COME PROTEGGERSI DALLE FRODI ONLINE

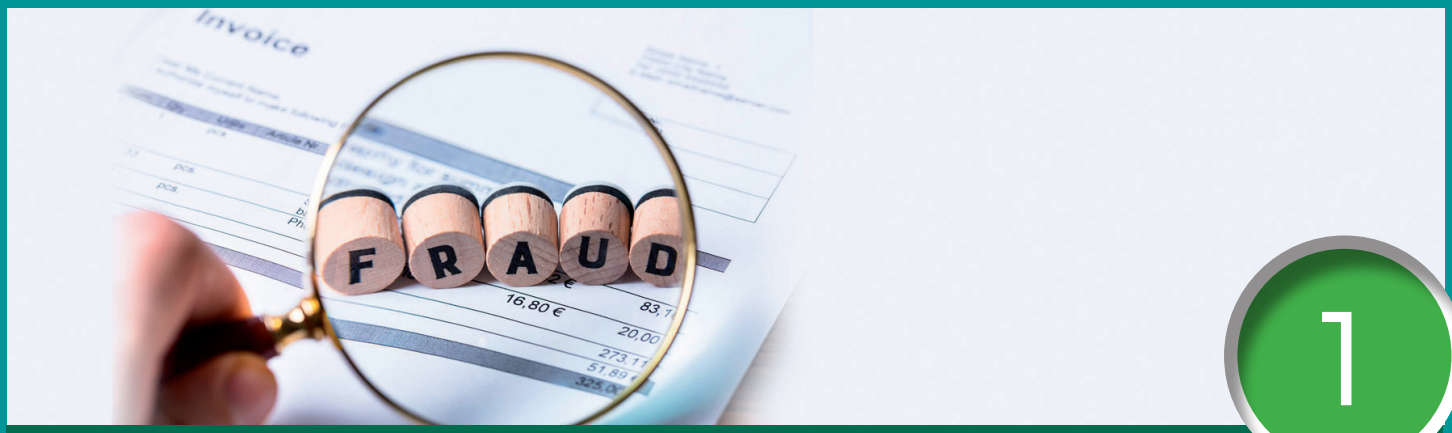
Creval
Gruppo CRÉDIT AGRICOLE

COME PROTEGGERSI DALLE FRODI ONLINE

Scopri come difendere la tua azienda
da possibili attacchi informatici
(Invoice Fraud | Malware| CEO Fraud)

Scopri di più nella sezione del nostro sito dedicata alla sicurezza
www.credit-agricole.it/sicurezza/categorie/frodi-online-per-le-aziende

Creval | Gruppo CRÉDIT AGRICOLE



1

INVOICE FRAUD

Il truffatore si sostituisce con l'inganno al fornitore per indurre l'azienda a modificare le coordinate da utilizzare per i pagamenti delle fatture.

Di cosa si tratta?

L'**Invoice Fraud** si verifica quando **il truffatore si sostituisce con l'inganno al fornitore** e notifica all'azienda nuovi riferimenti da utilizzare per i pagamenti delle fatture, fornendo indicazioni su fraudolenti riferimenti bancari alternativi
Il truffatore di solito si sostituisce al fornitore originale ma **potrebbe anche sostituirsi ad un collega di un'altra funzione aziendale**. I fondi fraudolentemente sottratti vengono spesso trasferiti rapidamente, quindi il recupero di denaro da conti fraudolenti può essere estremamente difficile
Anche in questi casi si possono verificare azioni per mettere pressioni sull'esecuzione della disposizione.

Tecnica

- **I truffatori sono spesso a conoscenza delle relazioni tra le società e i loro fornitori** e possono conoscere i dettagli sulle modalità di pagamento
- **La frode di solito viene scoperta solo quando il fornitore legittimo richiede notizie in merito ai mancati pagamenti**
- **Le lettere e le @mail fraudolente inviate alle aziende presentano a volte errori grossolani di sintassi**, ma sempre più spesso formulate in maniera corretta con maggiori difficoltà di individuazione della frode anche per una debole cultura delle aziende
- **La facilità di simulazione** degli indirizzi e-mail agevola le probabilità di successo della frode; in caso di PC infetti da malware, i criminali possono accedere e utilizzare indirizzi e-mail apparentemente autentici
- **Il processo di modifica dei dati bancari relativi a un pagamento** deve essere sempre effettuato con estrema cautela con particolare attenzione in presenza di un fornitore non abituale

Creval | Gruppo CRÉDIT AGRICOLE

Come difendersi?

