.3.1.1**) , una Landing Page già realizzata (vedi **2.3.1.2**), l'indirizzo IP su cui viene ospitata la landing page fasulla, la data nella quale si vuole far partire la campagna, il sending profile, e infine il gruppo di utenti verso cui eseguire l'attacco.
Infine, si lancia la campagna cliccando sul pulsante *Launch Campaign*.
Nell'immagine seguente si può vedere l'interfaccia grafica in cui inserire i dati in questione.



2.3.1.1 Realizzare un Email Template

Per aumentare le probabilità di una buona riuscita dell'attacco, realizzare una e-mail credibile è un qualcosa di fondamentale.

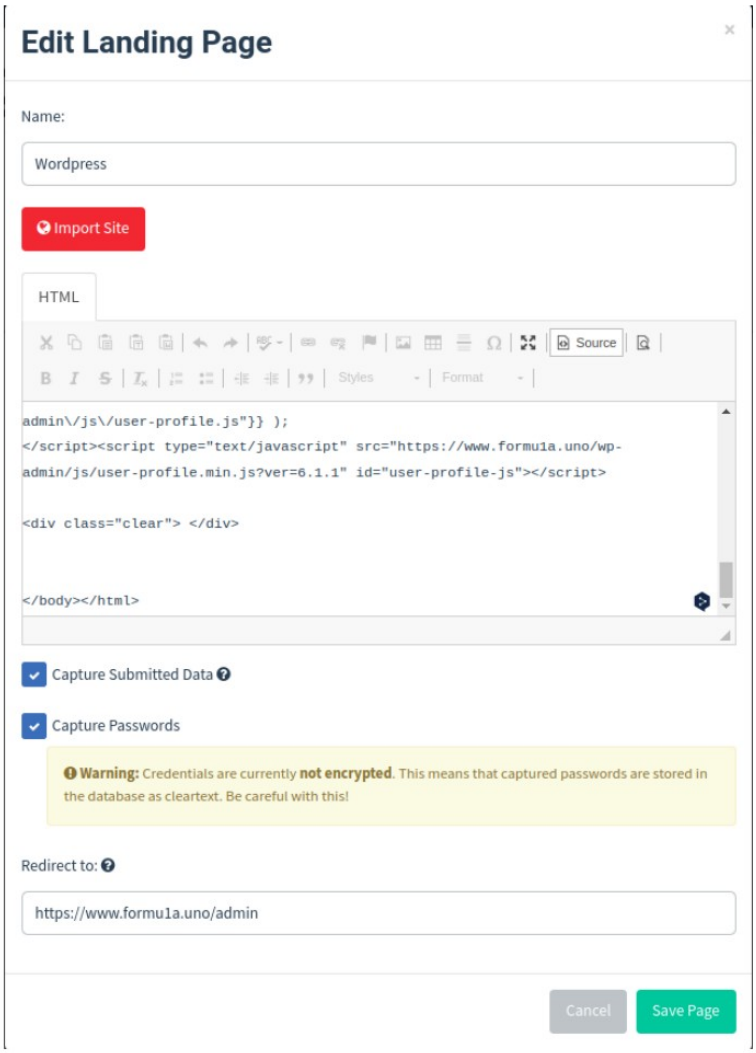
Per realizzare un Email Template, si clicca su Email Templates nel menu a sinistra, poi su *New Template.*
Nell'interfaccia grafica che compare e che si può vedere nell'immagine successiva, si inserisce l'oggetto della e-mail, poi si scrive il contenuto della e-mail. Nell'esempio alla parola "Accedi" è stato creato un collegamento alla "pagina trappola".
Al posto di {{.FirstName}} verrà posizionato automaticamente il nome della potenziale vittima a cui si invia.



2.3.1.2 Realizzare una Landing Page

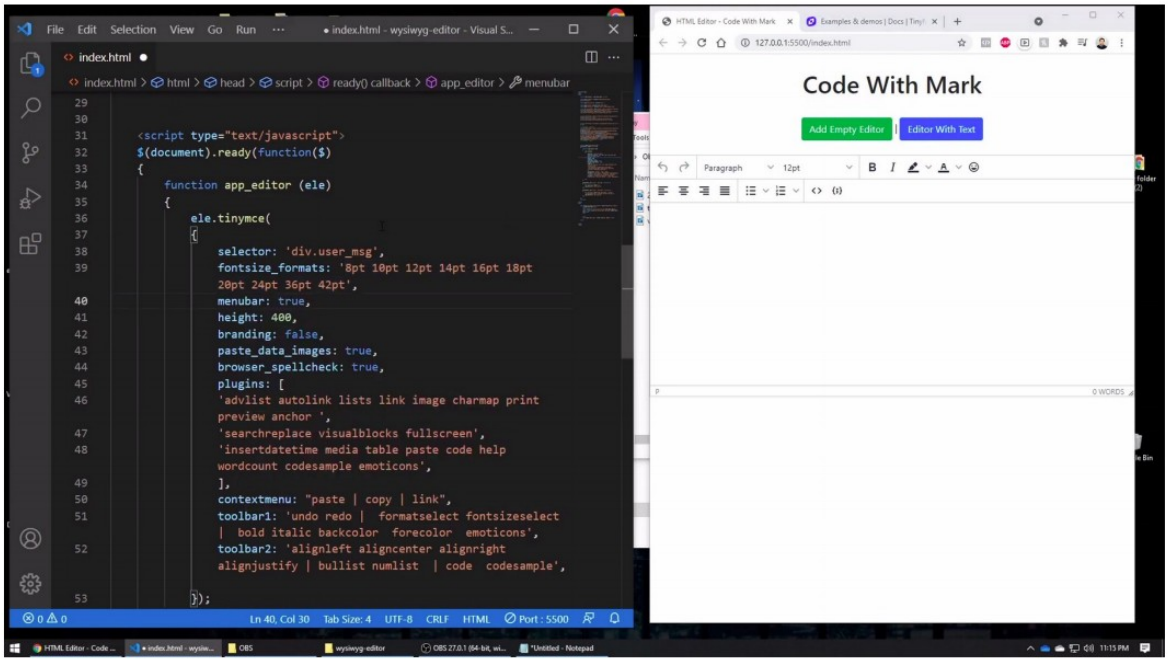
La landing page, insieme alla e-mail, è un'altra cosa importantissima in questo tipo ti attacchi. Se essa è ben realizzata, allora aumentano le probabilità di una buona riuscita dell'attacco.

