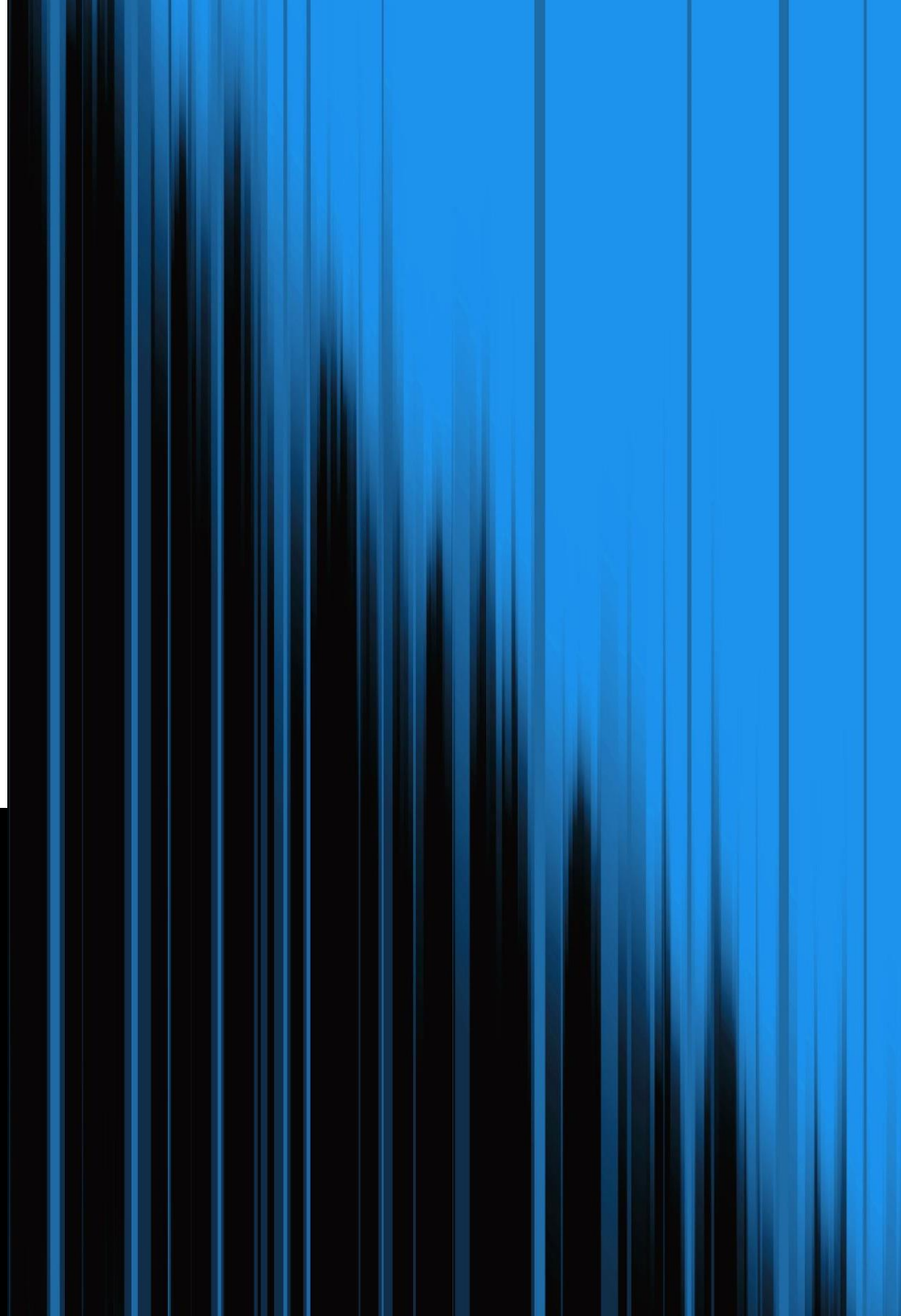
INGEGNERIA SOCIALE

Pablo Andres Balbuena Rios



PROGETTO DELLA SETTIMANA 3

Siete stati chiamati da un'azienda di nome Epicodesecurity, questa azienda ha un sito web suo personale con il nome di dominio www.Epicodesecurity.it. un server email con l'email aziendale Epicodesecurity@semoforti.com

- Il vostro ruolo è quello di spiegare e informare i dipendenti dell'azienda Epicodesecurity sui rischi di attacchi di ingegneria sociale, in particolar modo contro il phishing.

