La guida antiphishing per i clienti Helios

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

Scoprite come proteggervi dalle frodi online.

helios
la tua energia

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 costruiti apposta per sfruttare le caratteristiche tipiche dell'essere umano come la buona fede, la solidarietà verso l'altro o la paura.

Ai truffatori online piace travestirsi da buoni amici.

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, fornitori di utenze o di servizi finanziari o portali online (ad es. la vostra banca, il vostro fornitore luce/gas/telefono, Amazon, ecc.).

> **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.**

State 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.

1. Non fate mai clic sui link presenti nelle e-mail sospette

(lo stesso vale per i link di presunti annullamenti di iscrizione)

2. Non aprite/scaricate allegati contenuti in e-mail sospette

(malware)

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

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

State sospettosi.

I truffatori online adorano tutto ciò che muove e preoccupa le persone. Ecco perché c'è spesso un'esca di phishing "adattata" per argomenti che ci riguardano personalmente, che sono trattati intensamente dai media, o che ci riempiono di preoccupazione o di gioia.

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

Qui sotto riportiamo alcuni esempi con cui i criminali informatici cercano di diffondere il malware, accedere ai dati, appropriarsi di denaro.

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

Opportunità uniche come offerte di prodotti molto richiesti o disponibili solo per un tempo limitato, alta possibilità di vincita, consigli di investimento intelligenti, ...

Richieste di dati/riconciliazioni dei dati di account online (dipendenti, clienti, utenti, membri, pazienti, ...)

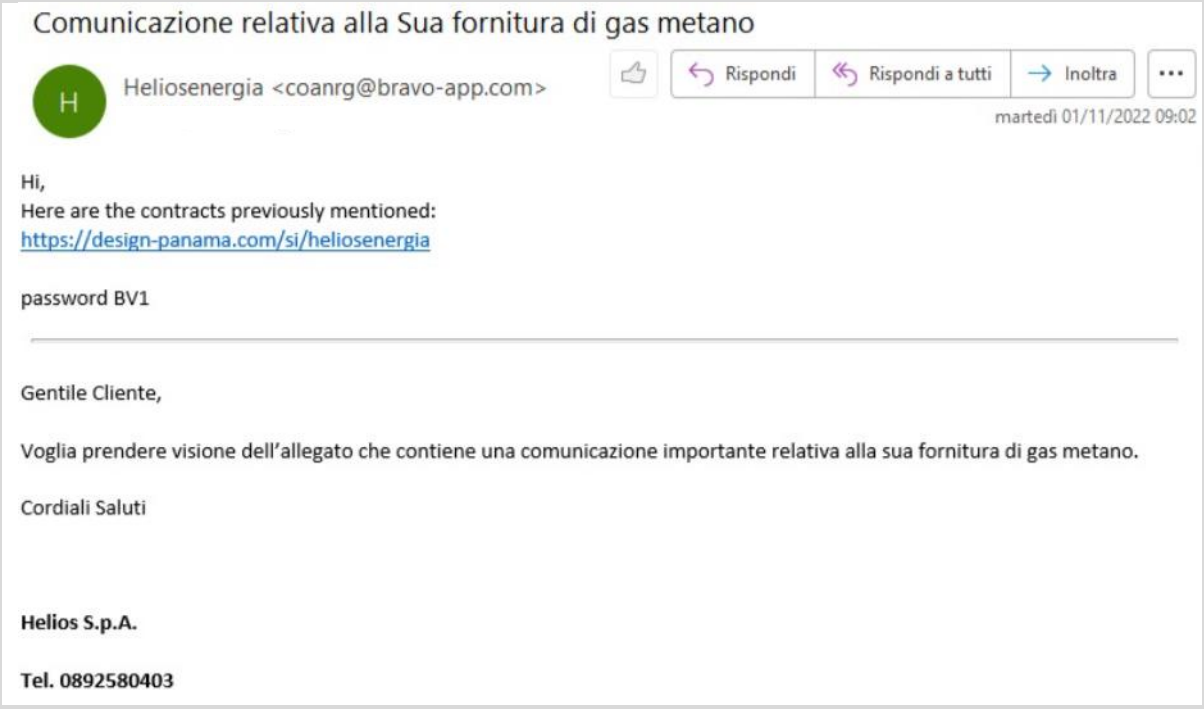
Istruzioni e richieste che mettono i lettori sotto pressione (per esempio in relazione a emergenze, omissioni, pericoli, ...)