Si clicca su *Landing Pages*, nel menu a sinistra, poi su *New Page*. Nell'immagine successiva si può vedere l'interfaccia grafica che ci aiuta a configurare il tutto.



Abbiamo la possibilità di clonare un sito web, indicando semplicemente l'URL. Oppure possiamo inserire del codice HTML, realizzato magari avvalendosi di wysiwyg HTML Editor. Cioè strumenti che ci consentono di creare o modificare del codice HTML esistente, contemporaneamente alla visualizzazione della pagina web.

Nell'immagine seguente è mostrato come si può lavorare con questi strumenti.



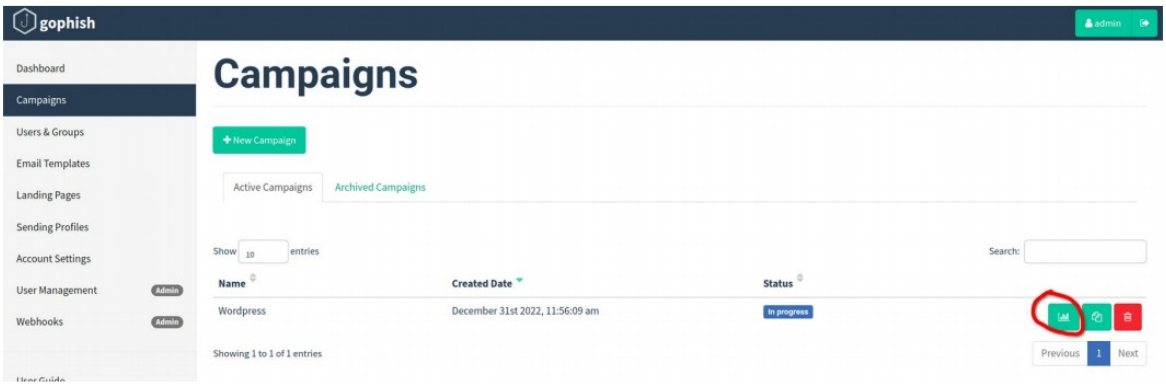
Sulla sinistra è aperto l'editor in cui si scrive il codice. A destra è invece presente il browser con il sito web avviato. Le modifiche al codice vengono mostrate in tempo reale.
Avvalendosi di questo tipo di editor, si riesce più agilmente a realizzare pagine web utili ad ingannare gli utenti e così li si convince ad inserire i propri dati.

In questo caso, però, abbiamo deciso di sfruttare la funzione integrata in Gophish, che permette di clonare pagina web semplicemente inserendo l'URL. Abbiamo deciso di importare la pagina di autenticazione di un sito realizzato con WordPress.

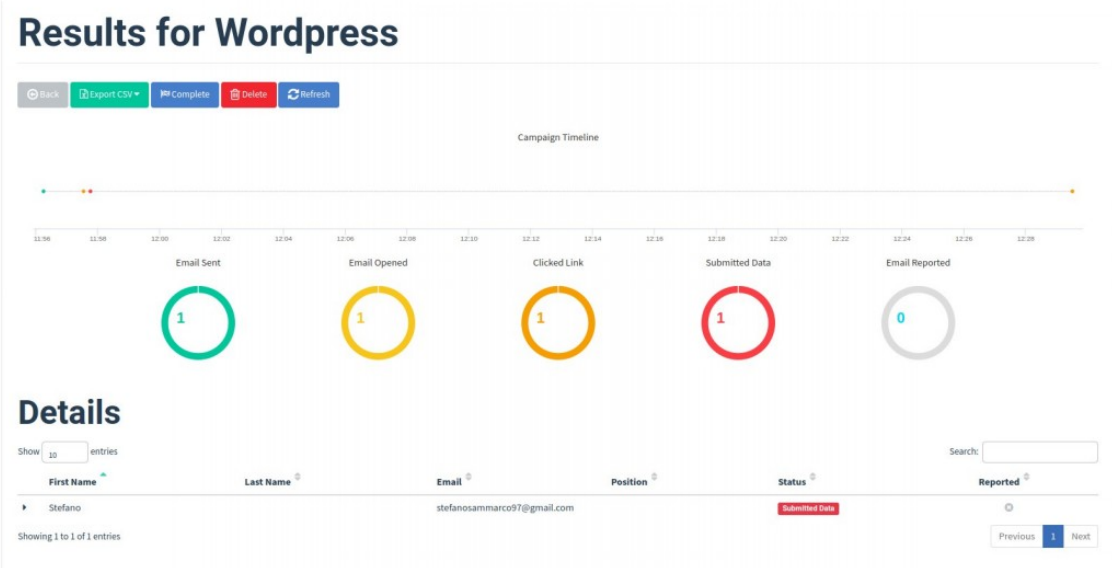
Per concludere la procedura di creazione di una Landing Page, spuntiamo infine le due caselle visibili nella grafica a pagina 20, che ci permettono di carpire le informazioni della vittima, e salviamo.

