

ESERCIZIO 2

Titolo

TECNICA DI DIFESA CONTRO IL PHISHING

Scopo

Il Phishing è un particolare sistema di truffa effettuata in rete. Il malintenzionato cerca di ingannare la vittima convincendola a fornire informazione personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale (Wikipedia).

Gli esperti generalmente sono in grado di difendersi da tale tecnica riconoscendo in anticipo che si tratta di una frode; stessa cosa non si può dire dei comuni cittadini, i quali sono soggetti spesso a questo tipo di truffa.

Lo scopo dell'esercizio è mostrare come chiunque possa difendersi da tale attacco.

Per chi

Chiunque sia in grado di navigare sul web o abbia ricevuto una mail sospetta.

Durata

5 minuti

Livelli arcobaleno

1. L3

Tag/keyword

Phising, difesa, educazione, rischi

Difficoltà (relativa all'utente)

Facile

Strumenti, s.o., pacchetti/app

- Connessione a Internet
- browser

Costi

Nessuno

Istruzioni dettagliate

- 1) Vi sono diverse diramazioni della tecnica di phishing, a seconda di come viene contattata la vittima e di ciò che la si vuole indurre a fare, però questo tipo di attacco si caratterizza solitamente per presentare un link che rimanda a codice malevolo o più comunemente ad una pagina in cui sono richiesti dei dati personali (che saranno ricevuti direttamente dall'attaccante).

Un esempio potrebbe essere il seguente:

Gentile cliente,

Grazie ai pagamenti da lei effettuati e ricevuti, nel tempo ha accumulato un bonus di EURO 217,32.

La promozione è valida per tutti i clienti che hanno una prepagata postepay fino al 31 agosto 2013.

Per ricevere il bonus è necessario di avere un saldo minimo di EURO 250,00 sulla carta prepagata PostePay.

Per aderire alla promozione è sufficiente completare [QUI](#)

Il bonus le verrà accreditato entro 24 ore sotto forma di ricarica postepay

Poste Italiane.

Cordiali Saluti,

[Poste Italiane](#)



<https://s.id/gYLi3> (attenzione, non cliccare sul seguente link)

- 2) La prima cosa da fare è aprire il sito VirusTotal
<https://www.virustotal.com/gui/home/url>

Attraverso il motore di ricerca di VirusTotal è possibile capire se il link che è stato fornito nella mail contiene codice maligno (malware).

Per fare ciò è necessario copiare e incollare il link nella barra di ricerca di Virus Total.

Anche se viene ritornato un solo codice positivo, è già abbastanza per comprendere che il contenuto è malevolo.



Analyze suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community

FILE URL SEARCH

Search or scan a URL

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the sharing of your URL submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more.](#)

Want to automate submissions? [Check our API](#), free quota grants available for new file uploads

https://s.id/gYLi3

1 / 79

1 security vendor flagged this URL as malicious

https://s.id/gYLi3
s.id

Community Score

DETECTION	DETAILS	COMMUNITY 1
Comodo Valkyrie Verdict	Malicious	
AlienVault	Clean	
Artists Against 419	Clean	
BADWARE.INFO	Clean	

- 3) Verificato che il messaggio ricevuto è una frode, l'utente più esperto potrebbe interessarsi degli eventi e dei rischi che intercorrono quando si apre il link. Ovviamente questo non può essere fatto sul proprio computer, altrimenti c'è il rischio di infettarsi. Per fare ciò è possibile usare una macchina virtuale oppure un altro software di test analysis presente in rete, come ad esempio "Joe SandBoxes". La maggior parte di questi strumenti sono a pagamento, perciò non verrà mostrato il loro utilizzo.
- 4) Nel caso il software VirusTotal non abbia riportato nessun pericolo, significa che il link non contiene codice malevolo, ma invece restituisce probabilmente una pagina con l'obiettivo di rubare informazioni personali. Non è necessario aprire il link, ci limiteremo ora ad osservare la mail e capire se effettivamente si tratta di phishing con un'attenta analisi dei dettagli.

- 5) La seguente mail pretende di essere stata inviata da Apple e afferma che il proprio account è stato sospeso a causa di un accesso sospetto da un sistema operativo Linux. Per risolvere questo problema si conclude che bisogna accedere al proprio account facendo clic sul link <https://appleid.apple.com>