- Come impostate la formazione? (spiegare cos'è il phishing).

- Cosa devono vedere, in particolar modo, i dipendenti per non cadere nel phishing?(quali parametri vedere per identificarlo.Esempio: SPF). Il direttore vi da il permesso di creare un phishing controllato.

- Descrivere come agireste.(Usare dei programmi è opzionale).

- L'obiettivo è cercare di ingannare le persone nel miglior modo possibile.

FORMAZIONE

Qui è riportato una tabella degli orari che potrebbe servire come riferimento, per parlare dell'ingegneria sociale.

Ingneria Sociale	10:00	11:00	12:00	13:00	14:00
Lunedì	Ingneria Sociale	Phishing	Smishing	Pausa	Attaccare con phishing

COS'È INGEGNERIA SOCIALE?

L'ingegneria sociale è una pratica manipolativa che coinvolge l'uso di tecniche psicologiche per ottenere informazioni riservate, accesso non autorizzato a sistemi informatici o persuadere le persone per compiere determinate azioni.

Alcuni esempi di ingegneria sociale sono:

- Phishing: Invio di e-mail fraudolenti che sembrano provenire da siti legittimi.
- Smishing: Invio di messaggi di testo fraudolenti che spingono le persone ad entrare sul link o fornire informazioni sensibili.
- Vishing: Utilizzo di chiamate telefoniche per ottenere informazioni personali o convincere le persone a compiere azioni specifiche.

QUALI SONO I RISCHI?

I più importanti sono:

- Violazione della Privacy:

Gli attacchi spesso mirano a ottenere informazioni personali e riservate delle persone, violando la loro privacy. Per esempio: i dati come nomi, indirizzi, numeri di telefono, informazioni finanziarie e altro.

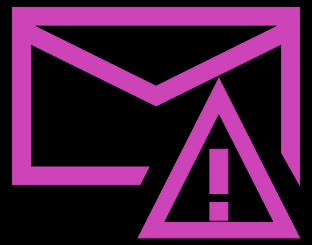
- Furto di Identità:

Gli aggressori possono raccogliere informazioni sufficienti sul identità per compiere gravi conseguenze finanziarie e legali per le vittime.

- Accesso Non Autorizzato ai Sistemi:

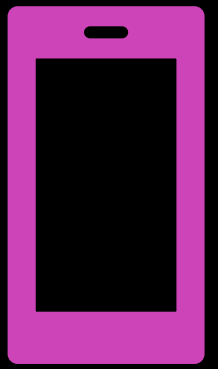
Gli aggressori possono ottenere accesso non autorizzato a sistemi informatici, reti aziendali o account online. Ciò gli consente di compromettere dati sensibili o effettuare attività dannose all'interno di organizzazioni.

COS'È IL PHISHING?



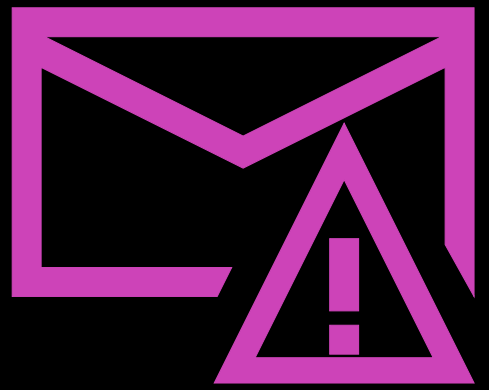
Il phishing è una forma di attacco informatico che coinvolge la frode e l'inganno per ottenere informazioni personali, come nomi utente, password e dettagli finanziari. Gli attaccanti di Phishing normalmente avviene attraverso l'utilizzo delle email.

COS'È LO SMISHING?