2.3.2 Visualizzare andamento campagna phishing

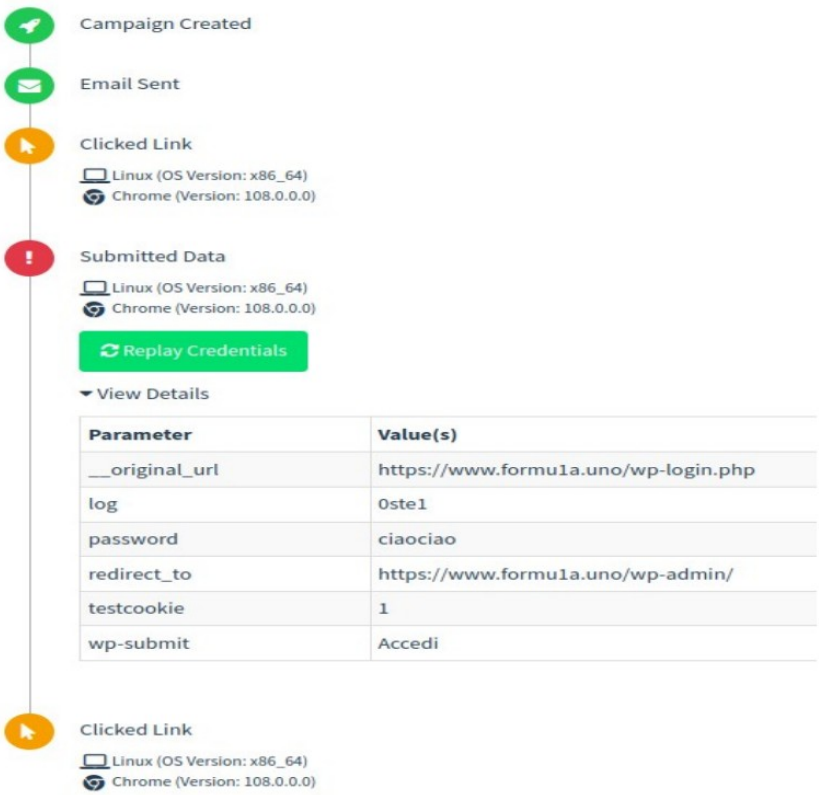
Dopo aver lanciato una campagna phishing è possibile conoscere il suo andamento in tempo reale. Per visualizzare le campagna attive o concluse in passato, si clicca su *Campaigns* sul menu a sinistra. Per visualizzare l'andamento di una specifica campagna, si clicca sul pulsante *View Results*, visibile nell'immagine successiva, evidenziato con un cerchio rosso.



Dopo aver clicca il pulsante in questione, ci ritroviamo davanti ad una schermata come quella visibile nell'immagine successiva.
Possiamo conoscere il numero di e-mail inviate e quante di queste sono state aperte. Inoltre abbiamo modo di capire anche quanti utenti hanno cliccato sul link inserito nella e-mail e quanti di questi hanno inserito dati nella pagina "trappola" raggiungibile dal link fornito.



Nella parte bassa della pagina è inoltre possibile avere informazioni su ogni singolo utente. Se questo ha "abboccato", possiamo vedere i dati da lui inseriti nella pagina fasulla, oltre al sistema operativo e il browser usato.
In questo caso la vittima usava Chrome su Linux, e la password inserita è "ciaociao".



3. Come si difendono le aziende

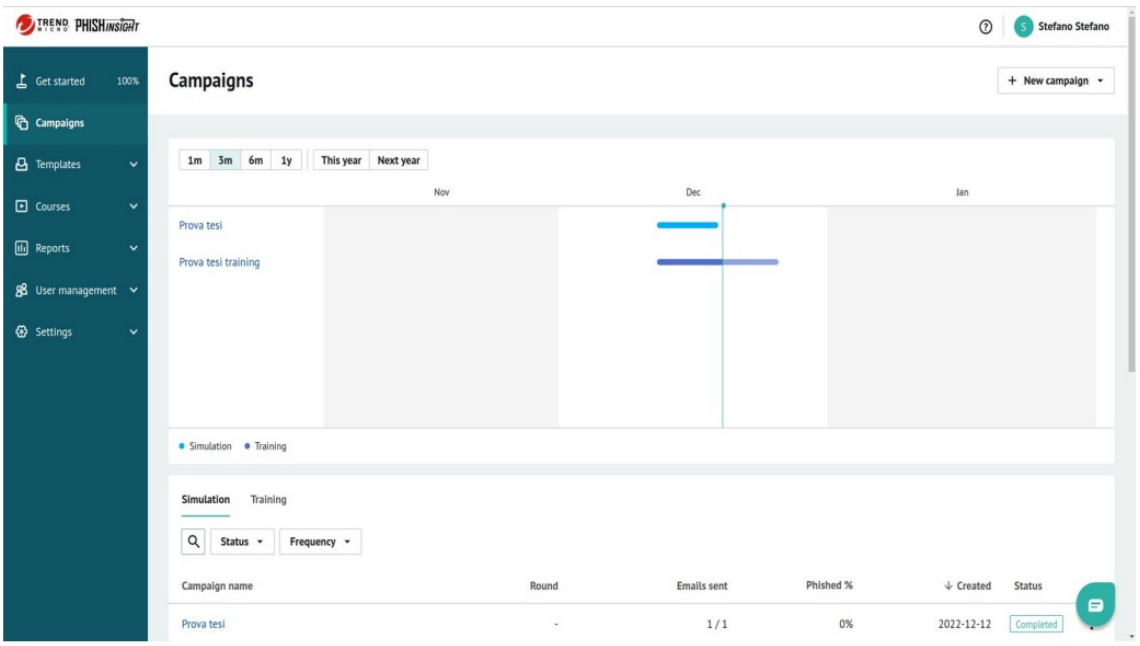
I danni degli attacchi phishing, sulle aziende, possono essere enormi. Infatti può succedere che i malintenzionati riescano ad avere accesso alle aree più sensibili di un'azienda.
Un attacco phishing ad un'azienda può comportare perdita di dati sensibili, danni alla sua reputazione ed ulteriori problemi. L'azienda dovrà quindi attivarsi su diversi fronti, e soprattutto si dovrà occupare di notificare la violazione al Garante per la protezione dei dati personali, nel caso in cui la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. Se il rischio è elevato allora deve essere fatta anche comunicazione a tutti gli interessati. [3]