Download o installazione di software o aggiornamenti di sicurezza
Richieste di password per la partecipazione a una videoconferenza

Richieste di dati/riconciliazioni dei dati per l'attivazione di uno strumento remoto (ad esempio manutenzione da remoto)

Siate sospettosi quando un'offerta arriva "come se fosse un segnale", quando un messaggio sembra attrarvi particolarmente. È meglio prendersi un momento e osservare i pensieri e i sentimenti che un messaggio scatena in voi. Una routine, un principio, una regola generale vi "guida"? Un'autorità vi "parla"? Risuona una paura? Un'opportunità fin troppo perfetta vi sta chiamando?
Se è così: fate un respiro profondo, pensate di nuovo, eventualmente fate qualche ricerca - e solo allora reagite. Oppure no.

Un esempio di come i criminali informatici hanno attaccato alcuni nostri clienti



Comunicazione relativa alla Sua fornitura di gas metano

H Heliosenergia <coanrg@bravo-app.com>

Rispondi | Rispondi a tutti | Inoltra | ...

martedì 01/11/2022 09:02

Hi,
Here are the contracts previously mentioned:
https://design-panama.com/si/heliosenergia

password BV1

Gentile Cliente,

Voglia prendere visione dell'allegato che contiene una comunicazione importante relativa alla sua fornitura di gas metano.

Cordiali Saluti

Helios S.p.A.

Tel. 0892580403

Nel caso in cui il malcapitato cliccasse sul link riportato nella email scaricherebbe a sua insaputa un malware!

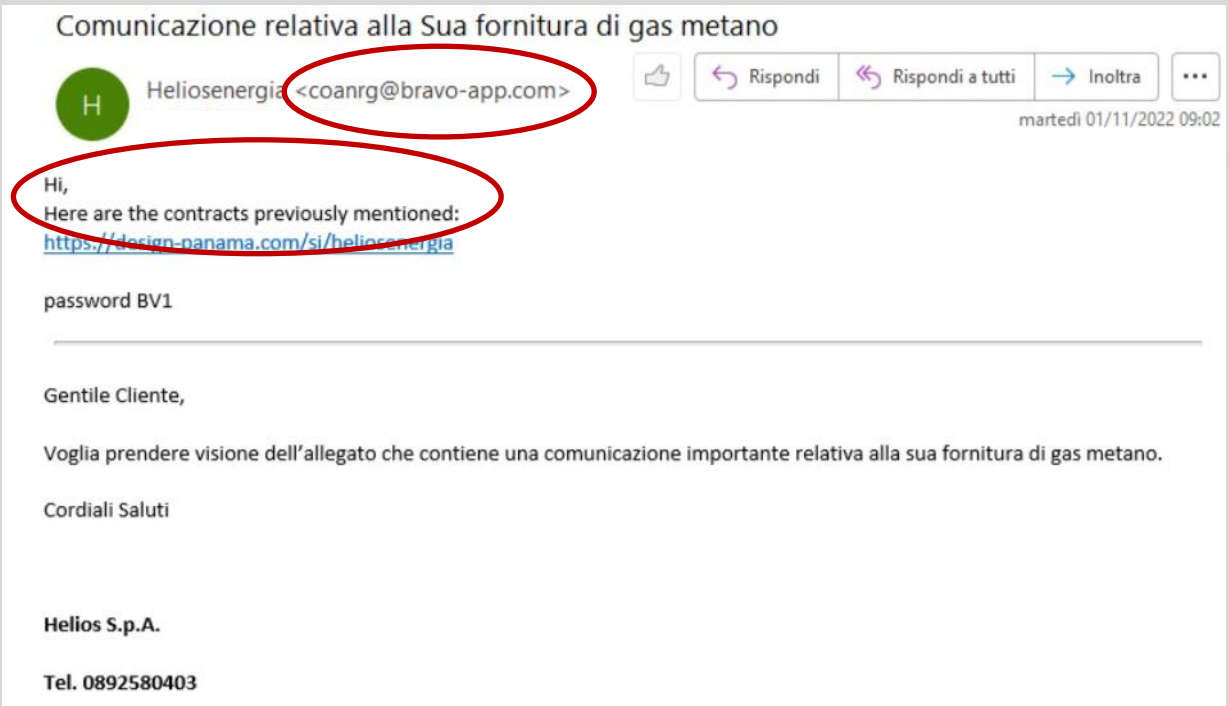
Malware o "software malevolo" è un termine generico che descrive un programma/codice dannoso che mette a rischio un sistema.
Ostili, invasivi e volutamente maligni, i malware cercano di invadere, danneggiare o disattivare computer, sistemi, reti, tablet e dispositivi mobili, spesso assumendo il controllo parziale delle operazioni del dispositivo. Proprio come l'influenza, interferiscono con il loro normale funzionamento.
Lo scopo dei malware è lucrare illecitamente a spese degli utenti. Sebbene i malware non possano danneggiare gli hardware fisici di un sistema o le attrezzature di rete, possono rubare, criptare o eliminare i dati, alterare o compromettere le funzioni fondamentali di un computer e spiare le attività degli utenti senza che questi se ne accorgano o forniscano alcuna autorizzazione.

