SE VEN INFORMATICA

RICONOSCERE LE EMAIL SOSPETTE E DIFENDERSI DAL PHISHING

Consigli pratici da tenere a mente

Riconoscere un'eventuale Email Phishing

Se la email contiene solo testo e nessun **link** da cliccare o **allegato** da aprire, allora non rischiate una **"infezione" da virus** o un furto delle vostre credenziali. Occorre fare attenzione lo stesso per non cadere nella trappola del "ricatto" o essere indotti ad eseguire dei pagamenti a coordinate bancarie "diverse" dalle solite.

Se la email contiene **link** e/o **allegati** allora la "parola d'ordine" è **dubitare!**

Prima di cliccare su **link** o **allegati**, occorre fermarsi e dedicare del tempo ad analizzare la email.

Se c'è anche il minimo sospetto che qualcosa non "quadri", non farsi prendere dalla curiosità e sottoporre la email ad una analisi più accurata da parte del vostro consulente informatico.

1 | Analizzare il mittente

- verificate che l'indirizzo email e il nome siano "congruenti" (se ad esempio vedo una email provenire da **Rossi SRL** ma l'indirizzo è **tom.hardh@gmail.com** c'è qualcosa che non va);
- verificate che il nome del dominio sia corretto (se ad esempio ricevete una email da **clienti@amazzon.com** invece di **clienti@amazon.com**, dovete insospettirvi). Se non conoscete il nome di dominio corretto può essere utile una veloce ricerca su Google);
- state aspettando una email dal mittente indicato? Se non lo conoscete e/o non avete abituale scambio di email c'è sicuramente di che dubitare.

2 | Analizzare l'oggetto e il testo del messaggio

- esaminate il testo alla ricerca di eventuali **errori di ortografia o lessicali**, che potrebbero essere dovuti ad una sommaria traduzione da una lingua straniera da parte dell'autore del messaggio malevolo;
- controllate la presenza di eventuali **loghi** o **immagini conosciuti** (simbolo delle Poste, logo della banca, ecc..): solitamente in una email contraffatta si presentano in **bassa qualità** o con **qualche errore** nei colori o nelle forme;
- il testo ha un **significato o è un po' "strano"**? Se conoscete chi vi scrive, di solito usa la stessa terminologia? Vi da del "tu" o del "lei"? Vi saluta con un "buongiorno" o con un "ciao"?

3 | Analizzare il link con Urlscan.io

Se ci sono dei LINK nel testo della email potete passarci sopra con il mouse **(senza cliccarci sopra)** per vedere **l'indirizzo reale** della pagina che verrà aperta. Se ad esempio c'è un link del tipo **controlla email Google,** se ci andate sopra con il mouse e vedrete comparire ad esempio **"http://virusmalevolo.it"**, allora cestinate subito il messaggio. Se la pericolosità del link in anteprima non fosse così **"lampante"** o volete stare tranquilli, basta che vi posizionate con il mouse sopra al link e cliccate con il tasto destro scegliendo poi la voce **"copia collegamento ipertestuale".**

Andate sul sito **urlscan.io**, "incollate" l'indirizzo e cliccate su **PUBLIC SCAN**: oltre a vedere l'anteprima della pagina che si dovrebbe aprire vi verrà detto sei il link è **"Clean"** (buono) oppure **"Malicious"** (dannoso).

4 | Attenzione allo Spear Phishing!

Se l'analisi della email sembra aver superato tutti i controlli effettuati dovete comunque allertarvi se vi viene chiesto (anche dal vostro capo, titolare , superiore o fornitore) di effettuare un pagamento "strano" magari ad un indirizzo IBAN diverso dal solito.

Il mittente in questo caso potrebbe essere stato vittima di furto delle credenziali e chi vi sta scrivendo è in realtà l'hacker.

RISORSE E LINK UTILI

https://seveninformatica.it/sicurezza-informatica-e-phishing-come-difendersi/
L'articolo di approfondimento del nostro blog che affronta nel dettaglio l'Email Phishing.

https://www.youtube.com/watch?v=xTUkvzbqm8A&t=704s
Il nostro video di approfondimento su come riconoscere le Email sospette e su come difendersi prima che sia troppo tardi.

https://urlscan.io
Sito utile per la scansione dei link che trovate nelle potenziali Email Phishing.

https://phishingquiz.withgoogle.com
Mettetevi alla prova con il quiz basato sul riconoscimento di 8 email "dubbie", per verificare se siete in grado di riconoscere i tentativi di Phishing.

https://haveibeenpwned.com/
sito per verificare se il nostro indirizzo Email è stato violato.

CONTATTI

Via delle Industrie 2,
30020 Marcon VE

041 5348422

info@seveninformatica.it

seveninformatica.it