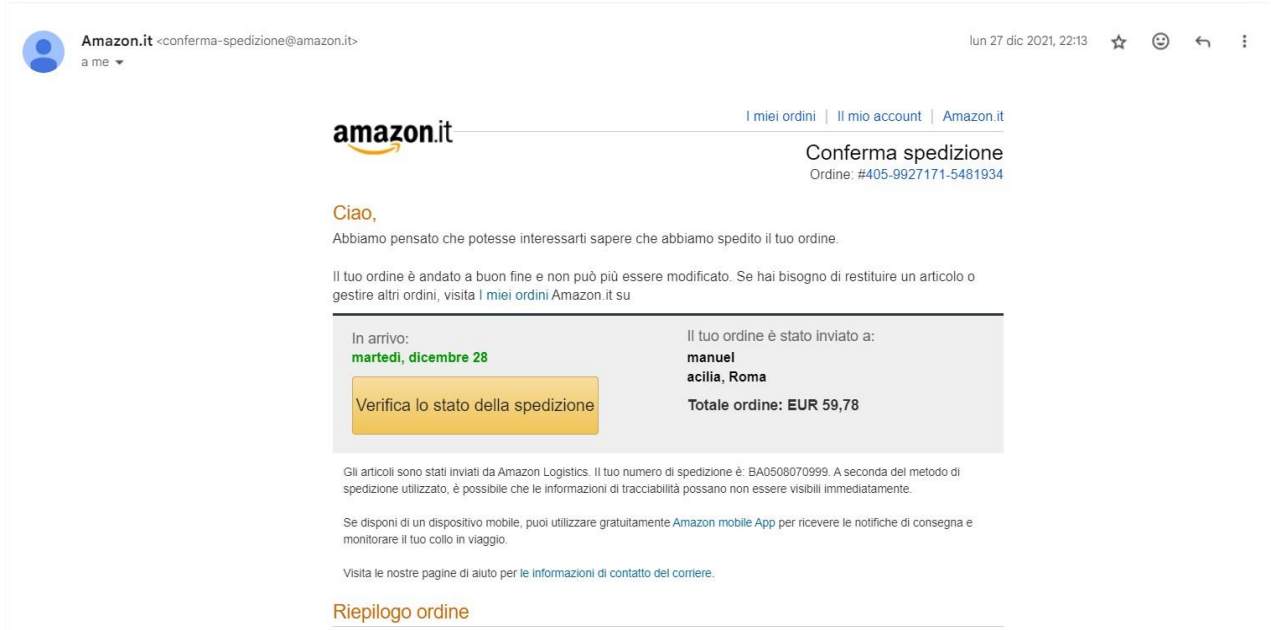
Lo "smishing" è una forma di attacco di phishing che avviene attraverso "SMS" o messaggi multimediali (MMS) inviati a dispositivi mobili. Il termine "smishing" deriva dalla combinazione delle parole "SMS" e "phishing".

COME PROTEGGERSI DAL PHISHING



COME PROTTEGERSI DAL PHISHING

La prima cosa da sapere è che il contenuto del messaggio non conta nulla, perché è molto semplice copiarlo.



Amazon.it <conferma-spedizione@amazon.it>
a me

lun 27 dic 2021, 22:13

amazon.it

I miei ordini | Il mio account | Amazon.it

Conferma spedizione
Ordine: #405-9927171-5481934

Ciao,

Abbiamo pensato che potesse interessarti sapere che abbiamo spedito il tuo ordine.

Il tuo ordine è andato a buon fine e non può più essere modificato. Se hai bisogno di restituire un articolo o gestire altri ordini, visita I miei ordini Amazon.it su

