Pubblicazioni
"Quaderni dell' ISEA"

percorsi di informazione e
di educazione ambientale

PHISHING

NON FACCIAMOCI PESCARE DAI TRUFFATORI

ISEA Onlus
volontari per passione

ISEA Onlus
volontari per passione
VALORIZZAZIONE
DELLA NATURA E DELL'AMBIENTE

COS'E' IL PHISHING

Il phishing è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

ISEA Onlus
volontari per passione

Pubblicazioni
"Quaderni dell' ISEA"

percorsi di informazione e
di educazione ambientale

PHISHING



ISEA Onlus
volontari per passione

COS'E' IL PHISHING

Si tratta di un'attività illegale che sfrutta una tecnica di ingegneria sociale: il malintenzionato effettua un invio massivo di messaggi che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi; tali messaggi fraudolenti richiedono di fornire informazioni riservate come, ad esempio, il numero della carta di credito o la password per accedere ad un determinato servizio. Per la maggior parte è una truffa perpetrata usando messaggi di posta elettronica, ma non mancano casi simili che sfruttano altri mezzi, quali i messaggi

ISEA Onlus
volontari per passione

COS'E' IL PHISHING

Il phishing è una minaccia attuale, il rischio è ancora maggiore nei social media come Facebook, Twitter, e Google+. Degli hacker potrebbero infatti creare un clone del sito e chiedere all'utente di inserire le sue informazioni personali. Gli hacker comunemente traggono vantaggio dal fatto che questi siti vengono utilizzati a casa, al lavoro e nei luoghi pubblici per ottenere le informazioni personali o aziendali.

ISEA Onlus

volontari per passione

COS'E' IL PHISHING

Il termine phishing è una variante di *fishing* (letteralmente "pescare" in lingua inglese), probabilmente influenzato da *phreaking* e allude all'uso di tecniche sempre più sofisticate per "pescare" dati finanziari e password di un utente. La parola può anche essere collegata al linguaggio leet, nel quale la lettera f è comunemente sostituita con ph. La teoria popolare è che si tratti di un portmanteau di *password harvesting*, è un esempio di pseudoetimologia.

ISEA Onlus
volontari per passione

COS'E' IL PHISHING

Secondo un'indagine realizzata nel 2019, solo il 17,93 per cento degli intervistati sarebbe in grado di identificare tutti i diversi tipi di phishing (tra cui email o sms contenenti link malevoli o siti web che replicano delle pagine legittime).

ISEA Onlus
volontari per passione

METODOLOGIA GENERALE DI ATTACCO

Il processo standard delle metodologie di attacco di *phishing* può riassumersi nelle seguenti fasi:

- **l'utente malintenzionato (*phisher*) spedisce a un utente un messaggio email che simula, nella grafica e nel contenuto, quello di una istituzione nota al destinatario (per esempio la sua banca, il suo provider web, un sito di aste online a cui è iscritto)**

ISEA Onlus
volontari per passione

METODOLOGIA GENERALE DI ATTACCO

Il processo standard delle metodologie di attacco di *phishing* può riassumersi nelle seguenti fasi:

- **l'e-mail contiene quasi sempre avvisi di *particolari situazioni o problemi* verificatesi con il proprio conto corrente/account (ad esempio un addebito enorme, la scadenza dell'account, ecc.) oppure un'offerta di denaro**

ISEA Onlus
volontari per passione

METODOLOGIA GENERALE DI ATTACCO

Il processo standard delle metodologie di attacco di *phishing* può riassumersi nelle seguenti fasi:

- **l'e-mail invita il destinatario a seguire un link, presente nel messaggio, per evitare l'addebito e/o per regolarizzare la sua posizione con l'ente o la società di cui il messaggio simula la grafica e l'impostazione (Fake login)**

ISEA Onlus
volontari per passione

METODOLOGIA GENERALE DI ATTACCO

Il processo standard delle metodologie di attacco di *phishing* può riassumersi nelle seguenti fasi:

- **il link fornito, tuttavia, *non* porta in realtà al sito web ufficiale, ma a una *copia fittizia* apparentemente simile al sito ufficiale, situata su un server controllato dal phisher, allo scopo di richiedere e ottenere dal destinatario dati personali particolari, normalmente con la scusa di una conferma o la necessità di effettuare una autenticazione al sistema; queste informazioni vengono memorizzate dal server gestito dal phisher e quindi finiscono nelle mani del malintenzionato**

ISEA Onlus
volontari per passione

METODOLOGIA GENERALE DI ATTACCO

Talora, l'e-mail contiene l'invito a cogliere una nuova "opportunità di lavoro" (quale operatore finanziario o *financial manager*), consistente nel fornire le coordinate bancarie del proprio conto online per ricevere l'accredito di somme che vanno poi ri-trasferite all'estero tramite sistemi di *money trasfert* (Western Union o Money Gram), trattenendo una percentuale dell'importo, che può arrivare a cifre molto alte. In realtà si tratta del denaro rubato con il *phishing*, per il quale il titolare del conto online beneficiario, spesso in buona fede, commette il reato di riciclaggio di denaro sporco.

