*Fai da WEB

Non abboccare alle truffe online

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

Il 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

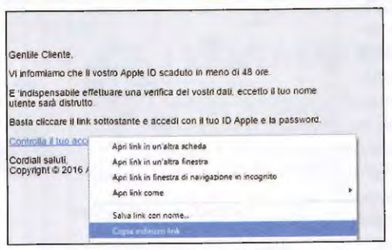
Purtroppo, nonostante le raccomandazioni di banche e istituti di credito di diffidare delle email che richiedono dati sensibili, un numero imprevedibilmente alto di utenti continua a cascare nella trappola del phishing. Fermo restando che la più efficace delle soluzioni è quella di non fidarsi mai di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

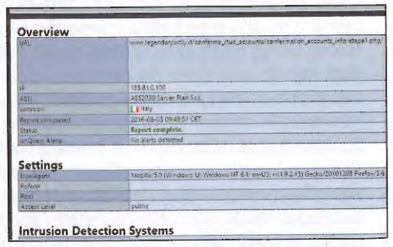
IL SERVIZIO PER SMASCHERARE I MALFATTORI!

01 LINK SOSPETTO



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.

02 RISULTATI DELLA VERIFICA



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.

ATTENTI ALLA URL
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.

METTIAMO AL SICURO TABLET E SMARTPHONE

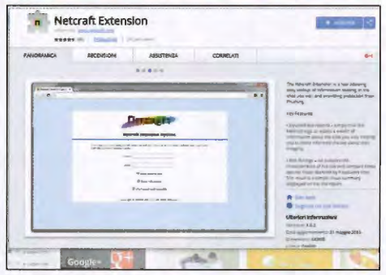
Gli utenti di smartphone e tablet sono al sicuro dalle truffe grazie alla suite di ESET, Mobile Security, che offre all'utente protezione dai tentativi di acquisizione di informazioni personali e dati sensibili come le password, i dettagli dell'account o i numeri della carta di credito, da siti Web apparentemente attendibili. L'applicazione è disponibile sul Play Store a questo indirizzo http://www.edmaster.it/url/6524/. Su dispositivi iOS l'operazione è ancora più semplice in quanto basta avviare il browser Safari, raggiungere le Impostazioni e attivare l'opzione **Avviso sito Web fraudolento**.

PROTETTI DAL PHISHING

ECCO LA PROCEDURA PER METTERE AL SICURO LA NAVIGAZIONE SUL WEB PROTEGGENDO I NOSTRI DATI PERSONALI

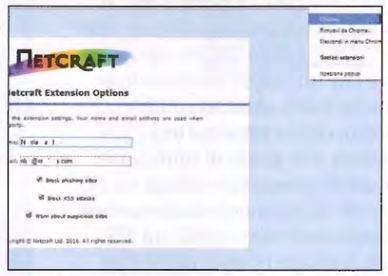
CON L'ESTENSIONE NETCRAFT PER CHROME POSSIAMO DORMIRE SONNI TRANQUILLI

01 AGGIUNGIAMO L'ESTENSIONE



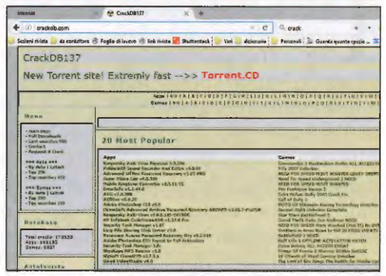
Raggiungiamo l'estensione sul Chrome Web Store all'indirizzo **http://www.edmaster.it/url/6522/** e clicchiamo sul pulsante **AGGIUNGI** in alto a destra. Attendiamo lo scaricamento del file e verifichiamo che l'icona di Netcraft si aggiunga nel pannello dove sono presenti le altre estensioni di Chrome.

02 CONFIGURIAMO IL BROWSER



Clicchiamo col tasto destro del mouse sull'icona di Netcraft e scegliamo la voce **Opzioni**. Nella schermata che appare inseriamo il nostro nominativo che sarà utilizzato nell'invio delle segnalazioni di phishing, quindi attiviamo o disattiviamo le tre funzionalità base dell'estensione.

03 VERIFICHIAMO LA SORGENTE

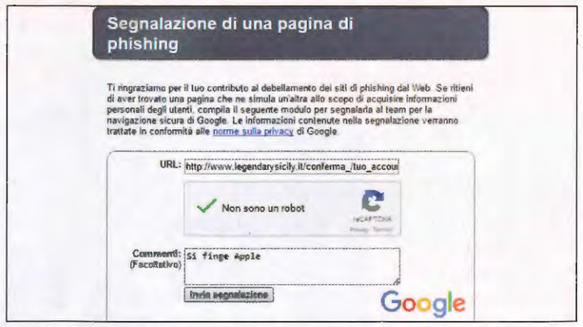


Durante la navigazione clicchiamo sull'icona di Netcraft per verificare la provenienza del sito (**Country**), il suo posizionamento (**Rank**), la prima volta in cui è stato visto on-line (**First Seen**) ed infine la rete alla quale si appoggia (**Host**). Già da queste informazioni possiamo valutarne l'attendibilità.

04 OCCHIO ALLE TRUFFE NASCOSTE

Nel caso in cui il sito sia già stato segnalato come non attendibile, la navigazione verrà interrotta. Potremo usufruire dei due pulsanti presenti nella schermata di Netcraft per segnalare rispettivamente un errore (**Report mistake**) o per continuare a navigare nel sito (**Visit anyway**).

05 VAI CON LA DENUNCIA



Se siamo sicuri di aver scoperto un sito truffa, colleghiamoci all'indirizzo **http://www.edmaster.it/url/6523/** e segnaliamolo a Big G inserendo l'URL sospetta nel relativo campo di testo ed indicando nel box dei **Commenti** perché riteniamo che si tratti di phishing.

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