In arrivo:
martedì, dicembre 28

Verifica lo stato della spedizione

Il tuo ordine è stato inviato a:
manuel
acilia, Roma

Totale ordine: EUR 59,78

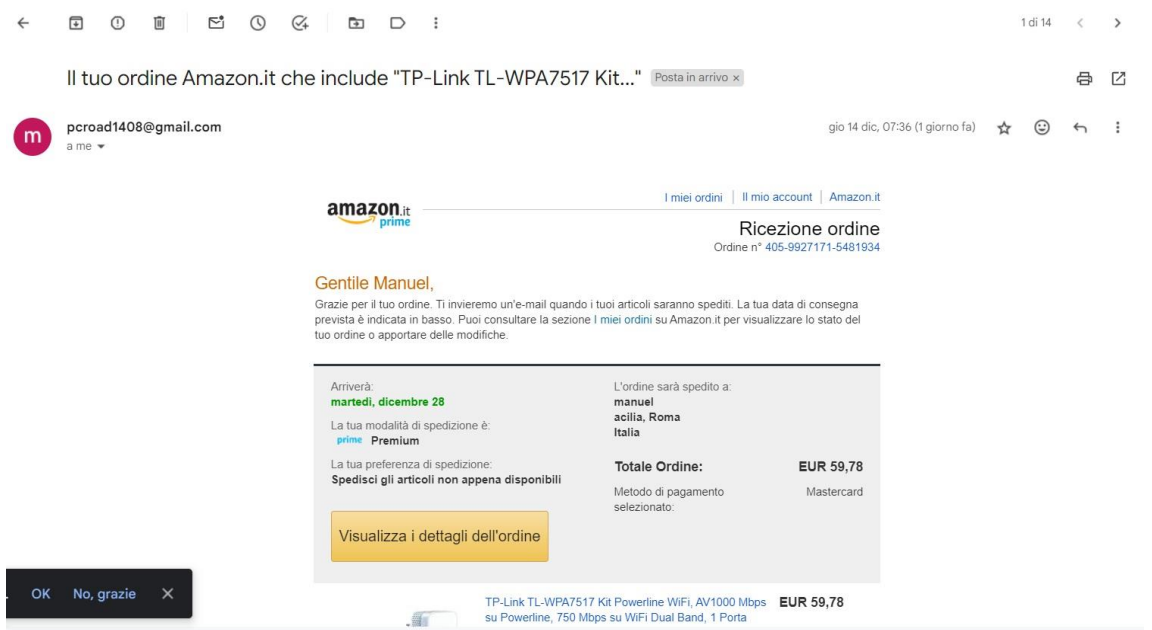
Gli articoli sono stati inviati da Amazon Logistics. Il tuo numero di spedizione è: BA0508070999. A seconda del metodo di spedizione utilizzato, è possibile che le informazioni di tracciabilità possano non essere visibili immediatamente.

Se disponi di un dispositivo mobile, puoi utilizzare gratuitamente Amazon mobile App per ricevere le notifiche di consegna e monitorare il tuo collo in viaggio.

Visita le nostre pagine di aiuto per le informazioni di contatto del corriere.

Riepilogo ordine

originale



1 di 14

Il tuo ordine Amazon.it che include "TP-Link TL-WPA7517 Kit..." Posta in arrivo ×

m **pcroad1408@gmail.com**
a me

gio 14 dic, 07:36 (1 giorno fa)

amazon.it prime

I miei ordini | Il mio account | Amazon.it

Ricezione ordine
Ordine n° 405-9927171-5481934

Gentile Manuel,

Grazie per il tuo ordine. Ti invieremo un'e-mail quando i tuoi articoli saranno spediti. La tua data di consegna prevista è indicata in basso. Puoi consultare la sezione I miei ordini su Amazon.it per visualizzare lo stato del tuo ordine o apportare delle modifiche.

