SERVIZI E SOFTWARE DA "USARE" ON LINE

ARE BEEL



# TI DIAMO LE DRITTE PER NAVIGARE SUL WEB E METTERSI AL RIPARO DAGLI ATTACCHI DI TIPO PHISHING **TI DIAMO I TOOL PER BLOCCARE E-MAIL E LINK FRAUDOLENTI**

l Phishing è un termine col quale è identificato un particolare tipo di e-mail che viene indirizzato ad una lista di ignari utenti per carpire i loro dati sensibili. L'inganno viene perpetrato attraverso un messaggio della propria banca, oppure di PayPal o Amazon, che chiede alla vittima di cliccare su di un link utilizzando come pretesto un fantomatico problema: sono tipici, ad esempio, i messaggi del tipo "c'è stato un problema col tuo ordine Amazon, clicca quì ed immetti le tue informazioni personali per accedere"; oppure "abbiamo riscontrato un accesso non autorizzato nel tuo conto PayPal, clicca quì per cambiare la tua password". Naturalmente il link in questione non conduce affatto al sito in questione, ma ad una pagina sviluppata dai truffatori che imita quella del servizio originale in modo da ingannare gli utenti più sprovveduti.

### **TRAPPOLE BEN CONGENIATE**

54 Idea Web

Purtroppo, nonostante le raccomandazioni di banche e istituti di credito di diffidare delle email che richiedono dati sensibili, un numero imprevedibilmente alto di utenti continua a cascare nella trappola del phishing. Fermo restando che la più efficace delle soluzioni è quella di non fidarsi mai di e-mail sospette e

di fare sempre attenzione all'aspetto del sito, le pagine di phishing hanno di frequente layout sgangherati, con immagini che mancano e loghi a bassa risoluzione. Chi vuole tutelarsi in maniera efficace dal phishing può servirsi di alcuni utili strumenti, tra cui un servizio on-line chiamato URLQuery che non fa altro che interrogare l'indirizzo Internet contenuto

nell'e-mail truffa per smascherare ogni aspetto di quest'ultimo (come ad esempio l'eventuale presenza di malware), nonché il suo indirizzo IP, la nazione di provenienza e molti altri dati utili a convincerci in maniera indiscutibile di non fidarci. In questa guida vedremo come utilizzare URLQuery ed una specifica estensione per Chrome.

# **SCOVIAMO I LINK TRUFFA** ABBIAMO RICEVUTO UNA STRANA E-MAIL DALLA BANCA? ATTENTI: POTREBBE TRATTARSI **DI UN ATTACCO PHISHING**

### **IL SERVIZIO PER SMASCHERARE I MALFATTORI!**

### OT LINK SOSPETTO

lile Cliente.		
formiamo che II vi	ostro Apple IO scaduto in meno di 48 ore	
dispensabile effe te sarà distrutto	ltuare una venfica del vostri dall, eccetto il tuo nom	e
a cliccare il link s	ottostante e accedi con il tuo ID Apple e la passwor	rd.
rolla il tuo acci	Apri link in un'altra scheda	1
liall saluti,	Apri link in un'altra finestra	
nght © 2016 A	Apri link in finestra di navigazione in incognito	
	Apn link come	
	Salva link con nome	_
		1000

Clicchiamo col tasto destro sul collegamento sospetto e dal menu contestuale scegliamo la voce Copia indirizzo link. Raggiungiamo quindi il sito http://urlquery.net e incolliamo il link nel campo Profile URL: con ogni probabilità il contenuto del link sarà diverso da quello che ci si aspetta.

Overview			
val	(www.legendarysci), dicontenna_hus_accounts/canternal.on_accounts_atta 486/24167		
14	185.81.0,100		
<b>半</b> 雪子)-	4552030 Server Plan SrJ.		
LORVEDA	L1 Wy		
Papart sampleted	2016-68-05 09:49:51 CET		
Status	Report complete.		
unQuery Alera	No slarts detected		
Longin on Report + Unignetied Statud un'Quezy Allera	L 1989 2016-66-53 (2014/53) CET Report complete. No Nets esterned		
Settings			
Waragent	Mapitar5.0 (Windows Un Weddaws NF 6.1: en-US: m1.9.2.13) Gecks/20101203 Pirefox		
Referen			
Pest			
Access Level	eutric		

**02 RISULTATI DELLA VERIFICA** 

Intrusion Detection Systems

Clicchiamo sul tasto Go accanto al campo Profile URL e attendiamo l'analisi del sito sospetto. Nella pagina successiva prestiamo attenzione al campo ASN che indica la rete alla quale appartiene il sito incriminato: il dato è già sufficiente a comprendere se si tratta di phishing.