È evidente, quindi, come sia indispensabile prendere delle precauzioni. Sono indispensabili cose come: filtri antispam efficaci, sistemi operativi e browser aggiornati in modo da evitare che i malintenzionati sfruttino nuove vulnerabilità. È anche importante, configurare backup automatici dei dati, in modo da poterli ripristinare in caso di violazione.

Visto che i malintenzionati trovano spesso nuovi modi per aggirare le misure di sicurezza dei sistemi, è importante anche che i dipendenti di un'azienda siano istruiti, in modo da identificare possibili e-mail sospette.
Gli attaccanti quindi, contano spesso sull'inesperienza dei dipendenti di un'azienda, per condurre attacchi di phishing.
Le aziende sono quindi interessate a risolvere questo problema, e una possibile soluzione sono sicuramente le piattaforme che consentono di simulare attacchi phishing. Simulare attacchi è utile a far comprendere ai dipendenti come non abboccare a questi tranelli. Una famosa piattaforma che consente di fare ciò è PHISHinsight.

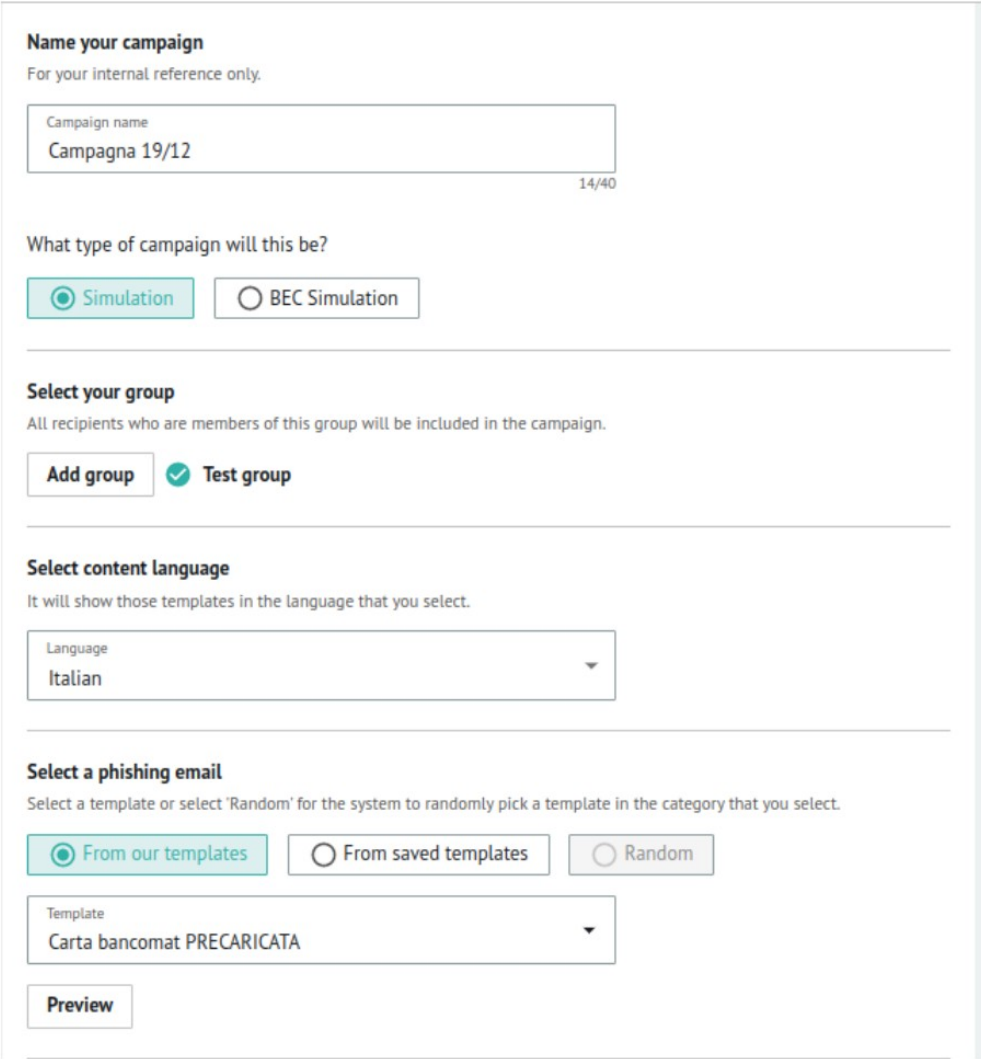
3.1 PHISHinsight

Uno delle piattaforme più famose in questo ambito è PHISHinsight. Su questa piattaforma è possibile effettuare, oltre che simulazioni di attacchi phishing per verificare quanto i dipendenti siano attenti, anche campagne di formazione utile, appunto, a mantenere i dipendenti pronti ad eventuali attacchi. Le campagne di formazione consistono in dei contenuti video che possono essere inviati periodicamente ai dipendenti. Nell'immagine sottostante è visibile l'interfaccia grafica della piattaforma in questione.