- **Verifica sempre direttamente con il fornitore** ai riferimenti noti nei nostri archivi i dettagli di eventuali disposizioni di pagamento nuove e/o modificate e/o di importo elevato, in particolare se domiciliate su paesi esteri
- **Non basarti sulle istruzioni presenti nella mail** potenzialmente fraudolenta in quanto i truffatori possono falsificare gli indirizzi e-mail per farli apparire "autentici" o «molto attendibili»
- **Controlla con la massima attenzione la correttezza dell'indirizzo e-mail del mittente**, nel quale si possono riscontrare differenze, a volte minime rispetto a quello corretto
  - l'inversione o la modifica di una lettera rispetto all'indirizzo del cliente: **ACMELIMITED@abcd.com – AMCELIMITED@abcd.com**
  - il dominio @ diverso da quello normalmente utilizzato dal cliente: **ACMELIMITED@abcd.com - ACMELIMITED@efgh.com**
  - il suffisso (.com, .it), diverso rispetto a quello presente nell'indirizzo del cliente: **ACMELIMITED@abcd.com – ACMELIMITED@abcd.it**
- **Attenzione alle azioni di sollecito telefonico o via mail** se sospetti di una richiesta effettuata telefonicamente, prendi qualche minuto di tempo e richiama ad un suo recapito già in tuo possesso
  - I truffatori di norma cercano di indurre nell'errore – in questi casi, prendi il controllo della situazione
- **Se hai dubbi esamina attentamente la fattura e confrontala con altre precedenti** già ricevute e confermate come autentiche, in particolare i dettagli del conto bancario del beneficiario, la formulazione utilizzata, i riferimenti di contatto e il logo dell'azienda
- **Attenzione perché i bonifici nell'area PSD2** vengono effettuati solo in base al codice del rapporto (IBAN) e il riferimento relativo all'intestazione del beneficiario non viene di solito verificato dai sistemi bancari, pertanto è importante una verifica effettuata direttamente con il fornitore

2

MALWARE - AZIENDE

Installazione (non consapevole) di software sui pc aziendali per acquisire credenziali del remote banking e variare le coordinate bancarie dei bonifici disposti dall'azienda o interporsi negli scambi mail con fornitori per variare le coordinate di pagamento.

Di cosa si tratta?

I **malware** (parola composta da "malicious" e "software") sono programmi, collocati all'interno di oggetti (allegati, foto, video, ecc...) **progettati per danneggiare gli utenti e i loro dispositivi, ottenere accessi non autorizzati e rubare/danneggiare i dati**. Si trasmettono via internet, tramite posta elettronica, attraverso la semplice navigazione in internet o attraverso un semplice scambio di supporti come chiavette USB, schede di memoria e DVD/BlueRay.

In generale, il **cybercriminale** riesce a nascondere i codici malevoli su siti violati, in demo di video giochi, file musicali, barre degli strumenti, software gratuiti ecc...) in modo che vengano scaricati e si attivino senza che la vittima nemmeno se ne accorga. Tutto ciò di cui ha bisogno è una visita o un click al link malevolo e l'hacker ha già raggiunto il suo obiettivo. I malware più conosciuti sono virus e worm e devono la loro definizione alla loro modalità di diffusione.

Il termine **virus** viene usato per indicare programmi che si integrano con un qualunque codice eseguibile (incluso il sistema operativo) del sistema informatico vittima, in modo tale da diffondersi all'insaputa dell'utente. Per quanto riguarda i **worm**, questi sono software completi a sé stanti (senza la necessità di doversi integrare in altri programmi), e si diffondono su una rete autonomamente per infettare altri computer. Il virus per diffondersi richiede che l'utente scarichi o esegua un programma infettato (o anche solo il sistema operativo), mentre il worm non ha questo limite e si può diffondere liberamente ai computer collegati alla rete informatica.

Il malware può essere scaricato da qualsiasi piattaforma (cellulare, PC) **e può attaccare ogni tipologia di strumento informatico**: dai cellulari, tablet, laptop e desktop ai server e/o dispositivi di archiviazione.

