GUIDA GALATTICA AL CONTRO-PHISHING

IL PHISHING

Il phishing consiste in una truffa online con cui si cerca di ottenere informazioni personali o aziendali (es. credenziali di accesso, dati finanziari, informazioni riservate) da parte del destinatario di una finta comunicazione (es. e-mail, popup, PEC, SMS, messaggistica istantanea) proveniente da un ente affidabile. L'attività ingannevole consente al criminale di "pescare" informazioni e password e di infettare i dispositivi delle vittime attraverso allegati malevoli.

UNA FORMA DI TRUFFA

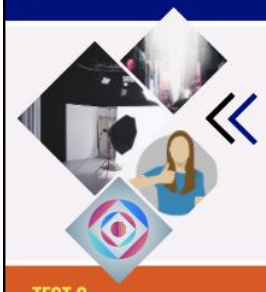
Il phishing è una forma di truffa che fa molto affidamento sull'errore umano, dal momento che richiede un'azione positiva da parte del destinatario (aprire l'allegato, cliccare sul link, rispondere alla comunicazione, ecc.). Proprio per questo, nel corso del tempo, la qualità delle "finte comunicazioni" o bait (propriamente: "esche") è nettamente migliorata fino ad apparire, quasi sotto ogni aspetto, come un messaggio legittimo ed è efficace per il contenuto ad indurre la vittima verso l'azione designata.

DIVENTARE CONSAPEVOLI CON I TEST

Essere consapevoli del rischio, ed istruire di conseguenza i propri dipendenti e collaboratori a riconoscere i potenziali indicatori di anomalia è diventata la principale e migliore linea di difesa contro questo tipo di attacchi informatici.
Ecco alcuni semplici test per rilevare alcune anomalie nelle comunicazioni ed essere in grado di riconoscere il tentativo di phishing.

TEST 1
CONTESTO

Analizzare il perché si dovrebbe essere destinatari di tale comunicazione in quella determinata forma (e-mail, SMS). E soprattutto, diffidare sempre delle comunicazioni che avvengono proprio in periodi di over-burn lavorativo da cui consegue una ridotta cautela (es. a ridosso di festività o di scadenze di adempimenti obbligatori) adottando un consequenziale approccio di maggiore cautela.



TEST 2
GENUINITÀ

Verificare il mittente e il contenuto del messaggio presso un punto di contatto già in proprio possesso (e non ai contatti offerti all'interno della comunicazione "sospetta") è la principale difesa di contro-phishing, che porta ad escludere la maggior parte delle comunicazioni fraudolente. Occorre però fare attenzione perché alcune di queste possono inserirsi nell'ambito di situazioni pubblicamente "note" (es. scontistica, bonus, scadenze fiscali).

TEST 3
CONTENUTO

Ogni tentativo di phishing tenta di far leva su un'azione positiva da parte del destinatario (es. apertura di un allegato, clic ad un link, risposta al messaggio, inserimento di credenziali, trasmissione di informazioni) agendo su un indotto senso di urgenza per ottenere un vantaggio o scongiurare una perdita. Una richiesta di azione urgente di per sé non è un'anomalia, ma se questa è collegata a determinate tipiche del phishing quali invio di dati, apertura di un link o di un allegato, costituisce evidenza di un'anomalia.

TEST 4
INFORMAZIONI

Badare sempre a che cosa viene richiesto e quali informazioni materialmente andremo a trasmettere, al fine di comprendere l'attendibilità della richiesta e valutare il rischio dell'invio dei dati. Questo parametro è particolarmente valido e costituisce un'evidenza di anomalia se il preteso mittente sta chiedendo dati di cui dovrebbe già essere in possesso o in modo difforme da una procedura nota (ad es. l'istituto bancario che chiede i dati di pagamento della carta di credito o le credenziali dell'online banking).

TEST 5
FORMA

Grazie agli strumenti di traduzione automatica e di machine learning, la forma testuale dei messaggi fraudolenti si è evoluta ed è quasi priva di errori. Parimenti, il layout grafico è spesso contraffatto. Ad ogni modo alcuni errori di grammatica o interpunzione, scelte lessicali incoerenti (ad es. dare del "tu" all'interno di una comunicazione formale) e firme mittenti poco chiare ed "istituzionali" (nonostante la presenza di loghi) possono costituire evidenze di anomalie.

Le principali difese contro gli elaborati metodi di truffa sviluppati attraverso l'ingegneria sociale non sono altro che la consapevolezza e l'adozione di azioni coerenti, preventive ed efficaci.

INFOSEC news