retarus

Abbiamo l'antidoto contro il phishing da coronavirus:

La guida antiphishing di Retarus

I messaggi che dovessero arrivare nella casella di posta, nonostante le misure di sicurezza implementate, hanno ancora un nemico da superare: voi.

Scoprite come proteggere voi e la vostra azienda dalle frodi online.

retarus.com

State allerta.

Siate sempre pronti ad affrontare i tentativi di frode online, ridurrete notevolmente la probabilità di cadere in una trappola di phishinig.

Il phishing è una truffa online in cui i criminali informatici cercano di diffondere malware, rubare dati e ricavare un ritorno economico. Lavorano con identità false e messaggi costrutiti apposta per sfruttare le caratteristiche tipiche dell'essere umano come la buona fede, la solidarietà verso l'altro o la paura (Social Engineering).

Ai truffatori online piace travestirsi da buoni amici.

I truffatori online si spacciano per amici e familiari, assumono il ruolo di colleghi, superiori o partner commerciali e si rivolgono a voi per conto di istituzioni ufficiali, noti fornitori di servizi finanziari (ad es. la vostra banca, PayPal) o portali online (ad es. Amazon).

Ciò comporta che, anche nel caso in cui si "riconoscesse" il mittente di un messaggio e-mail, ci si potrebbe trovare comunque in presenza di un tentativo di phishing.

Il livello qualitativo del phishing aumenta, in termini sia tecnici, sia visivi, sia di contenuti.

Diventano infatti sempre più rare quelle e-mail di phishing che contengono link lunghissimi e istruzioni maldestre piene di refusi o impaginate in modo scadente. La nuova generazione di e-mail di phishing è tecnicamente sofisticata, formulata con la massima precisione e progettata in modo professionale.

E-mail falsificate, mittenti manipolati, allegati, download e siti web spesso appaiono ingannevolmente reali e non sono necessariamente riconoscibili come falsi neanche a una seconda occhiata.

Siate prudenti.

Se avete la sensazione che ci sia qualcosa che non va in un messaggio e-mail o in un sito web, siate prudenti. In caso di attacco phishing, non reagire è la difesa migliore.

I criminali informatici confezionano il malware (che paralizza il computer e, nel peggiore dei casi, l'intera infrastruttura IT) in allegati, all'interno di link malevoli o finti download.

n. 1 Non fate mai clic sui link presenti nelle e-mail sospette (lo stesso vale per i link di presunti annullamenti di iscrizione*).

n. 2 Non aprite/scaricate allegati contenuti in e-mail sospette (malware).

n. 3 Non rispondete* a un'e-mail sospetta e non inoltratela.

n. 4 Non inserite mai nomi utente, password o altri dati personali su siti web sospetti.

*diversamente, confermereste il vostro indirizzo e-mail

Attenzione alla truffa del sedicente capo (CxO Fraud)!

CxO Fraud è un metodo di phishing particolarmente sfrontato, con cui i criminali informatici fingono di essere manager e sollecitano i dipendenti a compiere azioni (ad es. divulgazione di informazioni riservate su transazioni finanziarie) con dei falsi pretesti (ad es. situazione di emergenza).

Caratteristiche tipiche per le mail di phishing di questo tipo sono la grandissima urgenza e la richiesta di trattamento riservato.

Conoscete il mittente di un messaggio e-mail con contenuto dubbio?

Verificate l'autenticità dell'e-mail tramite una conversazione/ chiamata telefonica personale con il mittente.

Avete il dubbio di essere caduti in una trappola di phishing?

Informate tempestivamente il vostro superiore e/o i vostri colleghi del reparto informatico. Loro sanno cosa fare.

Siate sospettosi.

I criminali informatici adorano le situazioni di crisi. Sfruttano deliberatamente lo stato di emergenza del coronavirus, l'insicurezza delle persone e la condizione di telelavoro, che non è familiare a molti collaboratori.

Attenzione, i truffatori del coronavirus non sono in azione solo tramite e-mail e siti web, ma anche nei social media, via SMS, al telefono e persino alla porta.

Attenzione, coronaphishing!

Siate sospettosi di tutto ciò che vi viene offerto attualmente in Rete relativamente al coronavirus. E siate sospettosi rispetto alle istruzioni che si riferiscono al telelavoro.

Qui sotto riportiamo alcuni esempi con cui i criminali informatici stanno attualmente cercando di diffondere il malware, accedere ai dati, appropriarsi di denaro:

Presunte informazioni "ufficiali" sul coronavirus in forma di iscrizione a una newsletter, di allegato all'e-mail e/o di opzione di download

Offerte di prodotti molto richiesti come mascherine con filtro, tamponi per autodiagnosi, applicazioni di monitoraggio

Richiesta di dati per **nuova regolamentazione** dei servizi clienti/servizi a causa della chiusura di filiali/uffici

Richiesta di **donazione**, ad esempio per lo sviluppo di un vaccino

Consigli per investimenti "intelligenti", come ad esempio "Rendimenti elevati ai tempi del coronavirus"

Installazione di software utili per il telelavoro

Richiesta di password per la partecipazione a una videoconferenza

Sincronizzazione dei dati per l'attivazione di uno strumento remoto (manutenzione da remoto)

Download di un aggiornamento di sicurezza utile per il telelavoro

---

Avete dei dubbi su un'indicazione riguardante il vostro lavoro da remoto? Allora, rivolgete piuttosto una volta in più ai vostri colleghi del reparto informatico.

retarus

Le uniche cose che sono veramente efficaci contro il phishing sono una buona soluzione di sicurezza e-mail e voi stessi!

Siate vigili e sempre pronti a dover affrontare tentativi di frode online relativi al coronavirus. **Siate prudenti** ed evitate clic e download fatti senza riflettere. **Siate sospettosi**, fate domande, usate il buon senso e più di una fonte di informazioni.

Retarus Email Security
Per garantire che la posta elettronica di un'azienda continui a funzionare e non subisca rallentamenti.
retarus.it/email-security