



Taglio di Po, lì 07/03/2022

GENTILI CLIENTI

Loro sedi

## COME TUTELARSI DAI CRIMINI INFORMATICI

Gentile Cliente,

*il conflitto Russia-Ucraina e la crescita dei collegamenti delle attività svolte via Internet a causa della pandemia Covid-19 stanno comportando un'impennata dei crimini informatici.*

*I criminali informatici sono sempre alla ricerca di nuove soluzioni per sottrarre denaro ai navigatori su Internet, sia a soggetti fisici, sia a soggetti giuridici.*

*È molto importante infatti che tutti i datori di sensibilizzino i propri dipendenti su comportamenti appropriati nei collegamenti via Internet.*

*Presentiamo una breve guida su cosa sono i crimini informatici e su come difendersi.*

### Cosa sono i crimini informatici

Il **crimine informatico** rappresenta una minaccia sempre più attuale, considerando il numero in continua crescita di persone che si connettono a internet mediante portatili, smartphone e tablet, oltre che uno dei modi più redditizi di fare soldi nel mondo del crimine.

La maggior parte dei crimini informatici (ma non tutti), viene perpetrata da **cybercriminali o hacker** che intendono realizzare profitti illeciti.

Vi sono vari tipi di crimine informatico, suddivisibili principalmente in due categorie:

**a** i reati singoli, come l'installazione di un virus che ruba dati personali, e

**b** i reati ripetuti, come il cyberbullismo, l'estorsione, la distribuzione di materiale pedopornografico, o l'organizzazione di attacchi terroristici.

Alcuni crimini in particolare sono finalizzati allo sfruttamento commerciale della rete internet, altri insidiano i sistemi informativi di sicurezza nazionale di uno Stato.

### **Ma come possiamo difenderci da tutte queste minacce?**

L'agenzia europea **Europol**, che aiuta le autorità nazionali a contrastare le forme gravi di criminalità internazionale e il terrorismo, ha stilato un elenco di accorgimenti che contribuiranno a diminuire la possibilità di rimanere vittima di crimini informatici via Internet.



## Truffa dell'amministratore delegato, presidente o capo di azienda

La truffa del CEO si verifica quando un Dirigente e/o un dipendente autorizzato ad effettuare pagamenti viene indotto a pagare una fattura falsa oppure ad effettuare un trasferimento non autorizzato dall'account aziendale.

### Come funziona?

- Un frodatore chiama o invia un'email in qualità di figura di alto livello all'interno dell'azienda.
- Hanno una buona conoscenza dell'organizzazione.
- Richiedono un pagamento urgente.
- Utilizzano espressioni come: 'Riservatezza', 'La società si fida di te', 'Non sono al momento disponibile'.
- Fanno riferimento ad una situazione delicata (ad es. un controllo fiscale, una fusione, un'acquisizione).
- Il dipendente è invitato a non seguire le regolari procedure di autorizzazione.
- Le istruzioni su come procedere possono essere fornite in seguito, da una terza persona o via email.
- Il dipendente trasferisce i fondi su un conto controllato dal truffatore.
- Spesso, la richiesta è per pagamenti internazionali a banche al di fuori dell'Europa.

### Cosa puoi fare?

COME AZIENDA	COME IMPIEGATO
<ul style="list-style-type: none"><li>• Sii consapevole dei rischi e assicurati che anche i tuoi dipendenti siano informati.</li><li>• Invita il tuo staff a trattare le richieste di pagamento con cautela.</li><li>• Implementa protocolli interni relativi ai pagamenti.</li><li>• Implementa una procedura per verificare la legittimità delle richieste di pagamento ricevute via email.</li><li>• Stabilisci un processo di segnalazione per la gestione delle frodi.</li><li>• Rivedi le informazioni pubblicate sul sito web della tua azienda, limita le informazioni e sii prudente sui social media.</li><li>• Incrementa e aggiorna la sicurezza tecnologica.</li></ul> <p><b>!!! Contatta sempre la polizia in caso di tentativi di frode, anche se non sei rimasto vittima della truffa.</b></p>	<ul style="list-style-type: none"><li>• Applica rigorosamente le procedure di sicurezza in vigore per i pagamenti e le forniture. Non saltare alcun passaggio e non cedere alla pressione.</li><li>• Controlla sempre attentamente gli indirizzi email quando si tratta di informazioni sensibili/trasferimenti di denaro.</li><li>• In caso di dubbio su un ordine di trasferimento, consulta un collega competente.</li><li>• Non aprire mai link sospetti o allegati ricevuti tramite email. Presta particolare attenzione quando controlli la tua email privata sui computer aziendali.</li><li>• Limita le informazioni e sii prudente sui social media.</li><li>• Evita di condividere informazioni sulla struttura interna, sulla sicurezza o sulle procedure dell'azienda.</li></ul>

**!!! Se ricevi un'email o una chiamata sospetta, informa sempre il tuo dipartimento IT.**

## **Truffa della fattura (sostituzione e falsificazione)**

### **Come funziona?**

- Un'azienda viene avvicinata da qualcuno che finge di rappresentare un fornitore/un prestatore di servizi/ un creditore.
- Possono essere utilizzati vari approcci in combinazione tra loro: telefono, lettera, email, etc.
- I truffatori possono anche intromettersi nello scambio di email fra due aziende (o anche fra un privato ed un'azienda) e dirottando i pagamenti verso IBAN gestiti da loro.
- Il truffatore richiede che vengano modificate le coordinate bancarie per il pagamento delle fatture future (ad esempio i dettagli del beneficiario del conto bancario). Il nuovo account suggerito è controllato dal truffatore.

### **Cosa puoi fare?**

<b>COME AZIENDA</b>	<b>COME IMPIEGATO</b>
<ul style="list-style-type: none"><li>• Assicurati che i dipendenti siano consapevoli ed informati su questo tipo di frode e su come evitarla.</li><li>• Implementa una procedura per verificare la legittimità delle richieste di pagamento.</li><li>• Istruisci il personale responsabile del pagamento delle fatture per verificare sempre eventuali irregolarità.</li><li>• Rivedi le informazioni pubblicate sul sito web della tua azienda, in particolare contratti e fornitori. Assicurati che il tuo personale limiti ciò che condivide sulla società attraverso i propri social media.</li></ul>	<ul style="list-style-type: none"><li>• Verifica tutte le richieste che sostengono di provenire dai tuoi creditori, soprattutto se ti chiedono di modificare i loro dati bancari per le fatture future.</li><li>• Non utilizzare i dettagli di contatto indicati sulla lettera/ fax/email che richiede la modifica. Utilizza invece quelli della corrispondenza precedente.</li><li>• Definisci appositi Singoli Punti di Contatto con le società verso cui effettui pagamenti regolari.</li><li>• Limita le informazioni relative al tuo datore di lavoro che condividi sui social media.</li><li>• Quando paghi una fattura, invia un'email per informare il destinatario. Includi il nome della banca del beneficiario e le ultime quattro cifre dell'account designato, impostato per garantire la sicurezza.</li><li>• Per i pagamenti superiori ad una determinata soglia, imposta una procedura per confermare il conto bancario e il destinatario corretti (ad esempio un incontro con la società).</li></ul>



**!!! Contatta sempre la polizia in caso di tentativi di frode, anche se non sei rimasto vittima della truffa.**

### **Link utili**

---

La guida completa di Europol:

➤ <https://www.mizarsrl.it/wp-content/uploads/2022/01/Linea-guida-Europol-crimini-informatici.pdf>

Cordialmente  
Studio Duò e Associati