OUCH! | Luglio 2016

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...



# La truffa del CEO

## Cos'è la truffa del CEO?

I criminali informatici sono sempre più subdoli ed elaborano di continuo nuovi modi per ottenere ciò che vogliono. Uno dei metodi più efficaci è mirare alle persone che vi sono vicine. Nonostante sappiano che le persone con scarse conoscenze costituiscono l'anello più debole di ogni azienda, non sanno che i lettori di OUCH! possono esserne la miglior difesa.


### L'autore di questo numero

Angela Pappas è direttore della formazione sui temi della Sicurezza delle informazioni e della Security Awareness in Thomson Reuters.Tra i sui ruoli figurano le responsabilità del programma di eLearning e della formazione dei dipendenti sul phishing.


Uno degli attacchi sviluppati negli ultimi anni prende il nome di "truffa del CEO" poiché il truffatore finge di essere un CEO o un altro top manager della vostra azienda. Vi manda un email cercando di ingannarvi e portarvi a svolgere un'azione che non dovreste fare. Si tratta di un tipo di attacchi molto efficace perché si basa su ricerche effettuate in precedenza, ad esempio, sul sito web della vostra azienda dove è possibile trovare informazioni sulle sue locazioni geografiche, sui dirigenti e sulle altre aziende con cui lavorate, o su siti come Linkedin, Facebook o Twitter, dove è possibile reperire un gran numero di informazioni sui vostri colleghi. Una volta compresa la struttura organizzativa dell'azienda, i criminali partono alla ricerca di impiegati specifici. Scelgono i loro obiettivi sulla base di scopi ben precisi: se, ad esempio, vogliono un guadagno economico, potrebbero mirare allo staff dell'ufficio che effettua pagamenti. Se cercano informazioni sulle tasse, potrebbero rivolgersi alle risorse umane. Se vogliono accedere ai server dei database, si rivolgeranno a qualcuno del dipartimento IT.

Una volta determinato cosa vogliono e chi sarà il loro obiettivo, inizieranno a confezionare il loro attacco, utilizzando la tecnica dello spear phishing. Ricorderete sicuramente l'attacco phishing, in cui un attaccante invia un messaggio a milioni di persone per ingannarli con lo scopo di farli compiere un'azione, ad esempio aprire un allegato infetto o visitare un sito maligno. Lo spear phishing è simile al phishing, ma anziché inviare un messaggio generico a milioni di persone, viene inviata un'email personalizzata indirizzata a un piccolo e selezionato numero di potenziali vittime. Questi messaggi sono estremamente realistici e difficili da individuare: spesso appaiono provenire da qualcuno che conoscete o con cui

# La truffa del CEO

lavorate, come un collega o il vostro capo. L'email potrebbe impiegare lo stesso gergo usato in azienda, usare il logo aziendale o anche la firma ufficiale di un dirigente. Questi messaggi spesso creano un grande senso di urgenza, chiedendovi di agire immediatamente senza divulgare la cosa a nessuno. L'obiettivo del criminale è di costringervi a commettere un errore. Ecco due scenari molto comuni:


*La frode del CEO è un attacco in grado di oltrepassare la maggior parte delle misure di sicurezza. Ricordate che, in ultimo, siete voi la miglior difesa.*

- **Bonifici e pagamenti**. Il criminale vuole ottenere del denaro e per farlo cercherà i nomi delle persone che lavorano nell'ufficio che si occupa dei pagamenti o che amministra le finanze aziendali. Successivamente preparerà un'email fingendosi uno dei loro superiori: nel messaggio comunicherà che a causa di una necessità urgentissima dovrà essere trasferito del denaro a un determinato conto

- **Frode fiscale**: I criminali informatici vogliono rubare le informazioni sui vostri colleghi in modo che possano impersonare dipendenti per frode fiscale. Si ricerca la vostra organizzazione e determinare che gestisce le informazioni sui dipendenti, per esempio, qualcuno in risorse umane. Da lì, i criminali informatici inviano messaggi di posta elettronica fasulli che finge di essere un alto dirigente o qualcuno legale, chiedendo alcuni documenti essere fornite immediatamente

- **Falsi avvocati**. Non tutti gli attacchi fanno uso della sola email. Altri metodi prevedono l'uso del telefono. In questi scenari, i criminali inviano un messaggio spacciandosi per un manager e avvisando la vittima che un avvocato la contatterà per una questione della massima urgenza. In seguito, il criminale telefonerà fingendosi l'avvocato, vi metterà sotto pressione parlando di questioni confidenziali e della massima urgenza. Questa sensazione abbasserà le vostre difese e vi porterà ad agire nel modo sbagliato

## Come proteggersi

Per proteggersi, il buon senso è la miglior difesa. Se ricevete un messaggio da un vostro superiore o da un collega e vi sembra sospetto, potrebbe trattarsi di un attacco. Tra gli indicatori di questa minaccia troviamo il tremendo senso di

# La truffa del CEO

urgenza, la firma che non sembra corretta, un tono che non vi aspettereste mai da quella persona, o qualche discrepanza nei nomi. Altri indicatori sono indirizzi email o numeri di telefono che non avete mai visto prima, o indirizzi email molto simili, ma non esattamente corrispondenti a quelli dei vostri colleghi o superiori. Nel dubbio, chiamate la persona a un numero di telefono che conoscete o incontratela direttamente (non rispondete via mail) e chiedete conferma che sia stato effettivamente lui il mittente. Non cercate di scavalcare le policy e le procedure di sicurezza. La vostra azienda potrebbe avere policy che definiscono le procedure appropriate per autorizzare il trasferimento di fondi o la divulgazione di informazioni confidenziali. Le richieste che cercano di scavalcare queste policy, indipendentemente dalla loro fonte apparente, devono essere considerate come sospette e verificate prima di intraprendere qualsiasi azione. Se ricevete queste richieste e non siete sicuri su come comportarvi, contattate il vostro responsabile, l'help desk o il l'ufficio sicurezza.

## Per saperne di più

Iscriviti ad OUCH!, la newsletter mensile dedicata alla security awareness, consulta i suoi archivi online, e scopri le soluzioni di SANS sulla security awareness visitando il sito

securingthehuman.sans.org/ouch/archives

## Versione in Italiano

La versione in italiano è curata da Advanction S.A., un'azienda impegnata nella Sicurezza, nel Risk Management Operativo e nella Security Awareness. Seguila su www.advanction.com e su Twitter(@advanction).

## Risorse

| | |
|---|---|
| Social Engineering: | https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201411_it.pdf |
| Il Phishing: | https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201512_it.pdf |
| Il Malware: | https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_it.pdf |
| La verifica in due passaggi: | https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_it.pdf |



Direzione editoriale: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley