L'APPRENDIMENTO ESPERIENZIALE PER RIDURRE IL RISCHIO PHISHING

WHITE PAPER

CyberGuru

EXECUTIVE SUMMARY

L' e-mail phishing (da ora in poi phishing) è al momento la più pericolosa tecnica di attacco utilizzata dal Cyber Crime per penetrare le difese tecnologiche predisposte dalle organizzazioni e in modo particolare dai loro team di Cyber Security.
Esistono varie forme di phishing, ma la tendenza crescente è quella di sviluppare attacchi sempre più sofisticati e personalizzati (spear phishing) che esercitano sul destinatario una sorta di manipolazione psicologica, che lo induce a diventare un complice inconsapevole dell'attacco Cyber.

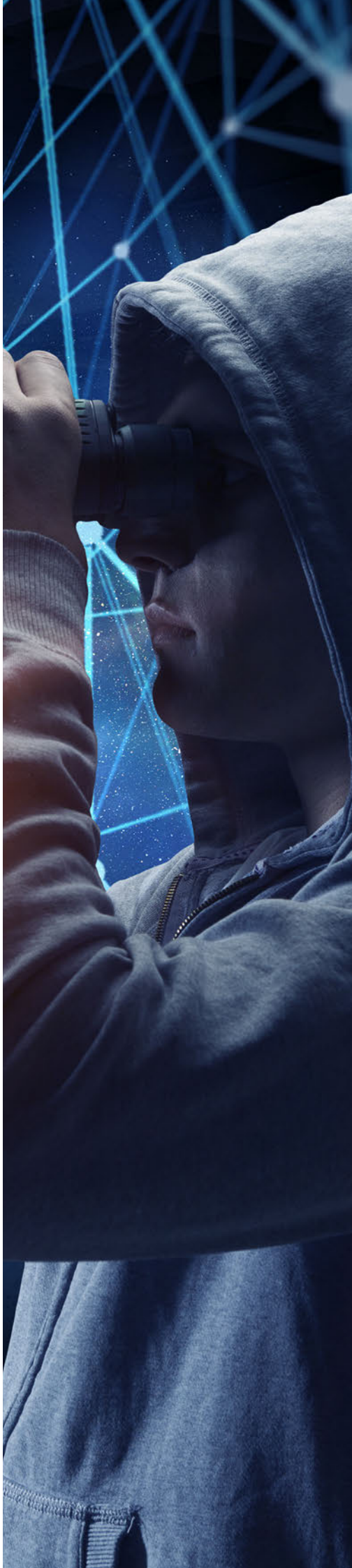
Tutte le statistiche che riguardano gli attacchi Cyber, evidenziano la crescita di questa tecnica. Non si tratta di una crescita solo di tipo quantitativo, ma anche di tipo qualitativo. Il livello di sofisticazione raggiunto dagli attacchi phishing, soprattutto in associazione con strategie avanzate di social engineering (ingegneria sociale), espone chiunque al rischio di diventare vittima di questa tecnica di attacco, paradossalmente anche persone preparate a fronteggiare i rischi Cyber.

AGIRE È FONDAMENTALE

Per contrastare questo fenomeno che sta assumendo proporzioni molto preoccupanti è fondamentale agire, e soprattutto agire a più livelli.

Oltre all'approccio di tipo tecnologico, è necessario agire sul "**fattore umano**", aumentando il livello di consapevolezza di tutti gli utenti rispetto al rischio phishing e alle diverse forme che questo può assumere, con un programma efficace di Cyber Security Awareness.

Per fare fronte a questa nuova emergenza non è sufficiente sviluppare processi di apprendimento sulle tecniche di phishing, agendo solo sulla sfera cognitiva, ma è indispensabile agire anche sulla sfera "istintuale", addestrando le principali caratteristiche umane difensive, come la **prontezza** e la **reattività**.



L'obiettivo è quello di creare al contempo utenti consapevoli, in grado di riconoscere il pericolo sulla base di alcune precise caratteristiche, e utenti pronti e reattivi, in grado di percepire il pericolo e di adeguare i loro comportamenti rispetto a questa percezione.

APPRENDIMENTO COGNITIVO E ESPERIENZIALE

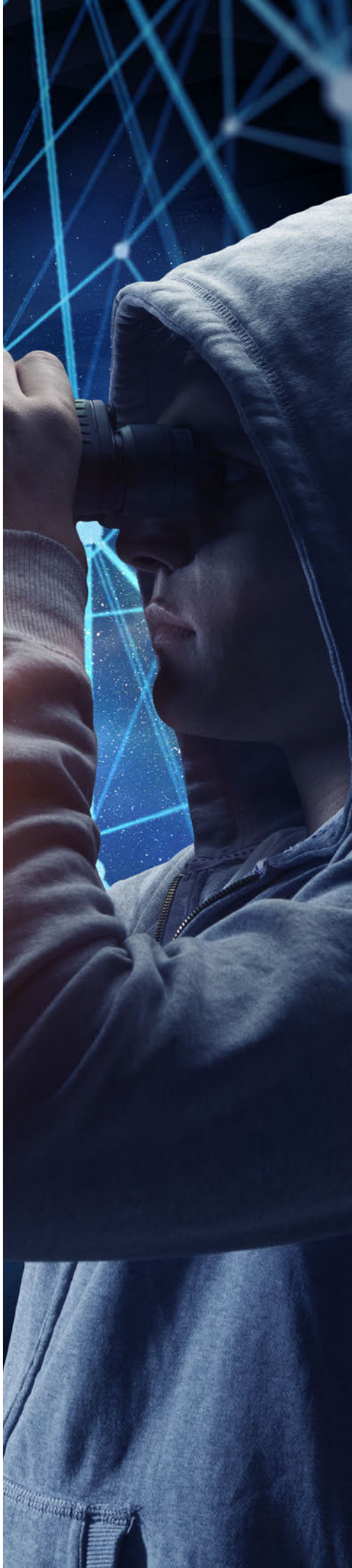
Basato su un concetto di formazione continua e di addestramento, l'apprendimento cognitivo ed esperienziale rappresenta la nuova frontiera della lotta al Cyber Crime, perché in grado di trasformare gli utenti da anello debole della catena a prima linea di difesa.

Eppure, fino ad'ora, la risposta più comune in funzione anti-phishing che le organizzazioni hanno adottato in questi anni, è stata costituita soprattutto dalle piattaforme di simulazione in grado di effettuare campagne di ethical phishing.

Questa attività è stata usata principalmente per determinare un ipotetico rischio phishing, associandolo in modo "improprio" al click rate (tasso di click). Si tratta di piattaforme che presentano dei limiti strutturali, che non consentono di sviluppare programmi efficaci di apprendimento esperienziale e che forniscono una valutazione del rischio phishing a dir poco approssimativa.

Questi limiti vengono superati da Cyber Guru Phishing, una piattaforma avanzata e innovativa che, sfruttando automazione, intelligenza artificiale, machine learning e reportistica avanzata riesce a portare avanti programmi efficaci di apprendimento esperienziale.

Cyber Guru Phishing è l'unica piattaforma di simulazione in funzione anti-phishing completamente autonoma, che consente quindi di ottenere un risultato efficace senza impatti sui team di Cyber Security.



SOMMARIO

IL PHISHING

COME SI CONCRETIZZA UN'ATTACCO PHISHING?

I criminali Cyber spediscono dei messaggi dal contenuto ingannevole e invitano il destinatario a compiere un'azione, generando in lui la prospettiva di ottenere un vantaggio o semplicemente di evitare una situazione spiacevole. Se il destinatario cade nella trappola e quindi esegue l'azione richiesta, i criminali ottengono un vantaggio fraudolento, provocando un danno al destinatario o alla sua organizzazione.

Le loro probabilità di successo dipenderanno da due fattori contrastanti:
.

- la capacità del messaggio di essere al contempo attrattivo e credibile nei confronti del destinatario, tanto da spingerlo ad eseguire l'azione richiesta;

- la capacità del destinatario di riconoscere l'intenzione fraudolenta del messaggio evitando quindi di eseguire l'azione richiesta.

Con messaggio ci riferiamo a qualsiasi mezzo digitale in grado di scambiare messaggi, anche se l'email resta il veicolo principale di diffusione degli attacchi phishing.

Per questa ragione il termine phishing viene associato specificatamente all'e-mail phishing, mentre per gli attacchi che vengono realizzati con altri canali sono stati coniati nuovi termini come ad esempio smishing o vishing.

COS'È' E COME FUNZIONA

Il phishing è la più comune tecnica di attacco utilizzata dai criminali Cyber: la maggior parte delle truffe informatiche sono realizzate attraverso questa modalità, che è in continua crescita.

Ha l'obiettivo di ottenere un vantaggio indebito, sfruttando la collaborazione involontaria e inconsapevole dell'utente finale.

Può provocare danni a individui e organizzazioni, ma il target diretto dell'attacco è sempre di carattere individuale.

e-mail phishing

OBIETTIVI DI UN ATTACCO PHISHING

Gli obiettivi principali di un attacco phishing e quindi la conseguenza primaria dell'azione eseguita dall'utente sono:

- infettare i dispositivi della vittima, e di conseguenza della sua organizzazione, tramite un malware, con lo scopo diretto di provocare un danno, oppure con lo scopo indiretto di ottenere informazioni critiche, per poi usarle come base di altri attacchi successivi;

- ottenere informazioni sensibili in modo diretto, spesso credenziali di accesso, indirizzando la vittima su false pagine web;

- effettuare una truffa in forma diretta, spingendo la vittima ad effettuare un acquisto, un pagamento, oppure a rilevare dati che riguardano un mezzo di pagamento.

Sono tutte forme di attacco che possono risultare particolarmente dannose per la vittima o per la sua organizzazione di riferimento.

TIPOLOGIE DI ATTACCO PHISHING

Tra le diverse classificazioni, una si basa sul contenuto del messaggio di phishing:

- **Spray Phishing** – è la tecnica più comune, di tipo massivo e quindi poco sofisticata. Si sfruttano i numeri, le quantità. Tante mail inviate a tanti utenti, nella speranza che, anche a livello probabilistico, il contenuto della e-mail diventi attrattivo, accattivante e credibile nei confronti di qualche destinatario. I messaggi "spray" sono realizzati in fretta, senza troppa cura e sono spesso il frutto di cattive traduzioni. Normalmente ad una lettura attenta del contenuto si trovano molti indizi che ne rilevano l'intenzione malevola.

  La tipica vittima di questo tipo di attacco è solitamente un utente inconsapevole e comunque distratto.

Attacco phishing

- **Spear Phishing** – è una tecnica più sofisticata perché molto diretta. Il contenuto del messaggio non è generico, ma costruito ad-hoc per un utente o per una determinata categoria di utenti. Si tratta di messaggi molto elaborati, spesso perfetti nella logica e nella sintassi, costruiti con una buona conoscenza del target e quindi con informazioni molto puntuali. Nessuno può considerarsi completamente al sicuro con questa tecnica e le uniche armi di difesa sono rappresentate dalla consapevolezza e dalla prontezza dell'utente, caratteristiche umane che approfondiremo successivamente.

Nel caso dello spear phishing abbiamo fatto riferimento alla conoscenza che il criminale ha del target, necessaria a confezionare messaggi in grado di attirare l'attenzione e apparire credibili, al punto da spingere la potenziale vittima a compiere l'azione richiesta. È in questa fase che il phishing si incrocia con il social engineering, o ingegneria sociale, una strategia articolata che usa l'inganno e la manipolazione psicologica per far scattare la trappola intorno alla potenziale vittima.

Da quanto esposto dovrebbe risultare evidente che con lo spear phishing, le tecniche di attacco sono diventate molto più sofisticate e quindi più difficili da riconoscere, e che per questo nessuno, anche individui con competenze avanzate, può sentirsi al riparo da questi attacchi.

IL SOCIAL ENGINEERING

Il social engineering prevede una fase informativa molto accurata, necessaria ad acquisire informazioni sul target come base fondante di tutta la strategia offensiva. Più informazioni verranno collezionate sul target, maggiori saranno le probabilità che l'attacco vada a buon fine. Per questa ragione, è probabile che l'attacco vero e proprio, quello in grado di produrre maggiori vantaggi per il criminale cyber e maggiori danni all'organizzazione target, verrà preceduto da attacchi necessari a supportare la fase informativa.
Informazioni sul target si possono ottenere sia attraverso l'uso di Malware, sia attraverso accessi fraudolenti al sistema target, magari con credenziali ottenute attraverso un precedente attacco phishing, oppure spingendo la vittima, con l'inganno, a rivelare informazioni sensibili.

La fase informativa viene spesso favorita dalla tendenza ormai prevalente da parte di individui e organizzazioni a comunicare informazioni usando i canali digitali, tra cui gli strumenti social. La comunicazione digitale rappresenta quindi un'esigenza e un'opportunità, ma implica anche un rischio Cyber.

Social engineering

LA TRUFFA DEL CEO

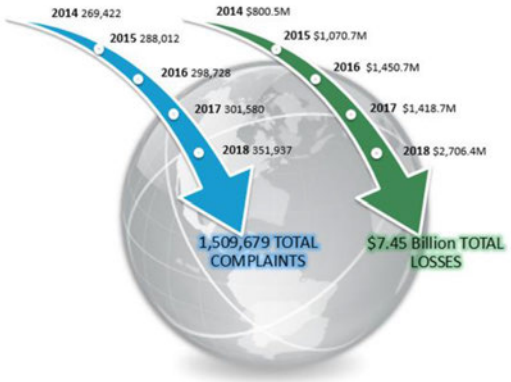
Esiste oggi una particolare strategia di attacco chiamata Business E-mail Compromise (BEC) oppure, in termini figurati, “La truffa del CEO”. Si tratta di una truffa online, sempre più efficace e sempre più diffusa, che provoca un danno economico, anche molto elevato, per l'organizzazione che la subisce.

Il truffatore induce un dipendente dell'organizzazione, a compiere un'azione, in risposta a una richiesta che arriva apparentemente da una figura apicale della stessa organizzazione.
L'azione consiste tipicamente in un pagamento in denaro oppure nella comunicazione di informazioni sensibili, a vantaggio di un'organizzazione criminale. Negli ultimi tempi la cronaca ha messo in luce la vicenda di una multinazionale dove si è proceduto addirittura all’acquisto di una società “fantasma” proprio sulla base di comunicazioni compromesse tra le diverse sedi.
Importante sottolineare che la truffa colpisce indifferentemente le grandi organizzazioni e le piccole e medie imprese. Nella maggior parte dei casi questa truffa viene innescata da una compromissione della casella e-mail di una figura apicale. In questo modo i criminali cyber riescono ad acquisire sufficienti informazioni sull’organizzazione target per poter innescare la trappola, inviando email che appariranno molto credibili.

Lavorando sulla consapevolezza degli utenti si può rafforzare la capacità di resistere agli attacchi phishing, ma per ridurre il rischio sarà necessario anche agire sull’attitudine delle persone a percepire la minaccia, addestrando caratteristiche umane come la prontezza e la reattività.

PERDITE FINANZIARIE

Dall'ultimo Internet Crime Report dell'FBI emerge con chiarezza che il numero e il valore delle perdite subite a causa delle truffe su internet continua a crescere in maniera esponenziale.



Internet Crime Report

In particolare la più grande perdita finanziaria deriva dalle truffe di Business E-mail Compromise e di compromissione dell'account e-mail.

Nell'ultimo anno sono state **20.373 *le vittime*** di questa tipologia di truffa per un totale **1.298 *miliardi di dollari*** persi.

La truffa del CEO

IL FENOMENO PHISHING NEI NUMERI

Il fenomeno Phishing sta assumendo proporzioni drammatiche.

Tutte le statistiche concordano: la maggior parte delle violazioni è riconducibile ad un'azione impropria effettuata da un utente a fronte di una e-mail di phishing. Il vero nemico delle organizzazioni si nasconde nelle caselle e-mail dei propri dipendenti e collaboratori.

Spesso l'e-mail fraudolenta e la conseguente azione dell'utente che l'ha ricevuta, rappresentano solo l'innesco di una strategia di attacco che poi si realizza attraverso l'uso di malware oppure attraverso l'uso delle informazioni sottratte "con destrezza" all'utente stesso.

Ci sono dati oggettivi che forniscono un quadro "preoccupante" del livello raggiunto dal fenomeno phishing.

Utilizzando ad esempio il **Verizon Data Breach Report del 2018** arriviamo a determinare che almeno l'***80% dei "data breach" possono essere ricondotti ad un attacco phishing.***

Per **SANS Institute**, il ***95% degli attacchi di livello Enterprise hanno utilizzato il phishing come primo vettore di attacco.***

Al di là dei dettagli e delle piccole differenze riscontrabili nei diversi report, possiamo stabilire con certezza che il phishing è il principale vettore di attacco utilizzato per fare breccia nella struttura difensiva.

FORME ALTERNATIVE DI PHISHING

Esistono delle forme di phishing che utilizzano canali alternativi alla e-mail, come:

- **Smishing:** attacchi effettuati con sms ingannevoli che propongono un link malevolo a cui accedere.
- **Vishing:** attacchi effettuati con messaggi ingannevoli, inviati utilizzando sistemi di messaggistica istantanea, come Whatsapp, che propongono un link malevolo a cui accedere.
- **Fake post:** attacchi effettuati con post ingannevoli pubblicati via Web o via canali social, che propongono un link malevolo a cui accedere.
- **Sneaky Phishing:** attacchi effettuati con una tecnica che tende a compromettere il doppio livello di autenticazione, sviluppato proprio per aumentare il livello di sicurezza di sistemi e applicazioni.

Statistiche phishing

Il quadro diventa più preoccupante se, ricorrendo a un dato fornito da **KPMG**, arriviamo a determinare che l'***88% delle organizzazioni ha denunciato di aver subito almeno un attacco phishing nel corso dell'ultimo anno solare (2018).***

Nel rapporto **Clusit 2019** sulla Sicurezza ICT in Italia, si evidenzia come, nel corso del 2018, si sia registrato un aumento degli attacchi gravi, e soprattutto un incremento deciso ***+56% degli attacchi riconducibili al phishing***.

TECNICHE DI ATTACCO PER TIPOLOGIA	2014	2015	2016	2017	2018	2018 su 2017	Trend
Malware	127	106	229	446	585	31,2%	↗
Unknown	199	232	338	277	408	47,3%	↑
Known Vulnerabilities / Misconfig.	195	184	136	127	177	39,4%	↗
Phishing / Social Engineering	4	6	76	102	160	56,9%	↑
Multiple Techniques / APT	60	104	59	63	98	55,6%	↑
Account Cracking	86	91	46	52	56	7,7%	↗
DDoS	81	101	115	38	38	0,0%	-
0-day	8	3	13	12	20	66,7%	↑
Phone Hacking	3	1	3	3	9	200,0%	↑
SQL Injection	110	184	35	7	1	-85,7%	↓

rapporto Clusit 2019 sulla Sicurezza ICT in Italia

Queste statistiche dovrebbero preoccupare ancora di più, perché spesso è difficile risalire fino alla prima causa di una violazione. Ci si ferma all'ultima causa, quella scatenante, associando ad esempio l'attacco al Malware che lo ha generato.

Eppure, come si può ricavare dal rapporto **Verizon**, il ***66% dei Malware viene installato a partire da un allegato ricevuto via e-mail.***

Per fare un esempio, il trojan Emotet, considerato molto pericoloso, è stato diffuso attraverso campagne di e-mail con più di 1 milione di e-mail inviate ogni giorno per tutto il periodo di diffusione.

Phishing
+56,9%

Un altro numero impressionante è quello fornito da Webroot, che ci dice che in un mese vengono creati più di **1 milione e mezzo di falsi siti**, collegati ad attività di e-mail phishing.

I costi connessi a tutte queste azioni fraudolente sono quasi impossibili da calcolare.

Il fenomeno BEC, di cui abbiamo già parlato, produce, secondo l'FBI, quasi 12 milioni di dollari di perdite secche, soldi che non verranno mai recuperati.

Quindi, al di là delle sfumature, tutte le analisi concordano nel classificare il phishing come il principale veicolo di attacco, quello più diffuso, quello che ha maggiori probabilità di successo, e quello che produce più danni in senso assoluto. Questo genera anche normali profili di responsabilità civile e penale per coloro che, in ambito professionale, non siano in grado di dimostrare di aver messo in campo tutte le azioni possibili di contrasto rispetto a questo fenomeno, incluse le attività di formazione rivolte agli utenti dell'organizzazione.

ARGINARE IL FENOMENO PHISHING

Tutte le organizzazioni in questi anni hanno tentato di porre un argine di tipo tecnologico al fenomeno phishing. L'obiettivo è quello di fermare l'e-mail malevola prima che questa raggiunga le caselle e-mail dei propri dipendenti, eliminando il problema alla radice.
Chiaramente, soluzioni di questo tipo si sono rivelate molto utili per ridurre la portata del fenomeno, ma non per fermarne la potenzialità distruttiva.
Di fatto è sufficiente una sola e-mail che riesca ad insinuarsi nell'organizzazione, eludendo i controlli tecnologici, per generare un danno.

Quindi se da una parte è vero che i filtri per la posta indesiderata bloccano grandi quantità di e-mail sospette ogni giorno, è altrettanto vero che ormai tutte le organizzazioni ammettono di aver subito attacchi phishing che non sono state in grado di fermare.

Le organizzazioni criminali continuano ad elaborare tecniche di attacco sempre più sofisticate, in grado di ingannare sia la macchina, e quindi tutti i sistemi di filtraggio, sia l'uomo, nel momento in cui il messaggio raggiunge la sua casella e-mail.
Anche i sistemi di controllo sui link di destinazione e i sistemi antivirus svolgono un'azione significativa, ma limitata rispetto alla portata e alla sofisticazione degli attacchi.

Arginare il phishing

Se si vuole combattere seriamente la battaglia contro il phishing, bisogna **trasformare gli utenti nella prima linea di difesa contro il crimine informatico, con una consistente azione sul "fattore umano".**

Non stiamo dicendo nulla che non sia già noto alle organizzazioni, che hanno adottato o che hanno in progetto di adottare, programmi di **Cyber Security Awareness**. Si prevede che nei prossimi anni, tutte le organizzazioni, grandi e piccole, si saranno incamminate su questa strada.

Sviluppare consapevolezza sui rischi Cyber, alzare il livello di attenzione degli utenti adeguando i loro comportamenti al rischio raggiunto dalla criminalità informatica, è un passaggio obbligato. L'innovazione negli ultimi anni ha viaggiato a ritmi poderosi, mentre la cultura dell'innovazione è rimasta fortemente in ritardo rispetto a questo sviluppo.

Il fattore umano

CYBER SECURITY AWARENESS

LE CARATTERISTICHE DEL PROGRAMMA FORMATIVO

Quindi il primo assunto che ci sentiamo di fare è che per contrastare il phishing è necessario avviare un significativo programma di Cyber Security Awareness, in grado di raggiungere la totalità di dipendenti e collaboratori.
È necessario però declinare alcune caratteristiche di questo programma, perché un programma di Cyber Security Awareness non deve essere solo un modo di "dimostrare", in caso di violazione, di aver fatto di tutto per prevenire questa situazione, ma deve essere un modo per ridurre concretamente il rischio di un attacco Cyber.

Di seguito quattro caratteristiche fondamentali per un programma formativo di Cyber Security Awareness:

- **Efficace** - in grado di incidere efficacemente sui comportamenti della popolazione aziendale, adeguandoli al livello raggiunto dalla minaccia Cyber. Questo comporta la capacità di "ingaggiare" i partecipanti e motivarli a partecipare, superando i limiti storici della formazione in ambito aziendale.

- **Aperto a tutti** – in grado di raggiungere tutta la popolazione aziendale, indipendentemente dal ruolo ricoperto all'interno dell'organizzazione. Questo comporta una particolare attenzione al linguaggio, che deve essere divulgativo e lontano da ogni ortodossia tecnologica.

- **Continuo** – in grado di mantenere elevato nel tempo il livello di attenzione sulle minacce Cyber. Questo comporta un programma di lunga durata che si rinnova costantemente seguendo l'evoluzione delle tecniche di attacco.

- **Compatibile** – in grado di avere un impatto minimo sui tempi e sugli impegni professionali. Quindi con un approccio diluito nel tempo e l'erogazione di pillole formative brevi.

Security Awareness

Come abbiamo già affermato, agire sulla consapevolezza in modo efficace è necessario ma non sufficiente nei confronti del fenomeno phishing. Oltre alla sfera cognitiva è importante agire anche sulla **sfera istintuale**, allenando prontezza e reattività dell'individuo.

Il livello di sofisticazione raggiunto dagli attacchi phishing, soprattutto nelle situazioni di spear phishing e nella combinazione di questa modalità di attacco con le strategie di social engineering, impone di andare oltre la sfera cognitiva. La manipolazione psicologica, il senso di pressione e urgenza, tipico delle comunicazioni aziendali è riprodotto abilmente nelle e-mail di phishing. Il numero elevato di e-mail e di sollecitazioni ricevute dagli utenti creano una condizione che porta spesso ad agire di impulso, senza mettere in campo tutti quei controlli che vengono suggeriti nei corsi di Cyber Security Awareness.

Inoltre una volta che viene compromessa l'integrità del sistema e-mail di un'organizzazione, come nella BEC, tutti i segnali "razionali" che aiutano a riconoscere un'attività fraudolenta risultano altrettanto compromessi e quindi diventa molto difficile individuare il tentativo di phishing. Del resto, è sufficiente un momento di distrazione per cadere nella trappola ordita dalle organizzazioni criminali, diventando una vittima del Cyber Crime.

Per questa ragione è assolutamente necessario sviluppare negli utenti un'attitudine, una sorta di propensione "naturale" a riconoscere il pericolo. Tutti gli uomini sono abituati a riconoscere rischi e pericoli nella realtà circostante, anche senza una specifica formazione, solo attraverso un **addestramento di tipo esperienziale**.

CYBER SECURITY AWARENESS

Per quanto riguarda la questione della Cyber Security Awareness, che chiaramente non è riferita solamente al fenomeno phishing, ma a tutte le tipologie di minacce Cyber, vi invitiamo a fare riferimento al nostro White Paper dedicato.

Sfera istintuale

PRONTEZZA E REATTIVITÀ'

Agire sulla competenza significa agire sulla sfera cognitiva, e quindi significa formare gli utenti a riconoscere i principali indizi di un attacco phishing, prestando attenzione alle e-mail ricevute.
Tre elementi risultano decisivi in questo processo: ***il mittente, il contenuto della mail, il link di destinazione***.

- Fare attenzione al ***mittente*** significa verificare che il mittente reale corrisponda o meno a quello apparente o comunque a quello atteso. Ma questa raccomandazione non funziona nel caso della BEC, ossia in caso di compromissione della casella e-mail, perché questo significa che il messaggio fasullo arriva proprio dalla casella e-mail della figura apicale dell'organizzazione, anche se non è stato inviato da questa.

- Fare attenzione al ***contenuto*** significa ricercare errori semantici oppure ortografici che mettano in evidenza la scarsa credibilità dello stesso. Ma questa raccomandazione rischia di non essere valida nei casi più sofisticati di spear phishing, specialmente se supportati da attività di social engineering. Il contenuto in questi casi è molto preciso e puntuale e per questo molto credibile.

- Fare attenzione al ***link di destinazione*** significa verificare l'aderenza tra il link apparente e quello reale e valutare l'appropriatezza e l'affidabilità della destinazione finale. In questo caso il controllo non è propriamente banale e spesso la sofisticazione dell'inganno tende a rendere la valutazione dell'utente ancora più complessa.

Acquisire consapevolezza attraverso un percorso efficace di apprendimento è quindi una strategia necessaria ma non sufficiente, e andrà sostenuta con un'attività di addestramento che vada oltre la sfera "razionale", ma che faccia leva su caratteristiche umane come la prontezza e la reattività per mettere "in guardia" il destinatario, facendo insorgere in lui un "sospetto" quasi istintivo rispetto ad eventuali e-mail malevole.

Caratteristiche umane che necessitano di essere allenate costantemente con un programma specifico di training.

Prontezza e reattività

APPRENDIMENTO ESPERIENZIALE

Nel caso dell'addestramento anti-phishing, il soggetto deve essere esposto ad attacchi regolari, così da allenarlo ad affrontare situazioni a rischio, sviluppando comportamenti adattivi.
Chiaramente il percorso esperienziale dovrà essere personalizzato sulla base della specifica attitudine di ogni soggetto rispetto al rischio phishing, un'attitudine che sarà condizionata da numerosi fattori, come ad esempio: la consapevolezza iniziale, il ruolo aziendale ricoperto, il tipo di dispositivo utilizzato [...].

È chiaro che per raggiungere questo livello di personalizzazione sarà necessario utilizzare una piattaforma avanzata che implementi un approccio adattivo basato su automazione, intelligenza artificiale e machine learning.

IL LIMITE DELL'ETHICAL PHISHING

In assenza di una piattaforma così evoluta, la risposta che le organizzazioni hanno adottato negli ultimi anni è risultata molto limitata rispetto alle sovraesposte necessità di un percorso di apprendimento esperienziale. In generale tutte le organizzazioni hanno utilizzato piattaforme di simulazione in grado di effettuare delle campagne periodiche di "ethical phishing", che consistono nell'invio di una e-mail ingannevole che produce l'effetto di un attacco simulato.

Spesso queste campagne vengono collegate a contenuti formativi che vengono effettuati dall'utente che cade nell'inganno. La loro finalità primaria consiste normalmente in una presunta misurazione del livello di rischio phishing, con un'identificazione quasi univoca del rischio con il "click rate", ossia il tasso di click riscontrato alla fine di queste campagne.

Per essere ancora più chiari, con il click rate si determina quanti utenti hanno cliccato sul link malevolo contenuto nella e-mail di simulazione, rispetto al numero di e-mail inviate. Se vengono inviate 100 mail e vengono riscontrati 25 click, il click rate si attesta appunto al 25%, dato che viene assunto al pari del rischio phishing. Il riferimento al 25% non è casuale, perché statisticamente il click rate di questo tipo di attività si attesta tra il 20% e il 30%.

Percorso esperienzale

Queste attività come abbiamo detto presentano alcuni limiti evidenti sia rispetto all'obiettivo per cui nella maggior parte dei casi vengono effettuate, ossia una mera valutazione del rischio phishing, sia rispetto ad un obiettivo più ambizioso di riduzione del rischio phishing.
Vediamo di comprendere meglio i limiti dell'Ethical Phishing:

- **1) IMPATTO SIGNIFICATIVO SUI TEAM DI CYBER SECURITY**

  Il primo limite è che si tratta normalmente di piattaforme che richiedono una grande sforzo in termini di configurazione (gestione delle liste utenti, approntamento dei template, esecuzione e interpretazione dei risultati [...]), cosa che ne limita fortemente l'utilizzo, soprattutto nelle grandi organizzazioni. Proprio per questa ragione, in una grande organizzazione, si procede normalmente ad effettuare una o due campagne l'anno e su un campione ridotto di utenti. E' evidente che con queste frequenze non si può sviluppare alcun programma di apprendimento esperienziale, che necessita di un'esposizione al rischio ricorrente.

- **2) INTERPRETAZIONE DEI RISULTATI OTTENUTI**

  Il secondo limite è legato all'interpretazione dei risultati ottenuti, sostanzialmente sotto due punti di vista:

  1. Valutazione del rischio phishing, perché l'associazione tra click rate e rischio phishing è fondamentalmente arbitraria, un'assunzione che non trova riscontro nei fatti.

  2. Difficoltà oggettiva ad andare oltre questo dato, e quindi ad entrare nel dettaglio, facendo ad esempio considerazioni di carattere organizzativo. Ci sono unità organizzative oppure filiali maggiormente a rischio? Sembra una domanda quasi banale a cui fornire una risposta, eppure comporta spesso uno sforzo molto arduo per piattaforme che richiedono grande impegno in termini di configurazione manuale.

  Per quanto riguarda l'associazione tra click rate e rischio phishing bisogna dire che molte piattaforme hanno introdotto un parametro di valutazione della difficoltà dell'attacco inviato. È infatti normale che il click rate sia fortemente influenzato dal template utilizzato per l'attacco.

Ethical Phishing

Una mail molto sofisticata, che tratta temi di elevata sensibilità rispetto all'organizzazione, avrà maggiori probabilità di ingannare il destinatario, rispetto a una mail generica che contiene degli errori ortografici.
Per cui è necessario definire un coefficiente di difficoltà per rendere più credibile la valutazione del rischio phishing. Il problema consiste proprio nella definizione di questo coefficiente, che nella maggior parte dei casi viene attribuito in modo empirico, secondo una valutazione basata su parametri generali e non su un riscontro oggettivo.

Ogni organizzazione è un'entità a sé stante e quindi reagisce in modo diverso ad un template rispetto a qualsiasi altra organizzazione.

Questo aspetto diventa ancora più complesso se ci si riferisce alle diverse articolazioni organizzative che ci sono all'interno di una stessa organizzazione.

Quindi, l'unico modo per attribuire un coefficiente di difficoltà ad un template è quello di osservare i risultati che ogni singolo template produce all'interno di quell'organizzazione e delle singole unità organizzative, tenendo conto anche di parametri più generali, come il settore verticale di appartenenza e la complessità organizzativa. Da qui l'esigenza di "apprendere" dai dati registrati "sul campo".

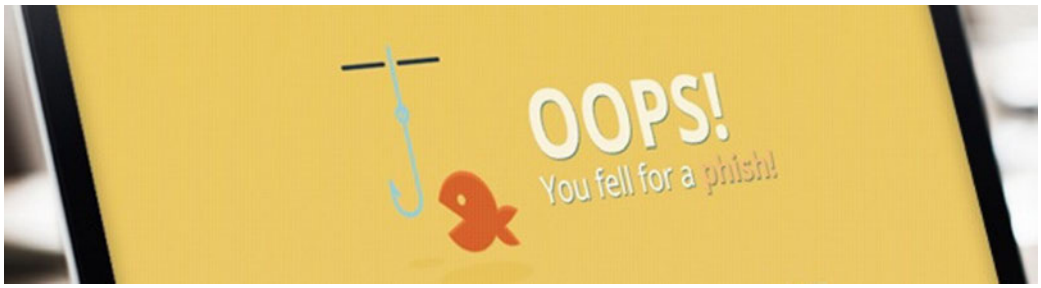
- **3) EFFETTO PASSAPAROLA**

Il terzo limite è legato al fenomeno del "passaparola". Queste campagne vengono spesso inviate in modo "massivo" utilizzando un unico template o comunque un numero limitato di essi. Questo significa che l'affidabilità della rilevazione si riduce sistematicamente nel tempo. La maggiore efficacia e quindi il click rate più elevato si registra nei primi minuti di ricezione, e l'effetto va via via scemando con il passare delle ore. Dopo un'ora la notizia di un'operazione di questo tipo si è già diffusa nell'organizzazione e quindi si riduce inevitabilmente il numero di destinatari che cade nell'inganno. La natura del fenomeno "passaparola" dipende da molti fattori e non può essere determinata "statisticamente", e questo rende ancora meno affidabile l'assunzione di un livello di rischio phishing sulla base del click rate riscontrato.

Simulazioni Phishing

- **4) NESSUNA INCIDENZA SUL RISCHIO PHISHING**

Il quarto limite è legato invece a quello che dovrebbe essere l'obiettivo "naturale" di un'attività di questo tipo, ossia procedere verso una sua decisa e concreta riduzione.
Per fare questo è necessario attivare i meccanismi dell'apprendimento esperienziale e quindi collegare una forma di apprendimento all'inganno, per cui è necessario che chi cade nell'inganno possa prendere atto del suo errore e seguire una specifica formazione. Molte organizzazioni, per ridurre il fenomeno "passaparola" preferiscono ad esempio evitare che all'inganno corrisponda un'evidenza dell'errore.



Spesso il link malevolo viene indirizzato su pagine che non mettono in evidenza nè la simulazione nè l'inganno subito: pagine web legittime, pagine di errore 404, pagine senza contenuto. In questo specifico caso il fenomeno del passaparola rimane più contenuto, ma l'apprendimento esperienziale risulta nullo.

Altre organizzazioni invece decidono di indirizzare la "vittima" dell'inganno verso una pagina dove mettono in evidenza che si tratta di un'attività di simulazione, aggiungendo a questa pagina contenuti formativi generici relativi al phishing. In questo caso, le organizzazioni non potranno sfuggire al fenomeno del passaparola descritto in precedenza, ma potranno giovarsi di un effetto positivo legato all'esposizione della vittima a una forma di apprendimento.

Anche in questo caso non possiamo però parlare di apprendimento esperienziale efficace, soprattutto a causa del primo limite che abbiamo evidenziato e cioè la bassa frequenza di queste attività di ethical phishing.

Limiti di valutazione

Il percorso per l'apprendimento esperienziale deve essere costante nel tempo e avere una frequenza di esposizione al rischio sufficientemente elevata per allenare la prontezza dell'individuo.

- **5) METRICHE QUANTITATIVE E AGGREGATE**

Il quinto limite è legato al fatto che queste attività ottengono nella maggior parte dei casi un risultato esclusivamente quantitativo e aggregato. Mettono quindi l'organizzazione nella condizione di capire ***quanti hanno cliccato, ma non chi ha cliccato***.

Questo limite a volte è dovuto a problemi strutturali della piattaforma di erogazione e al suo impatto nell'organizzazione, altre volte a problematiche che riguardano il diritto alla privacy o comunque l'assenza di accordi sindacali specifici.

La conseguenza è che non sarà possibile portare avanti programmi di formazione o apprendimento differenziato sulla base della propensione o meno del singolo individuo a diventare vittima di un attacco phishing. Sembrerebbe un limite insormontabile, ma in realtà esiste una via per coniugare la privacy o i diritti sindacali, con l'esigenza di portare avanti un programma di apprendimento esperienziale differenziato.

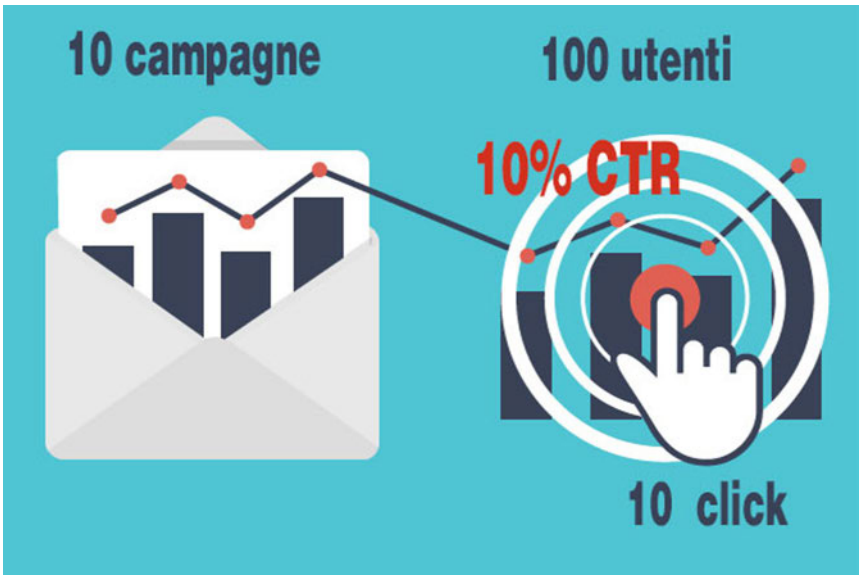
Mettendo insieme questi limiti possiamo senz'altro affermare che le tradizionali piattaforme di simulazione non risultano efficaci sia nella valutazione che nella riduzione del rischio phishing.

Metriche quantitative

VALUTAZIONE RISCHIO PHISHING

Per quanto riguarda le difficoltà di valutare il rischio phishing a fronte di un'attività tradizionale di ethical phishing possiamo fare un ulteriore esempio.

