

# Progetto S5/L5

## Creazione di una mail di phishing indirizzata ad una vittima

### Scenario

Creiamo una documentazione credibile che includa un pagamento sospetto recente effettuato tramite un servizio noto e ampiamente utilizzato a livello globale, come "PayPal". Il cliente, allarmato dalla notifica, sarà spinto a verificare cosa stia succedendo nel suo account cliccando sul link fornito. Questo link lo reindirizzerà a una pagina clonata, dove gli verranno richiesti indirizzo email e password. Una volta inserite le credenziali, queste saranno immediatamente visibili per la nostra consultazione.

Ciao Alessio Di Donato



**Hai pagato €3000,00 EUR a Tony Chan SPA**

Vedi o gestisci pagamento

**Codice transazione**  
1YD069232M4979303

**Data transazione**  
01 novembre 2024

**Commerciante**  
Tony Chan SPA  
Tonychan@gmail.com  
+27 800 900 860

Totale parziale€3000.00 EUR

Totale€3000.00 EUR

Pagamento€3000.00 EUR

L'addebito sarà riportato sull'estratto conto della tua carta di credito come "PAYPAL"

# Inserimento messaggio

Oggetto: Notifica di attività sospetta sul tuo account PayPal

Gentile [Alessio Di Donato],

Abbiamo rilevato un addebito recente di 3.000 euro sul suo account PayPal che non risulta comune rispetto alle sue transazioni precedenti.

Se ha autorizzato questo pagamento, non è necessaria alcuna azione da parte sua. In caso contrario, la invitiamo a verificare l'attività del suo account per garantire la sicurezza del suo profilo.

Per procedere, acceda al suo account direttamente dal link della mail. Una volta effettuato l'accesso, potrà visualizzare i dettagli della transazione e, se necessario, segnalare eventuali problemi.

In alternativa, può contattare il nostro servizio clienti al numero [+27 333 3333333] per assistenza.

Grazie per la sua attenzione e collaborazione.


Cordiali saluti,

[Il team di supporto PayPal ]

(reindirizzamento sito))

INTERNET ARCHIVE | <https://www.paypal.com/signin> | Go | Jan | Feb | Mar | success | fail | 13 | 2015 | 2016 | 2017 | About this capture

WayBackMachine

  
  
  
  
[Forgot your email or password?](#)  

---

Questo è ciò che vedremo una volta che la vittima cadrà nella nostra trappola.


```
back is if username and password form fields are available. Regardless, this captures
Kit Credential Harvester Attack
running on port 80
played to you as it arrives below:
[4:40:56] "GET / HTTP/1.1" 200 -
[4:40:57] code 501, message Unsupported method ('HEAD')
[4:40:57] "HEAD /web/20160213005026/http://web.archive.org/screenshot/https://www.pay
[4:40:57] "GET /__wb/sparkline?output=json&url=https%3A%2F%2Fwww.paypal.com%2Fsignin
[4:40:57] "GET /_static/css/iconochive.css?v=3PDvdIFv HTTP/1.1" 404 -
[4:40:57] "GET /_static/css/banner-styles.css?v=S1zqJCYt HTTP/1.1" 404 -
the output:
p17W65ojSpBAyB/L7ALJQ4=

ID: login_email=alessio@libero.it
ID: login_password=12345
ID: login_password=12345
na~a2=na~a4=Mozilla~a5=Netscape~a6=5.0+(X11)~a7=20100101~a8=na~a9=true~a10=Linux+x86_
X11;+Linux+x86_64;+rv:109.0)+Gecko/20100101+Firefox/115.0~a15=false~a16=en-US~a17=na
a24=969~a25=24~a26=934~a27=na~a28=Sat+Feb+13+2016+01:50:27+GMT+0000+(Coordinated+Univ
no~a35=no~a36=yes~a37=no~a38=online~a39=no~a40=Linux+x86_64~a41=no~a42=no~
IT CONTROL-C TO GENERATE A REPORT.
```

Lo scenario creato sembra realizzato su misura: il sito è riprodotto in modo identico all'originale, con loghi accuratamente copiati e un messaggio che appare genuino agli occhi della vittima. In realtà, sono visibili numerosi errori e segnali di allarme da notare per evitare di cadere nel tranello.