A volte i siti usati per attacchi di tipo phishing riproducono esattamente la grafica di quelli originali e anche gli utenti più accorti potrebbero cadere nella trappola, che scatta non appena ci si logga inserendo i propri dati di accesso.

Gli utenti di smartphone e tablet sono al sicuro dalle truffe grazie alla suite di ESET, Mobile Security, che offre all utente protezione dai tentativi di acquisizione di informazioni personali e dati sensibili come le password, i dettagli dell'account o numeri della carta di credito, da siti Web apparentemente attendibili. L'applicazione e disponibile sul Play Store a questo indirizzo

# **PROTETTI DAL PHISHING** ECCO LA PROCEDURA PER METTERE AL SICURO LA NAVIGAZIONE SUL WEB PROTEGGENDO I NOSTRI DATI PERSONALI **CON L'ESTENSIONE NETCRAFT PER CHROME POSSIAMO DORMIRE SONNI TRANQUILLI**

### OT AGGIUNGIAMO L'ESTENSIONE

DETCRAST	64	ABUTTENZA CORRELATI	DA ARCENSION
ATE I CIVER I			
letcraft Extension Option	The Relevant Johnston is a fast advance may unless at information manage in the effect of well and investiging publication trans- Products		
the extension settings, then nows and points. In the $\alpha$ - $\beta$	PERFERSION - Concerning and the concerning of t		2
ali pli ĝes ' scom. E Diusi plishenp ster	1 mm Antop - of parameters. Insurances of his side and parameters annum frame datasets by has been the The main a sector in the same sectory support on the therepare	Variantee Plan Anno	-
ill brack K55 sitzsta	R Sector		
enter all the sheat supposes the	Cherton Editornation Internet XA1 Delivery and the suggest 2015 Delivery ADMI		

Raggiungiamo l'estensione sul Chrome Web Store Clicchiamo col tasto destro del mouse sull'icona Durante la navigazione clicchiamo sull'icona di all'indirizzo http://www.edmaster.it/url/6522/ e clicchiamo sul pulsante AGGIUNGI in alto a destra. Attendiamo lo scaricamento del file e verifichiamo che l'icona di Netcraft si aggiunga nel pannello dove sono presenti le altre estensioni di Chrome.

di Netcraft e scegliamo la voce Opzioni. Nella schermata che appare inseriamo il nostro nominativo che sarà utilizzato nell'invio delle setiviamo le tre funzionalità base dell'estensione. ste informazioni possiamo valutarne l'attendibilità.

## **04 OCCHIO ALLE TRUFFE NASCOSTE**



Nel caso in cui il sito sia già stato segnalato come non attendibile, la Se siamo sicuri di aver scoperto un sito truffa, colleghiamoci all'indiriznavigazione verrà interrotta. Potremo usufruire dei due pulsanti presen- zo http://www.edmaster.it/url/6523/ e segnaliamolo a Big G inserendo ti nella schermata di Netcraft per segnalare rispettivamente un errore l'URL sospetta nel relativo campo di testo ed indicando nel box dei (Report mistake) o per continuare a navigare nel sito (Visit anyway). Commenti perché riteniamo che si tratti di phishing.



Su http://www.edmaster.it/url/6525/ trovi preziosi consigli del Garante della privacy per combattere il fenomeno Phishing.







**OS VERIFICHIAMO LA SORGENTE** 



Netcraft per verificare la provenienza del sito (Country), il suo posizionamento (Rank), la prima volta in cui è stato visto on-line (First Seen) ed infignalazioni di phishing, quindi attiviamo o disat- ne la rete alla quale si appoggia (Host ). Già da que-

### **05** VAI CON LA DENUNCIA

