Phishing: cos’è, come prevenirlo e come agire dopo un attacco

lunedì 02 settembre 2019

Più volte abbiamo parlato di phishing ealtre truffe online. Oggi pubblichiamo il contributo proposto alla nostraredazione da Aruba a cura di Nicola Tacconi, CISO di Aruba S.p.A.Il phishing è una truffa veicolatatramite Internet, in cui si cerca di ingannare la vittima al fine di recuperareinformazioni sensibili come username, password o dati bancari. Generalmente, il criminale informaticoinvia false comunicazioni al soggetto-vittima, fingendosi un Ente o un’aziendaben conosciuta o con cui è possibile che si stiano avendo conversazioni erelazioni, usando scuse plausibili per ottenere i dati personali della vittima. Il fenomeno del phishing è una minacciaattuale e frequente, tant’è che l’Italia, secondo una recente ricerca diKaspersky Lab, è il quarto target mondiale di attacchi con il 5,76% disegnalazioni. Dati ed evoluzione del phishing Secondo il report 2019 di Clusit,l’associazione italiana per la sicurezza informatica, il phishing online non siè mai evoluto così velocemente come nell’ultimo anno, tanto che nell’arco delbiennio 2017-2018 il numero di attacchi gravi è cresciuto in Italia del +37,7%.Solitamente il phishing si presenta come una comunicazione digitale che giungeal destinatario via e-mail, via SMS, tramite un social network o sulleprincipali piattaforme di Instant Messaging. Generalmente gli attacchi diphishing sono accomunati da una o più delle seguenti caratteristiche: comunicazione di una sospensione o blocco di un account senza alcunaspiegazione; sollecito di pagamento legato ad una determinata operazione entro unadata di scadenza fittizia; presenza di un indirizzo web che include un dominio simile ma diverso daquello originale dell’ente; richiesta di informazioni private; errori ortografici nel corpo del messaggio. Come comportarsi se si è vittima diphishingCome tutelarsi dagli attacchi Esistono una serie di accorgimenti checonsentono di navigare più sicuri e non cadere vittime dell’attacco, traquesti: mantenere il proprio browser sempre aggiornato. Installando le ultimeversioni e inserendo dei filtri anti-spam, o degli appositi plug-in, il browserriuscirà a prevenire un maggior numero di tentativi di phishing; controllare il dominio da cui proviene la comunicazione. Una società oun ente scriveranno sempre dal proprio dominio, bisogna controllare checorrisponda a quello ufficiale. Questa verifica non dà la massima garanzia diautenticità ma rappresenta un primo controllo da poter effettuare; fare attenzione a cliccare sui link nelle e-mail. Come buona norma siconsiglia di non cliccare mai sui link contenuti nella comunicazione madigitare direttamente nel browser l’indirizzo del sito ufficiale del mittentedella comunicazione e verificare sul sito il contenuto descritto nellacomunicazione dell’e-mail; utilizzare più indirizzi e-mail. Quando ci si iscrive a servizi, o sitiweb, di dubbia affidabilità, è preferibile utilizzare e-mail secondarie, inmodo da non rischiare di contaminare la propria casella e-mail principale; contattare il servizio clienti. Se arriva una e-mail ambigua e non sicapisce con certezza se sia una frode o meno, è meglio contattare il servizioclienti dell’azienda a cui la mail fa riferimento. segnalare un sito di phishing aiutando altri utenti a non cadere nellatruffa. Ogni segnalazione è utile per far comparire un messaggio di avvisoriguardo al sito potenzialmente pericoloso: le segnalazioni possono essereinviate, ad esempio, tramite PhishTank, Google Safe Browsing o Microsoft SmartScreen. utilizzare e-mail professionali, dotate di protocolli di sicurezza qualiSPF e DMARC sulla posta in ingresso (e in uscita). Cosa fare se si è rimasti vittima diphishing Se, però, si è ormai caduti neltranello, ci sono una serie di operazioni da compiere così da limitarne idanni, tra questi: • cambiare la password: nel caso diportali online bisogna cambiare la password o chiudere direttamente il profiloprima che gli hacker possano accedervi; • contattare il servizio clienti.Qualora l’account sia già stato compromesso e non sia più possibile fare illogin con i propri dati, è necessario contattare il servizio clienti perripristinare manualmente i propri dati d’accesso; • contattare la banca. In caso di furtodi dati bancari va contattato l’istituto di credito per bloccare i servizicoinvolti nella truffa (carte di credito, conti correnti, bancomat edulteriori); • avvisare gli enti colpiti. Oltre alrecupero dei dati personali, è opportuno segnalare l’attacco phishing agli entiche ne sono stati colpiti, cosicché possano prendere provvedimenti econtrastare la truffa; Il phishing, anche se può sembrare unasemplice e-mail ingannevole, è un reato vero e proprio, e come tale vaconsiderato. Motivo per cui il passo successivo alle eventuali segnalazioni èquello di informare le autorità competenti. Nonostante non sia previstodall’ordinamento penale, il phishing oggi viene giudicato come frodeinformatica e furto d’identità digitale. In quanto reato informatico, inoltre,va comunicato alla Polizia Postale, che sul suo sito ha disposto uno spazio perle segnalazioni di questo tipo. In conclusione, esiste una grossa moledi attacchi, ma grazie alle possibili contromisure da adottare, la percentualedi attacchi intercettati, bloccati e non andati a buon fine supera l’80%. Sulrestante 20% è necessaria una consapevole collaborazione fra i fornitori diservizi e i clienti: leggendo attentamente le e-mail che si ricevono, inserendoi propri dati solo su siti affidabili e evitando di aprire link sospetti, ilphishing può essere evitato.