- Primo accorgimento

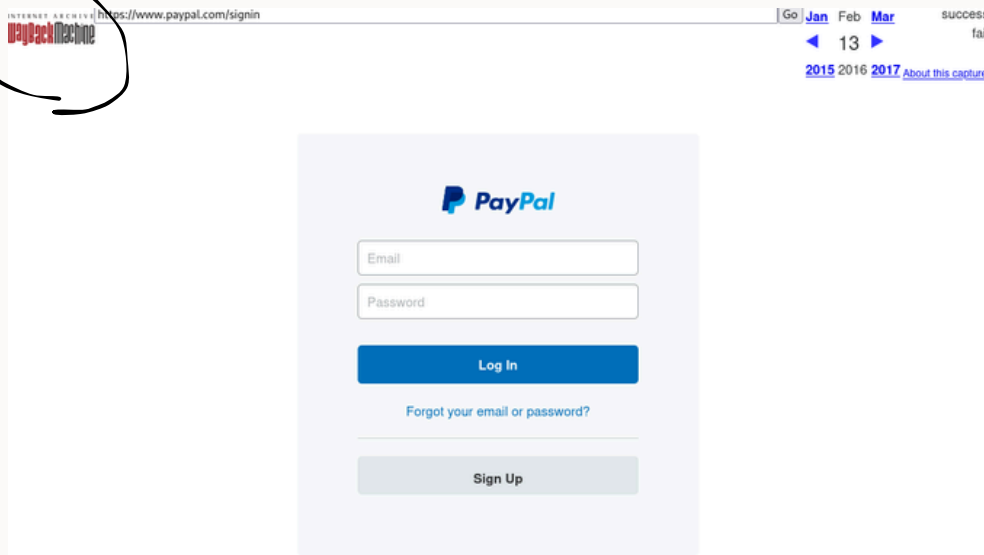
- CONTACT US URGENTLY: PAGAMENTO SOSPETTO



- **alessioddnt@gmail.com**
- Da:** alessioddnt@gmail.com
- A:** alessio didonato

La mail è stata inviata da un autore sospetto che non fa parte del team di paypal ma sembra essere una persona fisica.

- Secondo accorgimento



Una volta che l'utente è caduto nel tranello ed è stato reindirizzato alla pagina di PayPal, possiamo notare molti errori.

In alto a sinistra è presente un sito sospetto. Probabilmente è stata utilizzata un'immagine di un account che include sia l'email che la password, allo scopo di raccogliere tutte le informazioni della vittima. Inoltre, la pagina di login di PayPal risale a qualche anno fa, poiché non include i campi per inserire sia email che password contemporaneamente.

- Terzo accorgimento



Il numero inserito ha un prefisso proveniente dal Sudafrica. Generalmente, il servizio clienti di PayPal utilizza un numero verde o un numero italiano.

# Conclusioni

Le vittime del phishing sono spesso ingannate da siti e comunicazioni apparentemente legittimi, che sfruttano la fiducia e la somiglianza visiva con marchi noti per raccogliere informazioni personali e dati sensibili. Chi cade in questi tranelli rischia di subire gravi conseguenze, come la compromissione del proprio account, il furto d'identità e, in alcuni casi, la perdita di denaro.

Per evitare di cadere nelle trappole degli hacker, è fondamentale adottare alcune misure di sicurezza:

**Verificare l'URL:** Prima di inserire le proprie credenziali, controllare attentamente l'indirizzo web. I siti di phishing spesso presentano URL leggermente modificati o con prefissi/suffissi strani.

**Diffidare di richieste urgenti:** Gli hacker utilizzano la pressione del tempo per spingere gli utenti ad agire senza riflettere. Prestare attenzione a messaggi che richiedono azioni immediate.

**Evitare di cliccare su link sospetti:** È sempre consigliabile accedere al proprio account direttamente dal sito ufficiale o dall'app dell'azienda, senza fare clic sui link ricevuti via email o SMS.

**Controllare i dettagli di contatto:** Verificare che eventuali numeri di telefono o indirizzi email siano quelli ufficiali dell'azienda, poiché i servizi legittimi utilizzano sempre canali di comunicazione sicuri e verificabili.

**Utilizzare l'autenticazione a due fattori (2FA):** Abilitare questa funzione ove possibile per aggiungere un ulteriore livello di protezione al proprio account.

Essere consapevoli di queste tecniche e delle precauzioni di sicurezza è la chiave per evitare di cadere nelle trappole del phishing e mantenere al sicuro le proprie informazioni.