Tipologie

Trojan horse

Si installa in modo occulto su un dispositivo con diverse finalità, quali ad **esempio raccogliere informazioni riservate e dati sensibili e password o per facilitare l'accesso non autorizzato al computer infettato**.
Non sono rilevabili di per sé ma il computer potrebbe risultare rallentato dall'uso notevole del processore e del traffico di rete;

Banking Trojan

Particolare categoria di malware che permette ai cyber criminali di **rubare le credenziali bancarie delle vittime** e, più in generale, di **effettuare frodi online**, provocando danni per importi ingenti. Per fare ciò i Banking Trojan effettuano quelli che sono chiamati attacchi "Man in the Browser" (MIB) in cui prendono il controllo del browser della vittima (es. Chrome, Firefox, Edge) riuscendo ad intercettare e modificare tutti i dati utilizzati dal browser stesso. Tra questi anche i dati, come le password, inseriti dalla vittima nei form delle pagine web, con l'obiettivo ultimo di effettuare frodi attraverso transazioni fraudolente dagli account delle vittime.

Spyware

Malware che vengono usati **per raccogliere informazioni di un utente o azienda** a loro insaputa per trasmetterle a un destinatario interessato.

Keylogger

Programmi in grado di registrare tutto ciò che un utente digita su una tastiera o che copia e incolla, rendendo così possibile il **furto di password o di dati** che potrebbero interessare qualcun altro.

Backdoor

Letteralmente "porta sul retro". Sono programmi che consentono un **accesso non autorizzato al sistema** su cui sono in esecuzione.

Rootkit

Tipo di malware che mira a **nascondere sia all'utente che agli antivirus l'esistenza di altri malware**.

Ransomware

Blocca l'accesso o cripta i dati o le funzioni del dispositivo al fine di richiedere il pagamento di un riscatto (es. wannacry...). Ancora peggiore è **cryptolocker**: si diffonde come allegato di posta elettronica apparentemente lecito e inoffensivo poiché sembra provenire da istituzioni legittime. Si tratta solitamente di un'eseguibile (.exe), mascherato con l'estensione ".pdf".

Come difendersi?

Dotarsi di un **buon Anti-Virus** e mantenerlo aggiornato è il primo passo: gli antivirus sono in grado di rilevare le minacce e di identificare il malware impedendogli di fare danni. Una volta installato l'antivirus:

- **Verificare che l'antivirus sia aggiornato**
- **Effettuare l'analisi regolare** (o "scan") **dei dispositivi**
- **Mantenere aggiornato il PC/Tablet/smartphone**: Non aprire mai gli allegati pericolosi: I virus vengono trasmessi il più delle volte tramite gli allegati delle e-mail che ricevi. I tipi di allegati comunemente usati dai virus sono:
  - **.exe**
  - **.pi**
  - **.scr**
  - **.vbs**
  - **.vbe**
  - **.hta**
  - **.cpl**
  - **.cmd**
  - **.bat**
  - senza dimenticare di far attenzione anche ai file **"zip"**: **ZIP**, **7Z**, **CAB**, **RAR**, che potrebbero nascondere dei file eseguibili. La lista non è esaustiva e tende a evolvere.
- **Fare attenzione anche gli allegati Microsoft Office**: per diffondersi e infettare i dispositivi, i virus possono utilizzare macro di file di Office (con estensione doc, ecc.).
- **Fare attenzione a non attivare automaticamente le macro senza essere assolutamente certi del file ricevuto**. Nel dubbio consultare il sito Microsoft. Fai attenzione durante la navigazione Internet: i virus vengono divulgati anche da siti web infetti, quindi evita i siti rischiosi come quelli pornografici, di download illegali, di giochi online, ecc. Alcuni antivirus offrono un modulo complementare che migliora la sicurezza della tua navigazione.
- **IMPORTANTE**
  La sicurezza dei dispositivi si basa in gran parte dei comportamenti tenuti durante la navigazione su internet e dall'attenzione prestata alla e-mail ricevute. Di solito, passa un po' di tempo dalla scoperta di un virus all'aggiornamento dell'antivirus, periodo durante il quale, se non si presta attenzione, il dispositivo è vulnerabile. È bene prestare attenzione anche alle mail ricevute dagli amici, che possono essere state infettate a loro insaputa.