ISEA Onlus
volontari per passione

METODOLOGIA GENERALE DI ATTACCO

Quest'attività comporta per il *phisher* la perdita di una certa percentuale di quanto è riuscito a sottrarre, ma esiste comunque un interesse a disperdere il denaro sottratto in molti conti correnti e a fare ritrasferimenti in differenti Paesi, perché così diviene più difficile risalire alla identità del criminale informatico e ricostruire compiutamente il meccanismo illecito. Peraltro, se i trasferimenti coinvolgono più Paesi, i tempi per la ricostruzione dei movimenti bancari si allungano, poiché spesso serve una rogatoria e l'apertura di un procedimento presso la magistratura locale di ogni Paese interessato.

ISEA Onlus
volontari per passione

Pubblicazioni
"Quaderni dell' ISEA"

percorsi di informazione e
di educazione ambientale

PHISHING



ISEA Onlus
volontari per passione

LISTA DEI TIPI DI PHISHING

PHISHING

Il phishing è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ottenere informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

ISEA Onlus
volontari per passione

LISTA DEI TIPI DI PHISHING

SPEAR PHISHING

Un attacco mirato verso un individuo o una compagnia è stato denominato spear phishing.
Gli attaccanti potrebbero cercare informazioni sull'obbiettivo per poter incrementare le probabilità di successo. Questa tecnica è, alla lunga, la più diffusa su internet, con una quota del 91% degli attacchi.

ISEA Onlus
volontari per passione

LISTA DEI TIPI DI PHISHING

CLONE PHISHING

Di recente molti attacchi di phishing sono stati indirizzati verso figure di spicco di aziende o enti e il termine whaling è stato coniato per questi tipi di attacco.
Viene mascherata una mail/pagina web con lo scopo di ottenere delle credenziali di un manager. Il contenuto è creato su misura per l'obbiettivo, è spesso scritto come un problema amministrativo o una lamentela di un cliente.
Sono state utilizzate anche mail identiche a quelle dell'FBI cercando di forzare il ricevente a scaricare e installare del software.

ISEA Onlus
volontari per passione

LISTA DEI TIPI DI PHISHING

WHALING

È un tipo di phishing in cui una mail legittima viene modificata negli allegati o nei link e rimandata ai riceventi, dichiarando di essere una versione aggiornata.
Le parti modificate della mail sono volte a ingannare il ricevente. Questo attacco sfrutta la fiducia che si ha nel riconoscere una mail precedentemente ricevuta.

ISEA Onlus
volontari per passione

MANIPOLAZIONE DEI LINK

La maggior parte dei metodi di phishing usa degli exploit tecnici per far apparire i link nelle mail come quelli autentici.
Altri trucchetti diffusi sono utilizzare URL scritte male, oppure usando sottodomini ad esempio

http://www.tuabanca.it.esempio.com

può sembrare a prima vista un sito legittimo, ma in realtà sta puntando a un sottodominio di un altro sito. Un'altra metodologia è registrare un dominio lavorando su lettere visivamente simili.

ISEA Onlus
volontari per passione

AGGIRAMENTO DEI FILTRI

I phisher hanno iniziato, col tempo, a mascherare il testo inserendolo in immagini, in questo modo i filtri anti-phishing hanno più difficoltà nell'identificazione delle minacce.
Questo ha portato sull'altro lato a una evoluzione dei filtri, ora capaci di trovare testo in immagini.
Questi filtri usano OCR (riconoscimento ottico dei caratteri).

ISEA Onlus
volontari per passione

CONTRAFFAZIONE DI UN SITO WEB

Quando una vittima visita un sito di phishing l'attacco non è terminato. Nella pagina possono essere infatti presenti comandi JavaScript per alterare la barra degli indirizzi.
Può essere fatto o mettendo un'immagine nella barra degli indirizzi o chiudendo la finestra e aprendone una nuova con l'indirizzo legittimo.

