

La truffa dell'IBAN contraffatto

La truffa dell'IBAN contraffatto è una delle numerose frodi informatiche di cui spesso si sente parlare, e di cui anche i media riportano notizia.

Chi compie questo tipo di truffa cerca di farsi inviare denaro al proprio conto corrente sostituendo l'IBAN originariamente indicato per il pagamento della fattura con il proprio.

Ecco come funziona tipicamente la truffa:

- il soggetto malintenzionato viene in possesso delle credenziali per accedere all'applicazione di fatturazione o alla casella di posta elettronica utilizzata per la trasmissione delle fatture (fatture elettroniche o in PDF, ad esempio la fattura di cortesia)
- se il soggetto è in grado di accedere all'applicazione, può intervenire modificando l'IBAN della ditta e/o quello inserito nelle fatture in bozza
- se il soggetto è in grado di accedere alla casella di posta elettronica, può scrivere ai clienti rettificando l'IBAN a cui mandare il pagamento.

Come proteggersi

Per proteggersi da questo tipo di truffa, è importante adottare alcuni accorgimenti, parte dei quali valgono in generale per tutte le applicazioni informatiche:

1. Se già non l'avete, dotatevi di un efficiente software antivirus e antimalware e attivatelo su tutti i dispositivi che utilizzate (PC, tablet, smartphone, ecc.).
2. Cambiate la password dell'applicazione di fatturazione e della casella di posta, se è molto che non lo fate (e fatelo almeno trimestralmente). Adottate password sufficientemente complesse, del tipo:
 - a. lunghezza pari o superiore agli 8 caratteri
 - b. utilizzo di caratteri maiuscoli, minuscoli, numeri, lettere e segni di interpunzione
 - c. password non riconducibile ad una parola di senso compiuto o contenente numeri, date, o nomi riconducibili al titolare.
3. Se avete il sospetto che soggetti terzi non autorizzati abbiano fatto accesso alla vostra casella di posta, dotatevi di un'altra casella di posta e create o fatevi creare un nuovo account (che userà il nuovo indirizzo e-mail) per accedere all'applicazione di fatturazione.
4. Controllate sempre con attenzione le informazioni bancarie riportate in fattura e nei dati della Ditta.
5. Controllate le fatture emesse, verificando che l'IBAN inserito sia effettivamente quello atteso.
6. Non condividete MAI le credenziali di accesso all'applicazione di fatturazione e alle caselle di posta con soggetti terzi, soprattutto via e-mail o telefonicamente.
7. Evitate di memorizzare le credenziali sul PC o sul browser per gli utilizzi successivi a meno che non siate assolutamente sicuri della sicurezza del dispositivo.
8. Controllate sempre l'identità dei siti in cui digitate la password per evitare di inserirle su siti contraffatti gestiti da malintenzionati (cosiddetto "phishing").
9. Evitate di riportare le password su fogliettini volanti, di memorizzarle sui telefonini o di scriverle su file facilmente accessibili a terzi.
10. Evitate di accedere a internet sfruttando le reti wi-fi pubbliche.

Se effettuando i controlli sulla vostra applicazione di fatturazione riscontrate anomalie sospette, scrivete a gestione.utenti@sistemi.com riportando Ragione sociale e Partita IVA della ditta interessata.