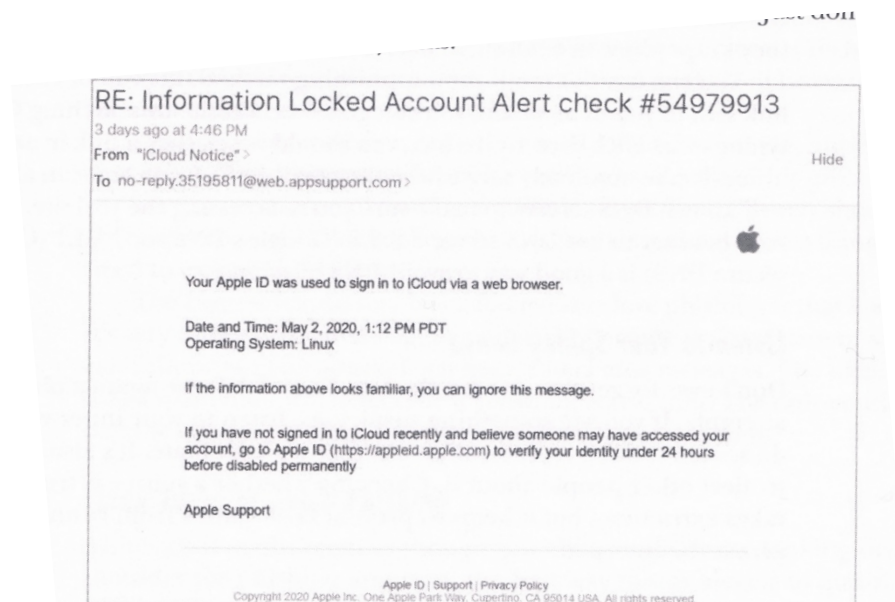
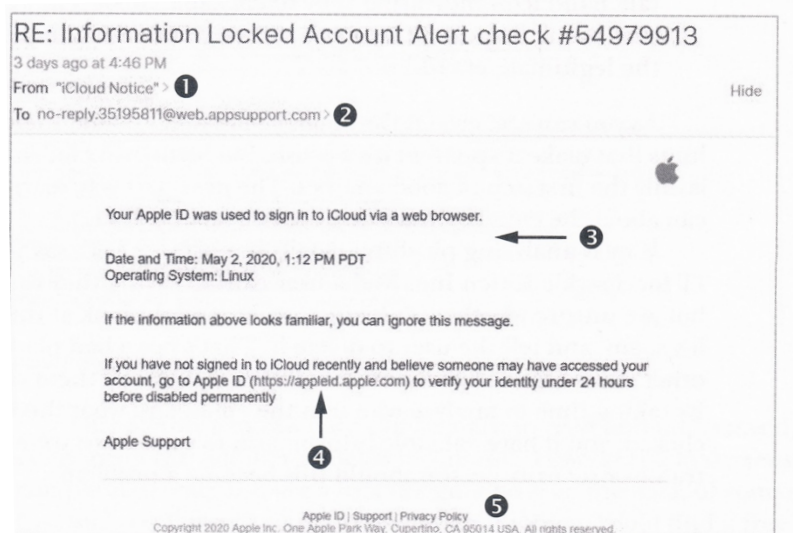


Figure 3-1: An example of a phishing email

Ci sono molti elementi da analizzare:



- I. Il mittente della posta è iCloud Notice, il quale è sospetto, perché ci si aspetterebbe solo Apple. Inoltre, è anche racchiuso tra doppi apici, i quali indicano che si tratta di un "nome amichevole". Molti client di posta infatti modificano i nomi per rendere più facilmente leggibile i mittenti con i nomi effettivi di contatto. Questo ovviamente non dovrebbe succedere per una mail da parte di Apple.

- II. Il campo 'To' non include il proprio indirizzo mail. Ciò indica che la mail è stata inviata usando il BCC (blind carbon copy), il quale nasconde a chi è stata inviata la mail. I malintenzionati usano questo trucco per inviare e-mail di phishing a più vittime senza farglielo notare.
- III. Il corpo della mail non mostra mai il proprio name account. Se questo messaggio di alert fosse indirizzato proprio a noi, non dovrebbe contenere da qualche parte il proprio nome?
- IV. Il link fornito è lo stesso di una legittima mail da parte di Apple, ma qui è attivo (cliccabile). Ancora più importante, quando si passa con il mouse sopra il link viene mostrato in sovraimpressione un URL che non è corrispondente a quello scritto e che non è un link che porta ad un servizio di Apple.
- V. In fondo alla mail ci sono tre link, rispettivamente Apple ID / Supporto / Privacy Policy. Quando si passa sopra di essi con il mouse non viene mostrato nulla e non si colorano come fanno i comuni link. La ragione è infatti che non si tratta di link, ma solo di un'immagine per mimare la firma della mail originale.

Ogni mail o messaggio di phishing è differente, ma sicuramente presenterà almeno uno dei punti critici esposti precedentemente.

Inoltre, si ricorda che qualsiasi operatore di servizi online come Apple, Google, Microsoft etc... non includerà mai un link che porta direttamente ad una pagina di login, ma chiederà esplicitamente di accedere al proprio sito tramite ricerca, per effettuare l'operazione che si vuole soddisfare.

Risultati attesi

L'utente è ora in grado di determinare se la mail / messaggio da lui ricevuto è un particolare attacco di phishing.

Obiettivi "formativi"

Comprendere come difendersi dagli attacchi di phishing, oltre che salvaguardare lo stato e i dati personali, aumenta inevitabilmente la consapevolezza riguardo lo stato interno dei processi tecnologici, poiché per difendersi bisogna prima obbligatoriamente capire, almeno superficialmente, ciò che accade.

Ora l'utente sarà in grado di distinguere un caso di phishing da una mail originale da parte un particolare ente.

Autore

Morgan Malavasi

Licenza (libera, compatibile con GNU/GPL o CC)

GPLv3