

Allerta Sicurezza Informatica – Rischi di frode e misure precauzionali

Gentile Cliente,

con la presente circolare desideriamo richiamare la Sua attenzione sul tema della sicurezza informatica. Negli ultimi mesi si è registrato

un aumento esponenziale di attacchi informatici ai danni delle piccole e medie imprese, non più mirati solo a "grandi gruppi", ma strutturati

per colpire l'operatività quotidiana di qualsiasi azienda e studio professionale.

La criminalità informatica è diventata estremamente sofisticata: non si tratta più solo di virus, ma di vere e proprie truffe ingegnerizzate per

ingannare l'utente.

⚠ Il caso più frequente: La truffa dell'IBAN (Man-in-the-Middle)

Vogliamo portarvi l'esempio di una frode recentemente accaduta a diverse realtà, nota come attacco *Man-in-the-Middle* o *BEC (Business*

E-mail Compromise):

1. I criminali riescono ad accedere alla casella e-mail di un fornitore o dell'azienda stessa (spesso tramite password deboli).
2. **Monitorano silenziosamente la corrispondenza** in attesa che vengano inviate o ricevute fatture.
3. Intercettano la mail contenente la fattura e la modificano (o ne inviano una successiva di rettifica), **sostituendo l'IBAN del fornitore**
4. **con un IBAN straniero o di un conto "mulo" gestito dagli hacker.**
5. Il cliente, fidandosi della mail apparentemente proveniente dal fornitore abituale, effettua il bonifico.
6. Quando il vero fornitore solleciterà il pagamento, ci si accorgerà che i fondi sono stati inviati a un soggetto terzo, spesso irrecuperabili.

Come difendersi: Buone prassi e Interventi Tecnici

Per mitigare questi rischi e proteggere il patrimonio aziendale, Vi invitiamo caldamente ad adottare le seguenti precauzioni:

- **Verifica Telefonica (Fondamentale):** Se ricevete una mail che comunica un **cambio di IBAN** o se la fattura riporta coordinate diverse
- dal solito, **contattate telefonicamente il fornitore** (usando i numeri già in vostro possesso) per chiedere conferma prima di pagare.
- **Consulenza Tecnica Specialistica:** La sicurezza "fai da te" non è più sufficiente. Vi consigliamo vivamente di **consultare tecnici**
- **informatici specializzati** per effettuare un controllo (audit) della vostra rete aziendale, verificare la robustezza delle difese attuali e
- valutare l'adozione di sistemi di protezione avanzati (firewall perimetrali, antivirus gestiti, sistemi anti-spam).
- **Autenticazione a due fattori (MFA):** Attivate l'autenticazione a due fattori su tutti gli account di posta elettronica e sui portali bancari.
- È la barriera più efficace contro gli accessi indesiderati.
- **Backup dei dati:** Assicuratevi di avere copie di backup dei vostri dati aziendali, possibilmente "offline" o scollegate dalla rete principale,
- per tutelarvi contro i *Ransomware* (virus che cifrano i dati chiedendo un riscatto).

La sicurezza informatica è un investimento necessario per la continuità del vostro business.

Lo Studio resta a disposizione per eventuali chiarimenti.

Cordiali saluti,

Studio Commerciale Giuliani