Arriverà:
martedì, dicembre 28

La tua modalità di spedizione è:
prime **Premium**

La tua preferenza di spedizione:
Spedisci gli articoli non appena disponibili

Visualizza i dettagli dell'ordine

L'ordine sarà spedito a:
manuel
acilia, Roma
Italia

Totale Ordine: **EUR 59,78**

Metodo di pagamento selezionato: Mastercard

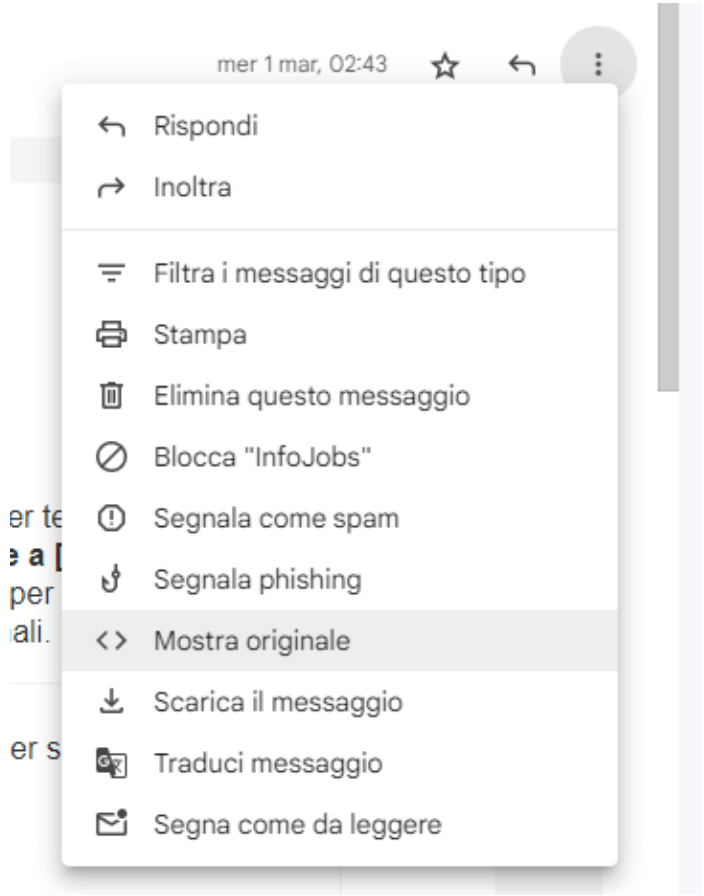
OK No, grazie ×

TP-Link TL-WPA7517 Kit Powerline WiFi, AV1000 Mbps su Powerline, 750 Mbps su WiFi Dual Band, 1 Porta **EUR 59,78**

Falso

COME PROTTEGERSI DAL PHISHING

Dopo di che, si deve andare a visualizzare l'origine messaggio, per vedere il codice del messaggio.



COME PROTTEGERSI DAL PHISHING

A questo punto bisogna vedere l'email del mandante, se coincide, e vedere se sono attive le tecniche di protezione dell'email " SPF, DKIM, DMARC"

Messaggio originale

ID messaggio	<f8cFFSf1RMuh4_aR0GA_EA@geopod-ismtpd-2>
Creato alle:	2 settembre 2023 alle ore 03:10 (consegnato dopo 0 secondi)
Da:	InfoJobs <offerte@push.infojobs.it>
A:	miticopablito2000@gmail.com
Oggetto:	16 nuove offerte per te in [Toscana] Firenze
SPF:	PASS con l'IP 149.72.129.117 Ulteriori informazioni
DKIM:	'PASS' con il dominio push.infojobs.it Ulteriori informazioni
DMARC:	'PASS' Ulteriori informazioni

Attive

Transport; Wed, 13 Dec 2023 10:40:08 +0000
Authentication-Results: spf=none (sender IP is 45.92.111.239)
smtp.mailfrom=ashgsjygg.us; dkim=none (message not signed)
header.d=none;dmarc=none action=none
header.from=carrefour-mail.com;compauth=fail reason=001
Received-SPF: None (protection.outlook.com: ashgsjygg.us does not designate
permitted sender hosts)

Non attive

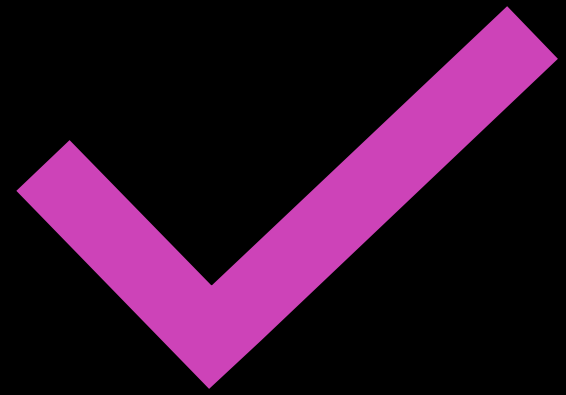
COS'È SPF,DKIM

Tutte e due sono tecniche di protezione che sono collocate nei server di chi riceve l'email.

SPF: Verifica se il server di invio di un messaggio è autorizzato a inviare email per il dominio specificato nell'indirizzo del mittente.

DKIM: Il DKIM è una firma digitale, Il mittente utilizza una chiave crittografica privata per firmare digitalmente e il destinatario può quindi utilizzare la chiave per verificare l'autenticità e l'integrità della firma DKIM.