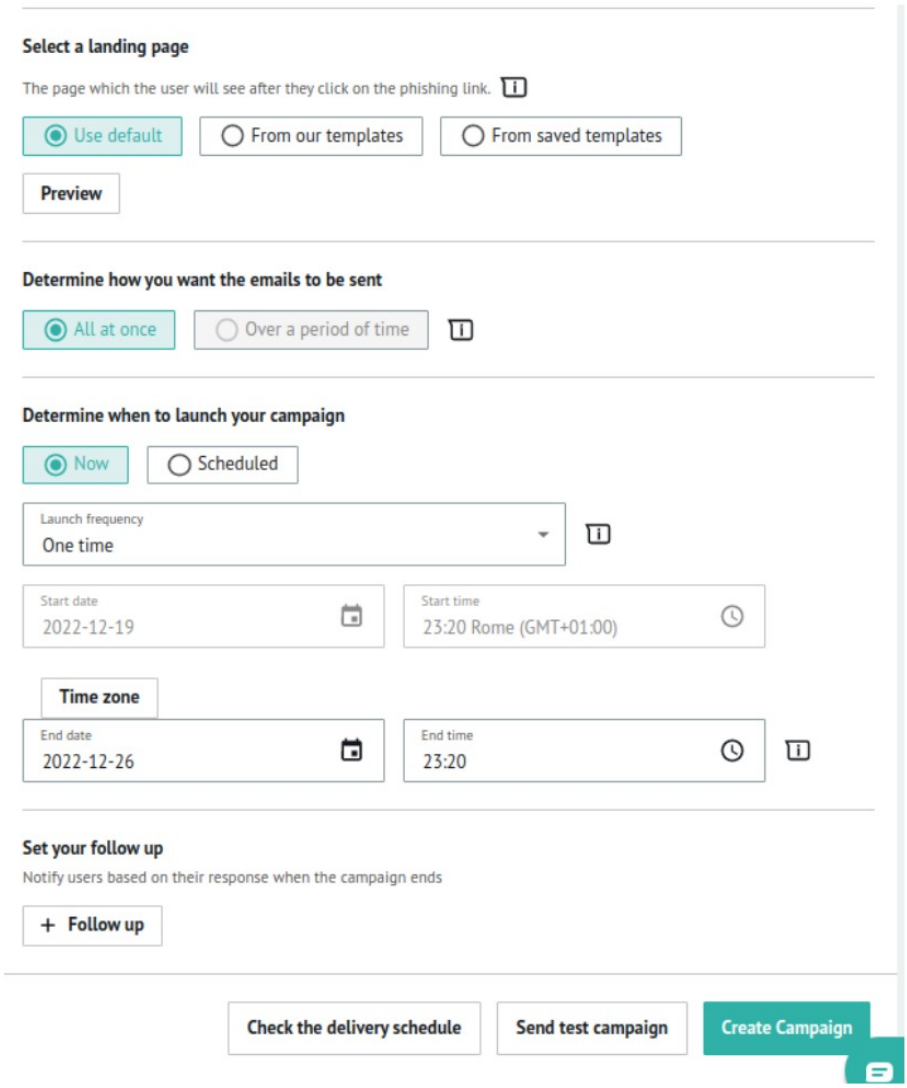


3.1.1 Simulare campagna phishing

È possibile simulare una campagna phishing cliccando in alto a destra sul pulsante *New Campaign* e poi su *Simulation*. A quel punto, dopo aver inserito il nome della campagna, serve selezionare uno specifico gruppo di dipendenti a cui mandare le email di phishing; in questo caso è stato selezionato il gruppo *"Test group"*. Si prosegue quindi selezionando la lingua desiderata per l'email che si sta inviando, e subito dopo è possibile selezionare il template tra quelli predefiniti, oppure selezionare un template predefinito ma con delle modifiche apportate in precedenza (vedi 3.1.1.1).



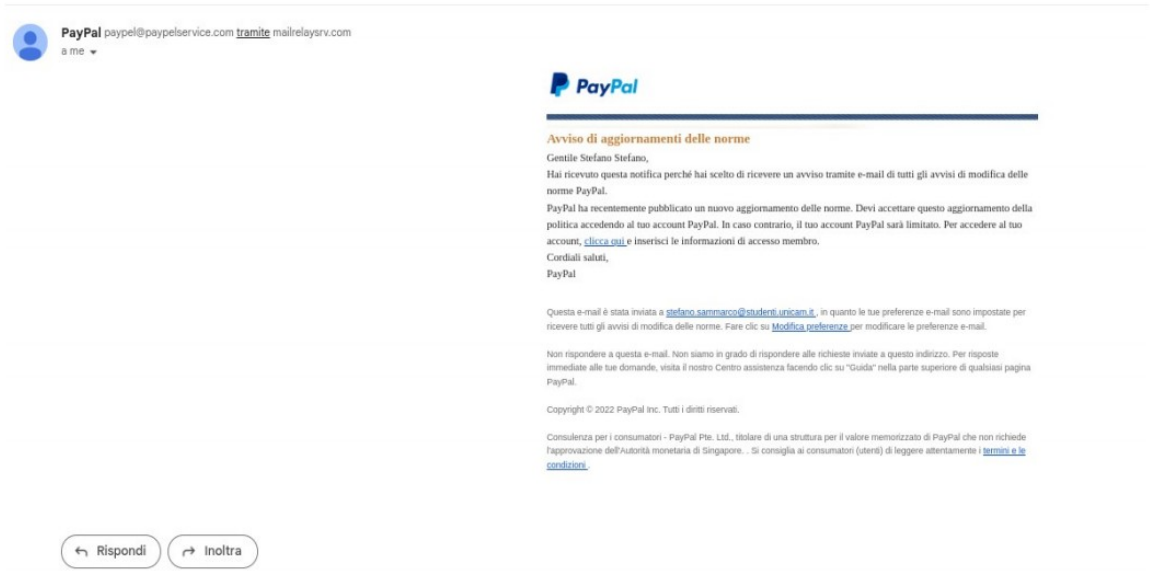
Successivamente si sceglie la landing page, cioè la pagina che sarà mostrata agli utenti che abboccheranno alla simulazione di phishing. Possiamo decidere di mostrare una semplice pagina di default, oppure scegliere tra i diversi template inclusi nella piattaforma (vedi **3.1.1.2** per modifiche template). Infine si seleziona quando far partire la simulazione, indicando data e ora. È possibile anche programmare una campagna in cui mensilmente o trimestralmente vengono inviate email.