Indipendentemente da dove l'hacker sia entrato, il risultato è lo stesso: **la tua azienda è stata violata!**

Che sia un computer di lavoro o un dispositivo personale ad essere stato infettato, il malware ora ha accesso a dati, password e qualsiasi cosa possa essere rubato. Quando il malware si introduce in un ambiente, è facile che questo tenti di replicarsi e infettare altri sistemi. Una volta che l'obiettivo infettato si connette alla rete aziendale, il malware può catturare dati e informazioni che vengono facilmente trasmessi al cyber criminale.

Per proteggere il patrimonio informativo aziendale, è opportuno quindi

- Cercare di ridurre i rischi identificando i dati sensibili, **creando specifiche policy** per proteggere i dati e controllare le attività di accesso
- Prevenire situazioni compromettenti attraverso un **percorso formativo al personale** su come identificare le e-mail di phishing oltre ad adottare soluzioni che prevengano software indesiderati
- **Rilevare le minacce**, identificando attività ed accessi utente anomali e/o sospetti e cercando i dispositivi infetti
- In caso di strumenti/device compromessi, **staccarli immediatamente dalla rete** una volta individuati
- **Isolare i dati sensibili**, fermando gli utenti e/o i dispositivi compromessi e impedendogli di entrare all'interno di applicazioni sensibili
- **Sostituire le password compromesse e riparare i dispositivi compromessi**

Creval | Gruppo CRÉDIT AGRICOLE

3

CEO FRAUD

I truffatori normalmente si sostituiscono ad una figura dirigenziale dell'azienda per spingere un collaboratore ad effettuare un pagamento, simulando istruzioni tramite mail, telefono, Whatsapp.

Di cosa si tratta?

La **CEO Fraud** è un tipo di frode compresa fra quelle rientranti nella **"social engineering"** L'ingegneria sociale è la **manipolazione di situazioni e persone da parte dei frodatori al fine di porre in essere trasferimenti di denaro o carpire informazioni riservate**.
I truffatori normalmente si sostituiscono con l'inganno ad una figura apicale dell'azienda - spesso lo stesso amministratore delegato - per disporre ad un collaboratore di effettuare un pagamento (mail, Whatsapp, telefono)

Tecnica

- La **CEO Fraud** è una **richiesta**, spesso effettuata via e-mail, che all'apparenza sembra provenire da una figura apicale dell'azienda o del Gruppo, **che richiede un pagamento urgente a un fornitore o un partner**
- Il tentativo di frode a volte si verifica quando la figura apicale è fuori sede e la richiesta di solito è riferita ad una presunta transazione per la quale è richiesta molta riservatezza, il tutto al fine di scoraggiare ulteriori verifiche da parte del dipendente "ingaggiato" o confronti interni alla struttura
- A volte, il truffatore tenta di convincere la vittima che la sua azienda sta per acquisire un'altra impresa e che il pagamento è necessario come acconto per l'accordo riservato
- In altri casi il sedicente CEO avvisa il dipendente che le disposizioni verranno impartite da altra persona di sua fiducia, di solito un avvocato di un noto studio legale

Come difendersi?

- **Verifica sempre direttamente con il cliente i dettagli** delle disposizioni di pagamento «dubbie» utilizzando i riferimenti già conosciuti e non basandoti sulle istruzioni presenti nella mail. I truffatori possono falsificare gli indirizzi e-mail per farli apparire "autentici" o con differenze marginali

- **Eventuali richieste di disposizioni di pagamento** ricevute tramite email, lettera o telefono devono essere sempre verificate senza utilizzare i recapiti presenti nella richiesta ma servendosi di quelli già noti

- **Non farti condizionare dai tentativi** di mettere pressione sulla rapidità o importanza di esecuzione motivate da questioni urgenti, anche se sembrano provenire dal management, che a volte chiedono di tralasciare le normali procedure di controllo (ricorda che questa è una tattica comune adottata dai truffatori)

- **Non lasciarsi intimorire** da un eventuale tono intimidatorio da parte del tuo interlocutore

- **Dubita di tentativi di persuasione accompagnati da promesse o prospettive di attenzione nei tuoi confronti**

- **Non divulgare, in ogni caso, informazioni di dettaglio** relative ai processi e/o alla normativa aziendale