ISEA Onlus
volontari per passione

CONTRAFFAZIONE DI UN SITO WEB

Un attaccante può anche usare vulnerabilità in un sito fidato e inserire i suoi script malevoli.
Questi tipi di attacco, conosciuti come cross-site scripting sono particolarmente problematici perché tutto sembra legittimo, compresi i certificati di sicurezza. In realtà tutto è fatto ad hoc per portare a termine l'attacco, rendendolo molto difficile da individuare senza conoscenze specialistiche.

ISEA Onlus
volontari per passione

PHISHING TELEFONICO

Non sempre il phishing implica l'utilizzo di un sito web o di mail, vengono infatti inviati messaggi sms agli utenti, che dicono che ci siano stati dei problemi con i loro account bancari.
Quando il numero indicato (gestito dal phisher, di solito si tratta di un numero Voice over IP) nel messaggio viene chiamato viene chiesto all'utente il proprio PIN. Il Vishing (voice phishing) qualche volta utilizza un finto numero di chiamante, in modo da dare l'apparenza di un'organizzazione fidata.
In alcuni casi il phisher cerca di ottenere in maniera fraudolenta tramite WhatsApp, non dati finanziari o codici pin, ma copie di documenti d'identità che utilizzerà poi per successive truffe.

ISEA Onlus
volontari per passione

COME PREVENIRE IL PHISHING

1

- Fai attenzione alle spam.
- Non rispondere alle email che ti chiedono informazioni finanziarie, anche se sembrano provenire da un mittente affidabile.
- Non rispondere alle email provenienti da mittenti sconosciuti.
- I tentativi di phishing non sono personalizzati.
- Non cliccare sui links inviati all'interno di email sospette, messaggi istantanei o messaggi in chat.

ISEA Onlus

volontari per passione

COME PREVENIRE IL PHISHING

2

- Comunica le tue informazioni personali soltanto al telefono o attraverso un sito internet affidabile.
- I siti internet certificati sono riconoscibili grazie ad un lucchetto che appare sulla barra di stato del browser o grazie al prefisso "Https://" al posto di Http://.
- E' il caso di comunicare informazioni personali al telefono solo se la chiamata effettuata è diretta ad un numero affidabile. Per esempio, è meglio telefonare al numero della banca che trovi sull'estratto conto, piuttosto che uno riportato in una email , in cui ti si chiede di farlo.

ISEA Onlus
volontari per passione

COME PREVENIRE IL PHISHING

3

- Non utilizzare mai la posta elettronica per comunicare informazioni personali. Anche se conosci i destinatari di una email, qualcuno potrebbe accedere senza autorizzazione al tuo account o a quello di qualche altro destinatario.
- Qualcuno in possesso di abilità tecniche avanzate potrebbe intercettare la tua email.

ISEA Onlus
volontari per passione

COME PREVENIRE IL PHISHING

4

Evita di utilizzare la posta elettronica da computer pubblici.
Le informazioni contenute in una email sono temporaneamente memorizzate nel local disk del computer utilizzato e potrebbero essere recuperate da un altro utente, se non cancellate a dovere.

ISEA Onlus
volontari per passione

COME PREVENIRE IL PHISHING

5

- Non cliccare in nessun punto delle finestre pop-up.
- Se il tuo browser ti permette ti bloccare le finestre pop-up, fallo.
- Non copiare nel tuo browser nessun indirizzo proveniente da una finestra pop-up.
- Un'azienda seria non ti chiederà mai di inserire informazioni in una finestra pop-up.

ISEA Onlus
volontari per passione

COME PREVENIRE IL PHISHING

6

- Proteggi il tuo computer utilizzando dei programmi per la sicurezza.
- Usa un filtro per le spam, un programma anti-spyware, un anti-virus ed un firewall. Potrai trovarli da un rivenditore di software o su internet.

ISEA Onlus
volontari per passione

COME PREVENIRE IL PHISHING

7

- ❑ Controlla regolarmente il tuo saldo e l'estratto conto.
- ❑ Assicurati che non sia presente nessuna transazione non autorizzata e che nel saldo tutte le voci risultino corrette.

ISEA Onlus
volontari per passione

CONSIGLI UTILI

- Se pensi di essere vittima di phishing, rivolgiti alla Polizia Postale.
- Se pensi di essere stato raggirato attraverso il phishing, rivolgiti all'istituzione che il truffatore ha simulato di essere all'interno della comunicazione.
- Non cliccare su links contenuti in email fraudolente, poiché potrebbero collegarti a siti internet poco raccomandabili.

ISEA Onlus
volontari per passione

GRAZIE PER L'ATTENZIONE

ISEA Onlus
volontari per passione

ISEA Onlus
volontari per passione
VALORIZZAZIONE
DELLA NATURA E DELL'AMBIENTE