Select a landing page
The page which the user will see after they click on the phishing link.
Use default
From our templates
From saved templates
Preview
Determine how you want the emails to be sent
All at once
Over a period of time
Determine when to launch your campaign
Now
Scheduled
Launch frequency
One time
Start date
2022-12-19
Start time
23:20 Rome (GMT+01:00)
Time zone
End date
2022-12-26
End time
23:20
Set your follow up
Notify users based on their response when the campaign ends
+ Follow up
Check the delivery schedule
Send test campaign
Create Campaign

Dopo aver avviato la simulazione, è possibile conoscere l'andamento della campagna in tempo reale. Un esempio nell'immagine sottostante.

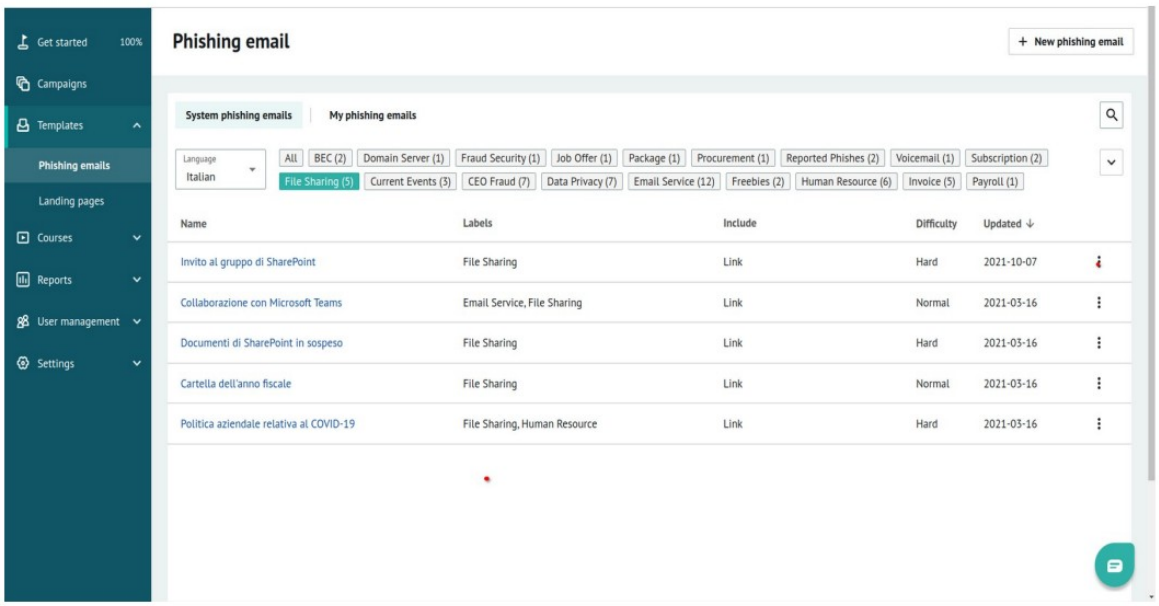
Cliccando sul nome dell'utente vittima, visibile nella parte bassa dell'immagine precedente, è possibile inoltre vedere il comportamento dell'utente. Può essere visto se c'è stato un click sul link presente nell'email, oppure se c'è stata una risposta all'email in questione.

L'utente vittima riceve una email simile a questa che si vede nell'immagine sotto. Se clicca sul link viene quindi reindirizzato alla landing page scelta da chi ha creato la campagna.