Ipotizziamo di organizzare **10 *campagne*** di ethical phishing su **100 *utenti***, e di esporre gli utenti che cadono nell'inganno ad una pagina formativa. Ipotizziamo che in tutte e 10 le campagne otteniamo un ***click rate del 10%*** ossia che 10 utenti cliccano ogni volta sul link malevolo proposto o che comunque eseguano l'azione ingannevole suggerita nel template.



Se facessimo una mera valutazione tra click rate e rischio phishing potremmo assumere che l'organizzazione **presenta un rischio costante del 10%**. Un dato di questo tipo, al di là di essere un dato poco significativo, potrebbe risultare frustante per un'organizzazione che in quel periodo di tempo ha portato avanti numerose iniziative di Awareness che sembrerebbero non aver avuto alcun effetto positivo.

Click rate e rischio

Se fossimo in grado di valutare questo risultato in modo qualitativo, potremmo ad esempio scoprire che quelle 10 persone non sono sempre le stesse e che tutti gli utenti alla fine delle 10 campagne hanno cliccato una volta sola sul link malevolo. Questo starebbe a significare che l'apprendimento esperienziale, combinato con tutte le altre attività di Awareness ha prodotto un risultato positivo.

Infatti, i 10 utenti che ad ogni attacco simulato cadono vittima dell'inganno e vengono conseguentemente esposte al contenuto formativo di cui sopra, diventano immuni ai successivi attacchi. Seguendo questo trend potremmo ipotizzare che all'undicesima campagna otterremmo il fantastico risultato del rischio zero, ossia zero click, perché tutti e 100 gli utenti sarebbero stati già esposti al contenuto formativo.

È chiaro che si tratta di un esempio teorico, anche perché nessun utente può maturare una resilienza (capacità di subire un attacco senza diventarne vittima) infinita agli attacchi phishing, soprattutto perché gli stessi diventano sempre più complessi e sofisticati, e quindi sempre più difficili da riconoscere e che proprio da questa considerazione nasce l'esigenza dell'addestramento costante e continuo.

Questo esempio teorico ci aiuta a comprendere che ***il solo dato quantitativo aggregato non ci aiuta a valutare correttamente il rischio phishing e ad incidere su di esso.***

SOLUZIONI CUSTOM

Di fronte a questi limiti, alcune organizzazioni hanno pensato di realizzare soluzioni custom utilizzando le varie piattaforme open-source disponibili. Il risultato però non si discosta molto da quello evidenziato nel caso delle attività tradizionali di ethical phishing.

Una piattaforma custom, a meno di investimenti eccessivamente elevati rispetto alle necessità di una singola organizzazione, presenterà gli stessi limiti che abbiamo evidenziato nei paragrafi precedenti e difficilmente sfuggirà dalla logica che c'è dietro una piattaforma di ethical phishing di mercato.

Soluzioni Custom

In modo particolare:

1. limiti in termini di automazione, e di conseguenza impatto eccessivo sui team di Cyber Security;

2. limiti in termini di interpretazione dei risultati, e di conseguenza difficoltà a valutare l'efficacia della piattaforma in termini di riduzione dell'effettivo rischio phishing;

3. limiti in termini di layout e distribuzione delle campagne, con la conseguenza di essere soggetta al fenomeno del passaparola;

4. limiti in termini di "machine learning", e di conseguenza difficoltà a sviluppare un adeguato programma di apprendimento esperienziale;

5. limiti in termini disponibilità di metriche, e di conseguenza un'ulteriore difficoltà a sviluppare programmi di apprendimento personalizzati sull'individuo o sull'unità organizzativa.

I limiti del Custom

CYBER GURU PHISHING

LA SOLUZIONE AVANZATA PER UNA PRATICA SOSTENIBILE

E' quindi evidente che per incidere seriamente sul rischio phishing è necessario un programma di **addestramento "continuo" che agisca sulla prontezza e la reattività degli individui**, incrementando in questo modo la resilienza agli attacchi dell'intera organizzazione. Un programma, basato sull'apprendimento esperienziale, in grado di differenziare il percorso di apprendimento a livello individuale.

Per portare avanti un programma di addestramento anti-phishing che abbia queste finalità è chiaramente necessaria **una piattaforma avanzata che trasformi una teoria ambiziosa in una pratica sostenibile**.
Questo è proprio il ruolo della piattaforma Cyber Guru Phishing che puntando su caratteristiche avanzate come **automazione, approccio adattivo e machine learning** riesce a ridurre concretamente e rapidamente il rischio phishing dell'intera organizzazione.

1. CONFIGURAZIONE SEMPLIFICATA E AUTOMAZIONE

Partiamo dal primo limite che avevamo evidenziato: il grande impatto che le piattaforme di simulazione hanno sui team di Cyber Security, che ne limita fortemente l'utilizzo e quindi non consente di simulare attacchi con una frequenza adeguata a incrementare la prontezza dell'individuo. Con 2 campagne all'anno non è certo possibile incidere efficacemente sulla sfera istintuale degli individui e trasformare i loro comportamenti.

Cyber Guru Phishing automatizza la maggior parte dei processi necessari alla gestione delle campagne di simulazione riducendo al minimo l'impatto nei confronti dei team di Cyber Security. Anche lo sforzo di on-boarding e di attivazione del programma si limita alla preparazione di una "lista utenti" che tenga conto di alcuni parametri come unità organizzativa di appartenenza, ruolo aziendale ricoperto, aspetti logistici, elementi di carattere culturale, lingue utilizzate [...]

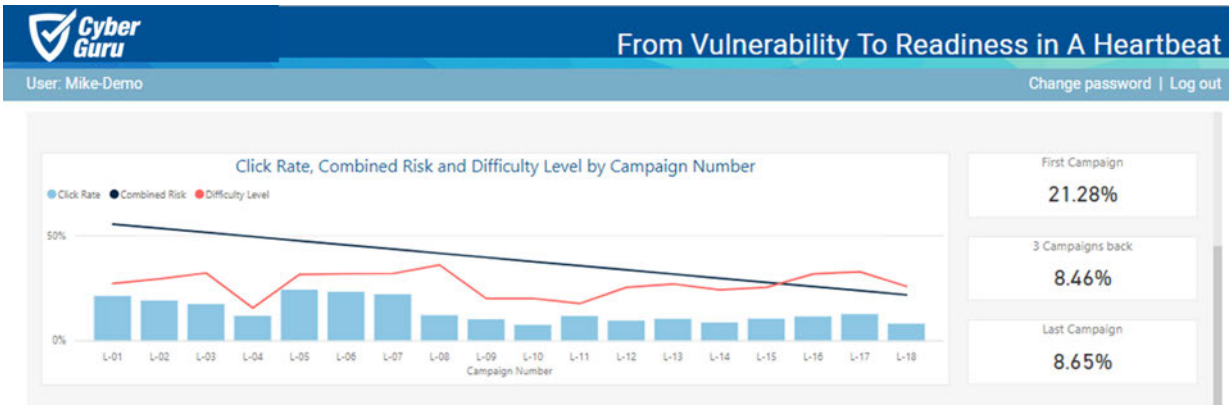
Cyber Guru Phishing

Una volta attivato, il programma procede autonomamente lasciando ai team di Cyber Security la capacità di governo di alcuni aspetti importanti del processo, come ad esempio l'approvazione dei template via via suggeriti dalla piattaforma. Quest'attività viene supportata con una reportistica molto efficace, focalizzata sull'abbattimento del rischio phishing.

Cyber Guru Phishing è l'unica piattaforma di simulazione in funzione anti-phishing completamente autonoma, che consente quindi di ottenere un risultato efficace senza impatti sui team di Cyber Security.

2. REPORTISTICA EFFICACE

Il secondo limite, legato all'interpretazione dei risultati, viene superato fornendo all'organizzazione una reportistica efficace che consente di monitorare l'avanzamento del programma di addestramento e i reali risultati ottenuti, espressi sia come riduzione del rischio phishing sia come aumento del livello di resilienza agli attacchi phishing.