Come difendersi da questi attacchi? Stando attenti, prudenti e sospettosi!

Anche se molto pericolose e ben congeniate questo tipo di comunicazioni ''malevoli'' non sono perfette e se si agisce con attenzione e prudenza si possono scongiurare le brutte sorprese.

Ritornando alla nostra email vi erano almeno due elementi sospetti:

- **l'email del mittente** <coangr@bravo-app.com>
- **il testo scritto in inglese.**


Comunicazione relativa alla Sua fornitura di gas metano

H Heliosenergia <coanrg@bravo-app.com>

Rispondi | Rispondi a tutti | Inoltra

martedì 01/11/2022 09:02

Hi,
Here are the contracts previously mentioned:
https://design-panama.com/si/heliosenergia

password BV1

Gentile Cliente,

Voglia prendere visione dell'allegato che contiene una comunicazione importante relativa alla sua fornitura di gas metano.

Cordiali Saluti

Helios S.p.A.

Tel. 0892580403

Gli attacchi malware non funzionerebbero senza l'ingrediente più importante: ***tu***. O meglio, una versione ingenua di te, disposta ad aprire allegati e-mail sconosciuti , cliccare su link o a installare qualcosa che proviene da una fonte inaffidabile.

In caso di dubbio cosa faccio?

Nel caso in cui arrivi una comunicazione da Helios che in qualche modo vi sembri sospetta, non aprite allegati e non cliccate su link, l'unica cosa da fare è contattare il vostro consulente energetico Helios di fiducia o chiamare direttamente il numero Helios:

> **089 2580403**

Helios S.p.A. non è da ritenersi responsabile per i danni generati da fake message e/o phishing che hanno indebitamente utilizzato il nome della Helios.

Di seguito i contatti certificati di Helios S.p.A., che potete trovare anche sul nostro sito www.heliosenergia.it

> **089 2580403**
> **349 602 2400**
> **info@heliosenergia.it**
> **heliosenergia@pec.it**

Potrebbero arrivare comunicazioni anche da email diverse dalle principali, perché inviate direttamente dall'indirizzo di posta aziendale del dipendente Helios o dell'ufficio di riferimento, ma in ogni caso i domini delle nostre email sono:

> **…@heliosenergia.it**
> **…@heliosenergia.store**

In conclusione.

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. 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.