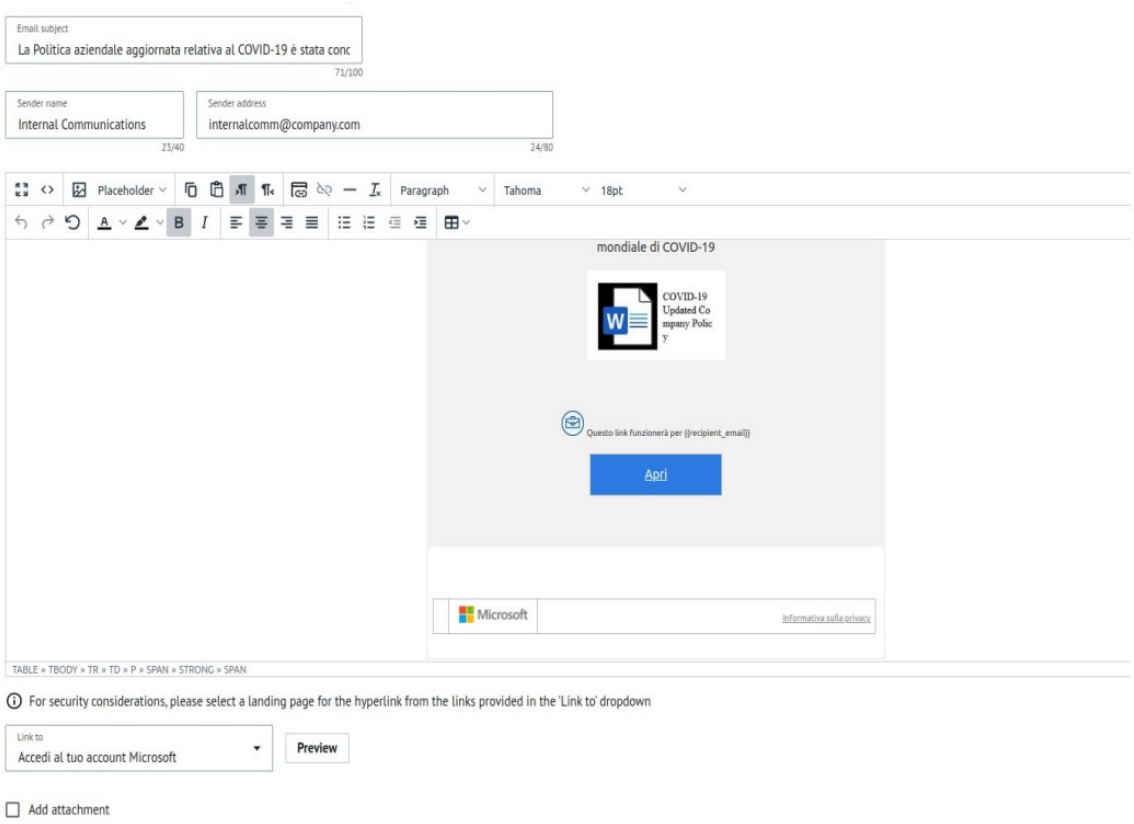


3.1.1.1 Personalizzare un template email phishing

Cliccando su *Templates* e poi su *Phishing emails*, nel menu a sinistra, è possibile visualizzare tutti i template già inclusi nella piattaforma. Dopo aver selezionato la lingua e la categoria, clicchiamo sui tre pallini a sinistra del template che ci interessa, e quindi clicchiamo su *Edit* per modificare.



Nell'immagine a seguire si vede come possiamo modificare, oltre al contenuto, anche l'oggetto dell'email, il nome e l'indirizzo del mittente. Inoltre possiamo anche scegliere la landing page collegata al link che l'utente vittima cliccherà.
Una volta terminate le modifiche possiamo salvare e utilizzare il template in questione per le future simulazioni.

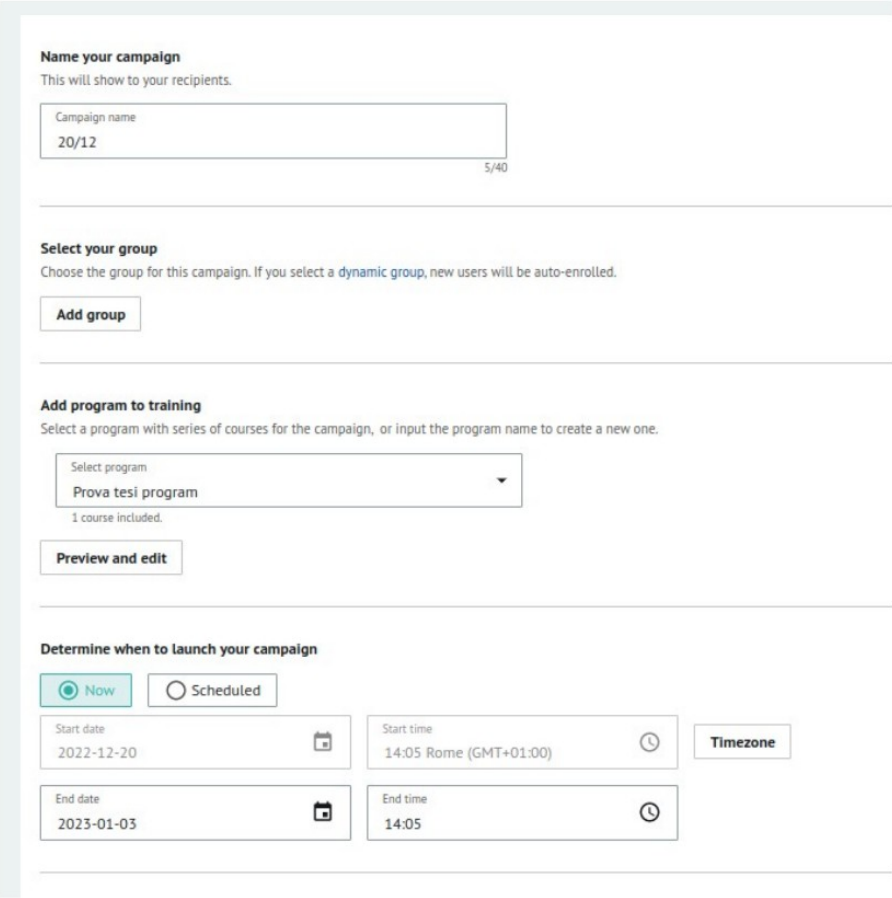


3.1.1.2 Personalizzare template landing page

Possiamo personalizzare il sito web che l'utente si troverà davanti dopo aver cliccato sul link presente nell'email.
Possiamo farlo con la medesima procedura vista per la personalizzazione delle email phishing.
L'unica differenza sta nel fatto che dopo aver cliccato su *Templates* poi bisogna cliccare su *Landing Pages*, nel menu a sinistra.