Quando parliamo di rischio phishing non ci riferiamo in modo esclusivo al click rate, che come abbiamo visto è un indicatore "limitato", ma ci riferiamo a un **valore combinato** che tiene conto di altri indicatori, come il livello di difficoltà dell'attacco subito. In questo caso non si tratta di un livello di difficoltà stimato in termini generali, ma di un livello di difficoltà che tiene conto sia di parametri generali, che riguardano le caratteristiche di quella specifica organizzazione, sia di dati "misurati" sul campo, che esprimono le sensibilità specifiche di quella singola organizzazione e che non sono riscontrabili in altre.

Reportistica efficace

Queste informazioni non vengono espresse solo in termini aggregati, ma anche con dei livelli di dettaglio che riguardano ogni singola unità organizzativa, ogni singola sede, ogni diversa tipologia di dispositivo utilizzato, fino ad arrivare all'analisi comportamentale del singolo individuo, seppur nel rispetto della sua privacy.

Gli indicatori più importanti che vengono forniti sia a livello aggregato sia a livello di dettaglio sono:

- il **rischio combinato**, che tiene conto sia del click rate sia delle valutazioni teoriche e reali del livello di difficoltà dell'attacco;
- il **livello di resilienza** agli attacchi (di fatto il numero di attacchi a cui si è in grado di resistere prima di cadere nell'inganno);
- l'identificazione dei "**serial clicker**", ossia di coloro che hanno un'elevata propensione a cadere nell'inganno, effettuando l'azione suggerita nella e-mail dal contenuto malevolo.

3. STRATEGIE DI SIMULAZIONE DIFFERENZIATE E DISTRIBUITE NEL TEMPO

Per rispondere al terzo limite legato al fenomeno del "passaparola" che altera l'efficacia del programma e l'interpretazione dei risultati ottenuti, Cyber Guru Phishing utilizza delle strategie di attacco simulato che sono appositamente studiate per evitare questo fenomeno.

Per prima cosa la campagna non è costituita da un solo template, ma da una serie di template diversi che vengono distribuiti tenendo conto del profilo comportamentale del target. La campagna inoltre non viene effettuata in modo massivo ma in un arco temporale di circa tre settimane.
Per cui non accadrà mai che due persone che risiedono nello stesso ufficio o nella stessa unità organizzativa ricevano lo stesso tipo di e-mail nello stesso momento. L'estrema varietà dei template utilizzati nella stessa campagna, scelti tra le migliaia disponibili, eviterà il fenomeno del "passaparola" e produrrà un risultato più efficace e più credibile sul piano del risultato.

Strategie differenziate

Ci teniamo a sottolineare che questa sofisticazione verrà gestita in modo completamente automatico dalla piattaforma e quindi non avrà alcun impatto su chi governa il programma di addestramento.

4. APPRENDIMENTO ESPERENZIALE

E ora affrontiamo il quarto limite, quello forse più importante rispetto all'efficacia del risultato e quindi alla diminuzione del rischio phishing, che consiste nella capacità di portare avanti un programma di addestramento efficace e continuativo nel tempo. Abbiamo visto come l'efficacia sia fortemente condizionata dalla capacità di sviluppare una forma di apprendimento esperienziale che agisca sia a livello cognitivo sia a livello istintuale, sviluppando la prontezza dell'individuo.

Un apprendimento esperienziale richiede alcune condizioni, come ad esempio la frequenza delle simulazioni, che deve essere adeguata allo scopo (almeno un attacco al mese), la continuità nel tempo, ma soprattutto la personalizzazione dell'attacco sulla base del profilo comportamentale del singolo individuo.

Un individuo che dimostra un'elevata resilienza agli attacchi dovrà essere "attaccato" con simulazioni che abbiano un livello di complessità via via crescente. L'obiettivo della piattaforma è quello di generare esperienza in ogni componente dell'organizzazione, partendo dall'assunto che nessuno è immune dal rischio phishing.

Al contrario, un individuo che dimostra un'elevata propensione a cadere nell'inganno, fino all'estrema condizione rappresentata dal cosiddetto "serial clicker" (colui che clicca consecutivamente e compulsivamente su ogni attacco ricevuto), dovrà essere accompagnato nel suo percorso con attacchi più frequenti ma della stessa tipologia e dello stesso livello di complessità. Aumentare la complessità degli attacchi su soggetti di questo tipo non produrrebbe alcun beneficio e sarebbe contrario ad ogni logica di apprendimento esperienziale.

Un percorso di apprendimento con queste caratteristiche produce benefici tangibili e si dimostra particolarmente efficace sia in termini di riduzione del rischio phishing sia nello sviluppo della resilienza degli individui e dell'intera organizzazione. Cyber Guru Phishing è infatti l'unica piattaforma il cui risultato è garantito.

Simulazioni ad hoc

Portare avanti un percorso di apprendimento esperienziale richiede chiaramente una piattaforma con alcune caratteristiche avanzate e innovative, e cioè automazione, intelligenza artificiale e machine learning; caratteristiche che rendono la piattaforma in grado di funzionare in modo completamente autonomo.

5. INFORMAZIONI DETTAGLIATE NEL RISPETTO DELLA PRIVACY

Veniamo al quinto limite ossia alla difficoltà di ottenere informazioni che vadano oltre il dato quantitativo aggregato, condizione necessaria per portare avanti un programma di apprendimento esperienziale a carattere individuale.

Tutte le caratteristiche che la piattaforma deve avere per realizzare programmi efficaci di apprendimento esperienziale, le abbiamo già analizzate in precedenza, e consistono nell'automazione, nell'intelligenza artificiale, nel machine learning e nella reportistica avanzata. Sono caratteristiche che consentono di gestire un numero sufficiente di livelli di dettaglio organizzativo per poter ottenere e valutare correttamente la situazione dell'intera organizzazione, anche quando questa si presenta particolarmente complessa e articolata.

Il dato su cui riflettere è rappresentato dal **rispetto della privacy e dei diritti sindacali**, considerando che gli aspetti di carattere sindacale in Italia rappresentano un tema molto delicato, che in taluni casi potrebbe portare a limitare l'uso di informazioni che associano il rischio phishing all'individuo. E' quindi importante capire come sia possibile portare avanti un programma personalizzato, come lo abbiamo descritto in precedenza, senza avere impatto su aspetti che riguardano la privacy e i diritti sindacali del singolo individuo.

In questo senso Cyber Guru Phishing consente di **anonimizzare completamente** la piattaforma all'esterno, impedendo che ci sia ad esempio un'identificazione del "serial clicker". La piattaforma è in grado di gestire il profilo comportamentale di ogni singolo individuo, e quindi di personalizzare gli attacchi sulla base di questo profilo, ma consente al contempo di **mascherare qualsiasi informazione** che consenta di identificare chi che cade nell'inganno. In questo caso la reportistica fornirà report che arrivano ad associare le metriche e gli indicatori fino all'unità organizzativa di appartenenza, ma non oltre questo punto. Chiaramente si tratta di un'opzione a disposizione dell'organizzazione che sceglierà quale modalità adottare sulla base delle proprie necessità e regole.

Rispetto della privacy

I CONCETTI BASILARI

CYBER GURU PHISHING IN SINTESI

Cyber Guru Phishing è stata progettata seguendo uno schema di ragionamento basato sui seguenti principi:

.

- I dipendenti sono tutti diversi e hanno inevitabilmente curve di apprendimento differenziate. Valutare queste differenze richiede un'osservazione e un'analisi costante di tutti i dati.

- Considerando che il processo di apprendimento esperienziale è basato su logiche di formazione continua e che le decisioni possono essere prese solamente su un'analisi costante dei dati, il supporto dell'automazione è assolutamente necessario per ottenere un risultato efficace.

.

- Nell'attuale scenario, tutti i team che si occupano di sicurezza sono soggetti a un volume elevato di minacce che cresce di giorno in giorno, così come cresce costantemente il livello di sofisticazione degli attacchi. In questo scenario bisogna automatizzare tutti i processi che possono essere automatizzati, consentendo ai team di sicurezza di focalizzarsi solo su ciò che richiede inevitabilmente l'attenzione di uno specialista.

- Il fattore umano rappresenta il principale punto di vulnerabilità delle moderne organizzazioni, ed è proprio sulle caratteristiche del fattore umano che è stato indirizzato il massimo sforzo nello sviluppo della soluzione.