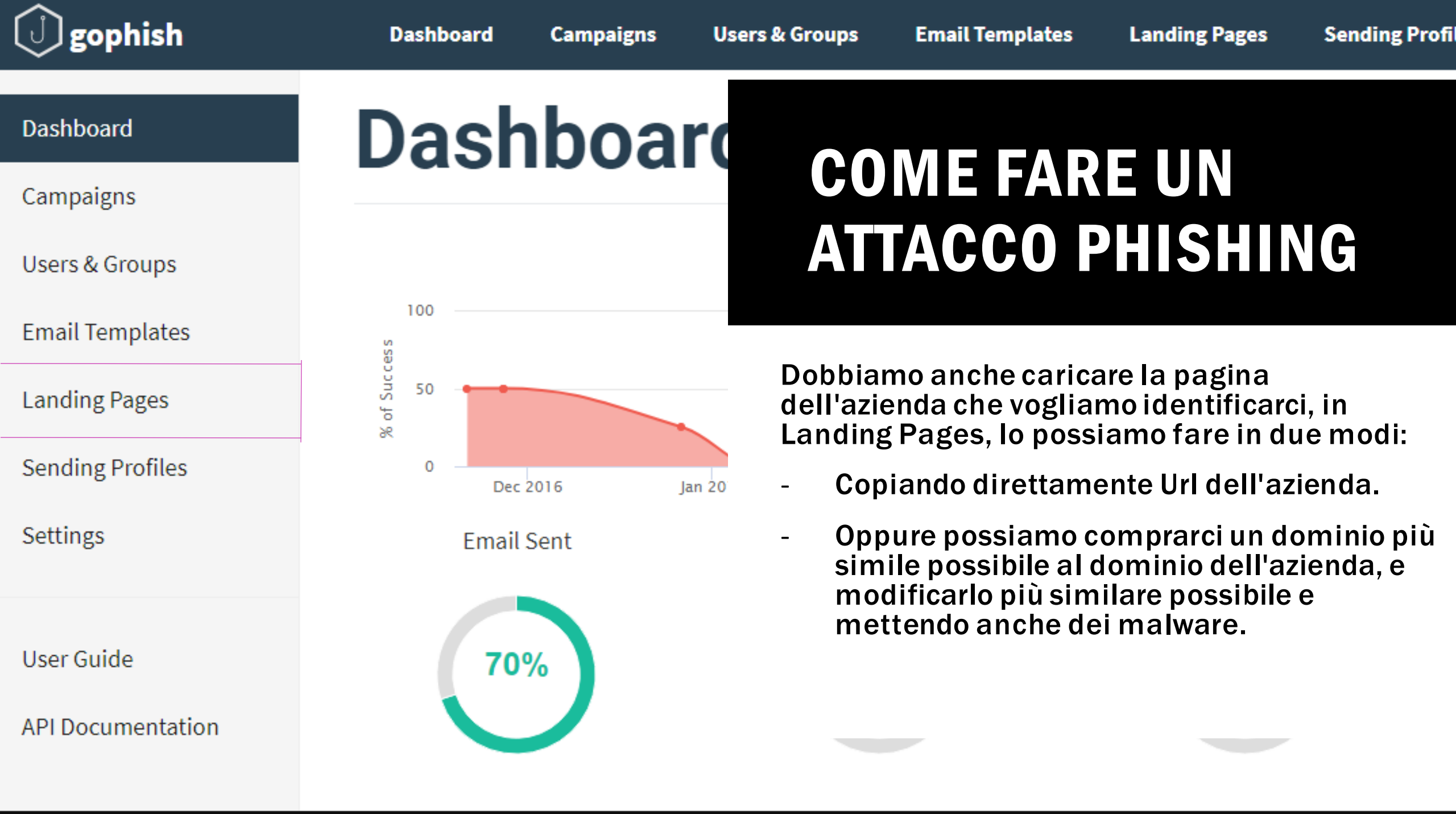
CREAZIONE DEL PHISHING CONTROLLATO

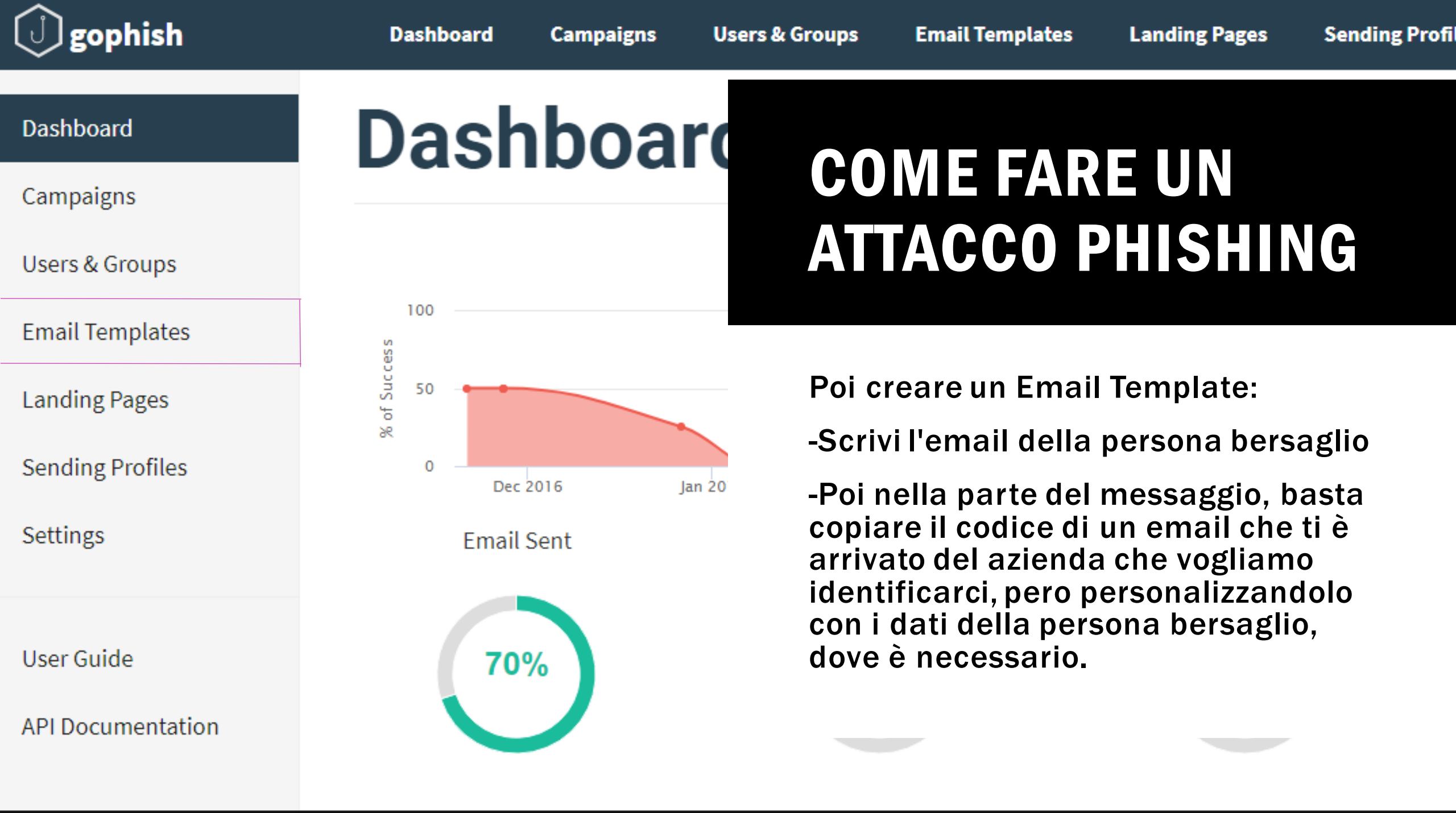


COME FARE UN ATTACCO DI PHISHING

La prima cosa da fare e avere un programma che può fare il Phishing Controllato, es: Gophish


gophish
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profi
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profiles
Settings
User Guide
API Documentation
Dashboard
100
50
0
% of Success
Dec 2016
Jan 20
Email Sent
70%
COME FARE UN ATTACCO PHISHING
Per prima cosa dobbiamo crearci un email più similare possibile all' email dell'azienda che vogliamo indentificarci, così la persona bersaglio non sospetterà nulla.


gophish
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profi
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profiles
Settings
User Guide
API Documentation
Dashboard
100
50
0
% of Success
Dec 2016
Jan 20
Email Sent
70%
COME FARE UN ATTACCO PHISHING
Dobbiamo anche caricare la pagina dell'azienda che vogliamo identificarci, in Landing Pages, lo possiamo fare in due modi:
- Copiando direttamente Url dell'azienda.
- Oppure possiamo comprarci un dominio più simile possibile al dominio dell'azienda, e modificarlo più similare possibile e mettendo anche dei malware.


gophish
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profi
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profiles
Settings
User Guide
API Documentation
Dashboard
100
50
0
% of Success
Dec 2016
Jan 20
Email Sent
70%
COME FARE UN ATTACCO PHISHING
Poi creare un Email Template:
-Scrivi l'email della persona bersaglio
-Poi nella parte del messaggio, basta copiare il codice di un email che ti è arrivato del azienda che vogliamo identificarci, pero personalizzandolo con i dati della persona bersaglio, dove è necessario.


gophish
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profi
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profiles
Settings
User Guide
API Documentation
Dashboard
100
50
0
% of Success
Dec 2016
Jan 20
Email Sent
70%
COME FARE UN ATTACCO PHISHING
Infine dobbiamo settare il Sending Profile, che è il server che lancia la campagna e lanciarlo attraverso "Campaigns".