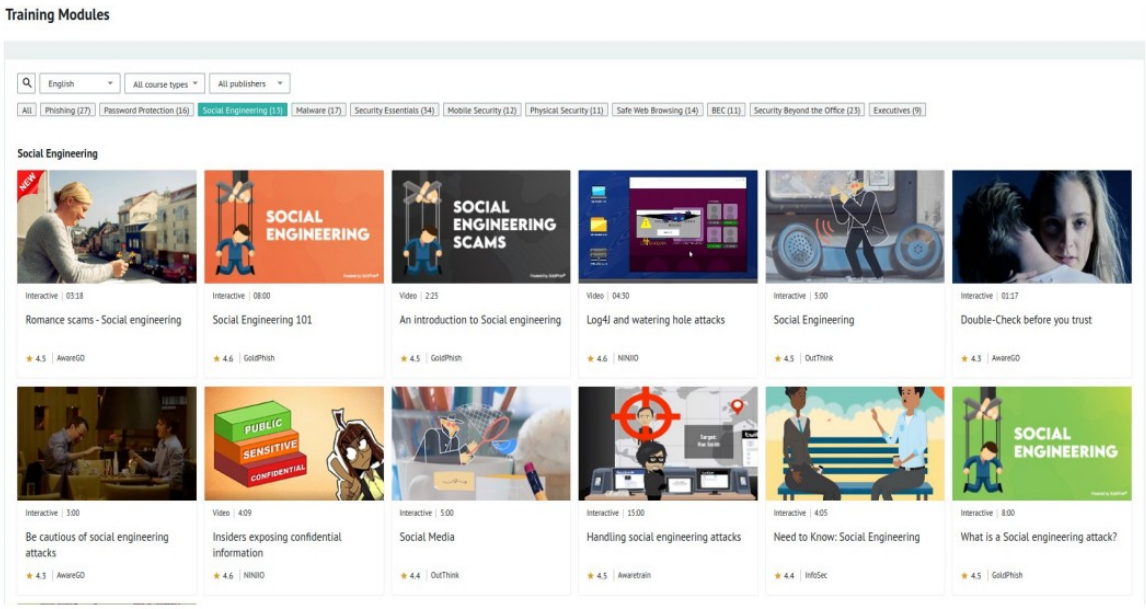
3.1.2 Fare training dipendenti con contenuti video o slide

Si può avviare una campagna training dipendenti, cliccando in alto a destra sul pulsante *New Campaign* e poi su *Training*. Si inserisce il nome della campagna, si seleziona il gruppo di dipendenti che si vuole sottoporre al training, si seleziona il programma creato in precedenza (vedi **3.1.2.1**), e infine si sceglie il periodo temporale più congruo alla campagna in questione.



3.1.2.1 Creare un nuovo programma training e scegliere un contenuto per esso

Sulla piattaforma sono disponibili molti contenuti in diverse lingue. Si può scegliere uno di questi e lo si può inserire in un nuovo programma di training. Si accede alla specifica sezione utilizzando il menu e a sinistra, cliccando su *Courses* e poi su *Training modules*. Poi si seleziona la lingua e si sceglie la categoria di contenuti in base alle necessità.



Si clicca sul contenuto più congruo, e lo si aggiunge ad un programma già esistente o in uno creato sul momento. Il programma con il contenuto scelto, potrà essere selezionato poi durante la procedura per creare una nuova campagna di training.

4. Conclusione

In questa tesi si è voluto analizzare alcuni tra gli strumenti di phishing più conosciuti. In particolare, gli strumenti analizzati, sono di supporto ai malintenzionati che vogliono carpire credenziali di accesso per i più disparati servizi presenti su internet.
Abbiamo visto, poi, che le aziende possono essere duramente colpite da questi attacchi, e quindi c'è un forte interesse per quanto riguarda la prevenzione.
Si può prevenire i danni derivanti da questi attacchi in molteplici modi: filtri antispam, sistemi operativi e browser aggiornati, backup automatici dei dati.
Noi però, abbiamo deciso di analizzare come fare prevenzione andando ad istruire i dipendenti. I malintenzionati, infatti, spesso riescono ad aggirare i sistemi di sicurezza, ed avendo dipendenti istruiti a riconoscere email fasulle, allora si possono evitare spiacevoli conseguenze. Abbiamo analizzato una particolare piattaforma che consente di simulare attacchi di phishing. La piattaforma in questione è phishinsight.

5. Fonti

1. it.wikipedia.org/wiki/SEToolkit
2. www.zscaler.com/resources/security-terms-glossary/what-is-phishing
3. www.garanteprivacy.it/regolamentoue/databreach

6. Ringraziamenti

I ringraziamenti vanno all'Università di Camerino per le opportunità che mi ha regalato durante questi anni.
Un ringraziamento speciale va a tutti i professori della sezione di Informatica; grazie a loro ho avuto modo di formarmi in modo adeguato.

Ringrazio inoltre il mio relatore, cioè il Professor Fausto Marcantoni, che mi ha seguito durante questo percorso conclusivo.

Ringrazio la mia famiglia che mi ha sostenuto economicamente e moralmente durante gli anni della mia permanenza a Camerino.

Ringrazio tutte le persone che standomi accanto, durante gli anni della mia permanenza a Camerino, mi hanno consentito di crescere molto.