Spettabili Clienti

Loro sedi

CIRCOLARE N. 19 – 24 OTTOBRE 2019

NUOVI TENTATIVI DI TRUFFA

Riteniamo opportuno segnalarVi questi nuovi tentativi di truffa che circolano nella posta elettronica o attraverso la clonazione delle SIM card.

PHISHING VIA PEC
Attenzione alle false mail sulla fatturazione elettronica

Con un Comunicato Stampa dello scorso 14 ottobre 2019 (consultabile al seguente link *Comunicato Stampa*), l'Agenzia delle Entrate torna a mettere in allerta i contribuenti sulle nuove mail di *phishing* via PEC, che stanno arrivando in questi ultimi giorni e sono relative alla fatturazione elettronica con l'obiettivo di raccogliere informazioni da utilizzare per frodare il destinatario.
Le mail hanno come oggetto la dicitura "Invio File <XXXXXXXXXX>".
Nel mirino ci sono soprattutto le caselle PEC di strutture pubbliche, private e di soggetti iscritti a ordini professionali.
Attenzione, la truffa è ben architettata. Il testo del messaggio è verosimile poiché ripreso da una precedente e lecita comunicazione inviata dal SDI.

Nell'*alert* l'amministrazione ricorda come riconoscere **un vero messaggio PEC del SDI**:

- il mittente è solo del tipo ***sdiNN@pec.fatturapa.it*** dove NN è un progressivo numerico a due cifre;
- il messaggio **deve contenere necessariamente due allegati** composti in accordo alle specifiche tecniche sulla fatturazione elettronica (pubblicate sul sito dell'Agenzia delle entrate).

Nell'informare i cittadini della sua assoluta estraneità all'invio di tali missive ingannevoli, l'Agenzia consiglia di non aprire mail provenienti da utenze sconosciute o sospette che richiedono di modificare l'indirizzo di recapito per le successive comunicazioni con il Sistema di interscambio (SDI) e di cestinarle immediatamente.

Cogliamo l'occasione per ricordare ancora una volta che la PEC (posta elettronica certificata) ha valenza legale e va controllata abitualmente in quanto attraverso la stessa vengono notificati eventuali accertamenti tributari e/o previdenziali, multe, comunicazioni da Enti vari e per cause civili, ecc.

FRODI DELLE SIM CARD CLONATE PER HOME BANKING

Purtroppo si sta diffondendo anche in Italia **la clonazione di SIM card** per smartphone, che consente ai malviventi di **controllare il sistema di home banking** (app, codici, generatore di password, SMS di conferma, ecc.) installato dal legittimo proprietario (anche in Studio è successo a un nostro collaboratore, ma fortunatamente è riuscito a bloccare il tentativo giusto in tempo).

C.F. - P.IVA 09288750962
Viale Brianza, 19 - 20821 Meda (MB) +39 0362 70653 r.a.
studiofusetti@studiofusetti.com
www.studiofusettiassociati.com

La SIM viene clonata e il truffatore è libero di accedere ai dati memorizzati sul cellulare e quindi di effettuare operazioni bancarie per conto del legittimo titolare frodato.

Paradossalmente, il boom delle frodi legate alle SIM clonate dipende proprio dal rafforzamento di alcune misure di sicurezza dei conti correnti online, come l'uso del numero di telefono come secondo fattore di autenticazione (il cosiddetto token software) al posto delle vecchie "*chiavette*" (i token fisici), oppure l'invio del messaggio di verifica tramite SMS.
Come al solito, però, tutto parte dalla raccolta dei nostri dati personali presenti online e dal furto della nostra identità.

Il suggerimento è **prevenire**: evitare di dichiarare troppi dati personali nei propri profili online, specialmente quelli dei social network, per impedire la raccolta automatizzata dei nostri dati.

Lo Studio rimane a disposizione per ogni ulteriore chiarimento.
Cogliamo l'occasione per porgere cordiali saluti.

STUDIO FUSETTI E ASSOCIATI

Le circolari e gli articoli pubblicati sono consultabili anche sul sito dello Studio al seguente link https://studiofusetti.com/

C.F. - P.IVA 09288750962
Viale Brianza, 19 - 20821 Meda (MB) +39 0362 70653 r.a.
studiofusetti@studiofusetti.com
www.studiofusettiassociati.com