Concetti basilari

LA METODOLOGIA

La metodologia di Cyber Guru Phishing si basa su concetti formativi internazionalmente riconosciuti e su una lunga esperienza maturata nella formazione relativa alla sicurezza delle informazioni in settori pubblici e privati. L'efficacia e l'efficienza delle campagne di simulazione si deve a queste conoscenze e ad alcuni concetti basilari che caratterizzano la metodologia di Cyber Guru Phishing:

1. **Formazione continua**: il cambiamento del comportamento dei dipendenti richiede l'implementazione di un programma di allenamento che venga eseguito continuamente. Per questa ragione è stata sviluppata una piattaforma automatizzata che può acquisire autonomia nell'esecuzione del programma, lasciando agli esperti di sicurezza solo la supervisione.

2. **Ripetizione senza noia**: un concetto chiave nella formazione è la necessità di ripetere l'allenamento senza annoiare gli utenti. Questo si ottiene costruendo un motore di regole che cambia costantemente i contenuti della formazione, per renderli unici dal punto di vista dell'utente finale.

3. **Diversità**: imparare a identificare il phishing è come imparare a guidare, per cui più situazioni una persona incontra nella sua esperienza di apprendimento, più le sue qualità di autista migliorano. Nel percorso di apprendimento per identificare gli attacchi phishing, questo effetto si ottiene usando diversi scenari di simulazione all'interno di una determinata campagna e all'interno dei cicli di apprendimento dei dipendenti.

4. **Sistemi di memorizzazione**: utilizzare i risultati delle principali ricerche scientifiche per comprendere come funziona la memoria ci ha permesso di dotare la piattaforma di un metodo e di contenuti particolarmente efficaci che favoriscono l'apprendimento individuale. Questa è una delle ragioni per cui abbiamo realizzato una piattaforma multilingua con contenuti molte volte costruiti direttamente nella lingua nativa del dipendente.

5. **Formazione basata sui dati**: integrando le tecniche di machine learning e l'analisi statistica, con concetti di formazione avanzata, si otterranno risultati nettamente migliori rispetto a un training manuale o basato su una percezione.

La metodologia

PERCHÈ CYBER GURU È DIFFERENTE

La soluzione consiste in una piattaforma autonoma, con una tecnologia di apprendimento automatico basato sui dati e con caratteristiche uniche che la differenziano da qualsiasi altra piattaforma di phishing. Queste differenze riguardano sia i benefici che i nostri clienti possono ottenere sia le metriche di misura, che forniscono un riscontro tangibile dei benefici ottenuti.

- Con Cyber Guru Phishing il team di sicurezza investirà pochissimo tempo nella gestione del programma di allenamento continuo, che è costituito sia dalla simulazione periodica degli attacchi phishing, sia dall'esposizione automatica di coloro che cadono vittima dell'attacco simulato a contenuti di training specifici. Il programma infatti viene portato avanti autonomamente dalla piattaforma, e al cliente spetterà solo il compito di supervisionare il processo e di interpretare i risultati. ***Nessuna altra soluzione presente sul mercato ha queste caratteristiche.***

- Con Cyber Guru Phishing, il tempo di "**on-boarding & running**" è molto veloce anche per realtà complesse, perché tutte le funzionalità richieste sono "pronte all'uso". Tra queste ci sono la predisposizione dei template, la personalizzazione dei contenuti formativi, la traduzione multilingua delle simulazioni, tutte attività che sulle altre piattaforme richiedono la presenza di un progettista e di sviluppatori con conoscenze in ambito HTML/CSS.

- Con Cyber Guru Phishing i tassi di engagement del personale sono particolarmente elevati, perché la formazione è strutturata secondo un modello di "training on the job", basato su lezioni essenziali e molto brevi, che si attivano all'occorrenza, solo quando l'utente cade vittima dell'attacco. Questo stimolerà la prontezza, la reattività, la predisposizione dell'utente a memorizzare i contenuti e ad essere parte attiva del meccanismo di difesa.

- Con Cyber Guru Phishing i risultati sono immediatamente visibili e possono essere oggettivamente misurati con indicatori e metriche più evolute rispetto a quelle fornite da altre soluzioni basate esclusivamente sul click rate che, come indicatore isolato, non ha alcuna relazione con il rischio reale.

Perchè Cyber Guru

- Con Cyber Guru Phishing si può misurare concretamente il TCO della piattaforma, senza alcun costo nascosto, e senza la necessità di ricorrere ad attività di consulenza e a servizi professionali particolarmente onerosi, cosa che avviene regolarmente con altre piattaforme, specialmente se si ha l'obiettivo di produrre un numero significativo di simulazioni per ogni dipendente.

- Con Cyber Guru Phishing si ha a disposizione un Customer Success Manager dedicato, perché il reale obiettivo di una piattaforma di questo tipo è quella di ottenere successo, e quindi di diminuire il rischio, agendo sul fattore umano.

Piattaforma unica

RISULTATI GARANTITI

Negli ultimi anni, grazie a Cyber Guru Phishing, un numero elevato di aziende enterprise e centinaia di migliaia di professionisti sono stati formati con successo, migliorando notevolmente la resilienza rispetto agli attacchi phishing.

SERIAL CLICKER

E' definito un "serial clicker" un dipendente che, negli ultimi cicli di simulazione di un attacco phishing, ha fallito ripetutamente, rappresentando quindi un rischio elevato per l'intera organizzazione. Per questa ragione il serial clicker deve necessariamente essere sottoposto ad un livello di addestramento più intenso e frequente.

Utilizzando Cyber Guru Phishing il gruppo di serial clicker:

1. Si attesta mediamente intorno al 17%, dopo le prime 3 simulazioni
2. Diminuisce al 10% dopo 6 simulazioni
3. Raggiunge il 4% dopo 12 simulazioni.

È importante sottolineare che il monitoraggio e l'intensificarsi dell'addestramento anche in questi casi viene effettuato in modo autonomo da parte della piattaforma. Quindi questo processo può avvenire anche quando l'azienda abbia deciso di mantenere completamente anonimizzata la piattaforma dal punto di vista della reportistica individuale.

RESILIENZA DEI DIPENDENTI

La resilienza dei dipendenti viene misurata rispetto al numero di simulazioni concluse con successo (senza che il destinatario della mail faccia click sul collegamento) tra due fallimenti.

Con Cyber Guru Phishing il punteggio medio di resilienza del dipendente:

1. Si attesta a 1 dopo la seconda simulazione
2. Raggiunge 2 dopo cinque simulazioni
3. Raggiunge 4 dopo dodici simulazioni

Il punteggio di resilienza riflette la capacità dei dipendenti di resistere agli attacchi. Il valore di questo punteggio aumenta sempre durante i periodi in cui le campagne phishing sono attive. Fornisce anche una misura concreta di quanto possa essere difficile per un utente malintenzionato superare le difese psicologiche dei dipendenti. Gli algoritmi di apprendimento automatico combinati con l'allenamento adattivo ad alta frequenza, hanno dimostrato di massimizzare i propri risultati su un programma di 12 mesi.

Risultati garantiti

RISCHIO COMBINATO

La valutazione del rischio viene effettuata sulla base di una combinazione di metriche diverse. Le piattaforme tradizionali di ethical phishing tendono ad associare in modo diretto il livello di rischio al click rate, cosa che riduce molto il valore della misurazione riconducendola a una mera considerazione di tipo statistico.

Cyber Guru Phishing effettua questa valutazione tenendo conto di più metriche, in modo particolare della combinazione tra il click rate e il livello di sofisticazione dell'attacco, che viene calcolato in modo algoritmico su un numero consistente di parametri.
È abbastanza frequente quindi che il livello di rischio si attesti su valori più bassi, anche a fronte di aumento del click rate.

SEGMENTAZIONI

La reportistica può essere letta sulla base delle campagne, dei profili specifici degli utenti, delle unità organizzative, delle location, dei linguaggi utilizzati e di altri elementi di segmentazione dell'utenza stabiliti dall'azienda stessa.

Rischio combinato

L'APPRENDIMENTO ESPERENZIALE PER RIDURRE IL RISCHIO PHISHING

Cyber Guru Phishing

www.cyberguru.it
contatti@cyberguru.it
Numero verde 800.741.423