VADEMECUM INFORMATIVO FRODI ONLINE

- **Navigare su siti sicuri**

Quando si utilizza la rete, navigando su un sito, il primo fattore da verificare è la sicurezza dello stesso. Occorre dunque verificare che la pagina web prescelta sia contrassegnata dalla presenza di un *lucchetto*, caratterizzata dall'estensione *https* in luogo della semplice estensione *http*, visualizzabile nella barra degli indirizzi del browser di navigazione. La presenza di tali indicatori garantisco che il sito prescelto sia sicuro ed affidabile, potendo dunque concludere acquisti attraverso i propri sistemi di pagamento prescelti.

- **Attenzione alle offerte troppo allettanti**

Sulla rete è facile rinvenire offerte molto allettanti e prezzi stracciati, ma quando il prezzo del prodotto appare particolarmente ribassato, è buona norma andare cauti: dietro tale convenienza potrebbe celarsi un falso od una truffa. Occorrerà dunque verificare su siti diversi la bontà dell'offerta e del prodotto attenzionato.

- **Software al passo coi tempi**

Per navigare sicuri è inoltre necessario avvalersi di strumenti informatici che siano in grado di tutelare la nostra incolumità in rete: premunirsi sempre di aggiornare il browser di navigazione ed il sistema operativo all'ultima versione disponibile, oltre a munirsi di un software antivirus.

- **Occhio a recensioni e feedback**

È sempre buona norma dare una occhiata alle varie recensioni degli altri utenti del web sul prodotto o sito prescelti.

- **Verificare le informazioni disponibili sui siti**

Prima di completare qualsiasi tipo di acquisto è buona norma verificare che il sito prescelto sia fornito di riferimenti quali numero di P.IVA, numero di telefono fisso, un indirizzo fisico e ulteriori dati per contattare l'azienda. Un sito privo di tali dati probabilmente non risulterà affidabile. Inoltre i dati fiscali indicati possono facilmente essere verificati sul sito istituzionale dell'Agenzia delle Entrate.

- **Diffidate da chi richiede troppi dati**

Per finalizzare una transazione online sono richiesti pochi dati fondamentali: numero di carta, data di scadenza della stessa ed indirizzo per la spedizione della merce. Qualora venissero richiesti ulteriori e non pertinenti dati sensibili, deve suonare il campanello d'allarme!

- **La carta *ricaricabile* presta maggiori garanzie**

Scegliendo quale metodo di pagamento la carta ricaricabile, si minimizzano i rischi, in quanto nel malaugurato caso di una truffa si perderà unicamente il plafond disponibile sulla carta. Conseguentemente il consiglio è quello di mantenere un plafond minimo, utile al completamento dell'acquisto del prodotto prescelto.

Dal punto di vista psicologico la carta prepagata può dare un senso di maggiore sicurezza perché la si può ricaricare del giusto per pagare un acquisto e quindi poi lasciarla vuota. Ma in realtà la legge protegge il titolare di qualsiasi tipo di carta e di app da utilizzi fraudolenti. In caso di usi fraudolenti bloccare la carta o qualsiasi altro strumento di pagamento con una telefonata all'emittente o alla banca o istituto di pagamento e quindi fare denuncia alle Autorità. Nulla potrà essere addebitato al titolare. In caso di problemi è bene fare reclamo per iscritto all'emittente che deve rispondere entro 15 gg lavorativi e poi ricorso all'Abf. Ovviamente evitate di pagare qualsiasi acquisto di un bene o di un servizio facendo una ricarica su una prepagata riconducibile ad una terza persona, anche se indicata dall'esercente.

- **La truffa del *phishing***

Metodologia di truffa online che viene perpetrata tramite mail truffaldine, che spesso richiedono di cliccare su un link indicato che reindirizza su un sito truffa. L'indirizzo a cui il link fa riferimento solitamente differisce, per qualche minuzia, da quello originale. Non rispondere mai a mail che richiedono dati personali, dati di pagamento, dati bancari o documentazione personale.

- **Attenzione a fornire i tuoi documenti a malintenzionati**

Spesso viene richiesto di inviare copia dei propri documenti personali. È bene farlo solo se strettamente necessario ed unicamente se sicuri della affidabilità con cui vengono trattati i tuoi dati personali. Inoltre, in caso di variazione dell'indirizzo di residenza, comunica tempestivamente il tuo nuovo recapito alla tua banca e a tutti i soggetti con cui intrattieni rapporti. Più in generale custodisci le tue informazioni che ti riguardano e non lasciarti convincere a fornire i tuoi dati a persone che non conosci a meno che non sussistano motivazioni reali.

- **Attenzione alla privacy**

L'identità digitale va tutelata: utilizzare mail dedicate appositamente ed unicamente alle varie iscrizioni online, settare al massimo il livello privacy dei vari social network, attenzione estrema alle foto ed ai dati personali che si sceglie di promulgare: sono terreno feritile per i truffatori.

- **Tieni sotto stretto controllo i movimenti del tuo conto corrente**

Effettua spesso un controllo del saldo del tuo conto corrente, al fine di individuare prontamente eventuali addebiti fraudolenti.

Nel caso in cui si sia malauguratamente incorsi in una truffa online:

1. Avvisare prontamente il proprio Istituto di credito, bloccando eventuali carte di pagamento o disconoscendo eventuali disposizioni di bonifico effettuate fraudolentemente.

2. Presentare immediata denuncia alle autorità competenti, preferibilmente presso la Polizia Postale.

3. Stampare tutti i documenti contabili che evidenziano l'operazione fraudolenta subita.

4. In caso di truffa avvenuta per mezzo di mail, sms o chat *whatsapp*, stampare tutte le conversazioni intercorse.

5. Rintracciare eventuali numeri di telefono da cui si sono ricevute eventuali chiamate sospette: annotare data ed ora.

6. Evitare di rispondere ad ulteriori mail o telefonate sospette.

7. Attenzione massima ad eventuali chiamate o mail da parte di soggetti che offrono aiuto per recuperare il maltolto: sono sempre gli stessi truffatori.

8. Consultare preferibilmente un avvocato esperto di frodi informatiche che saprà indirizzarvi relativamente al caso concreto ed avviare le necessarie azioni tese al recupero di quanto indebitamente sottratto.

***

Tipologie di attacchi informatici e problematiche collegate.

Un importante accenno deve essere, infine, svolto in merito alle modalità operative di alcuni attacchi informatici che rappresentano una notevole criticità nelle transazioni bancarie.

All'interno di tale categoria il *Man in the browser* rappresenta una aggressione informatica particolarmente pericolosa in quanto capace di assumere il controllo di una transazione bancaria completa insaputa della vittima.

A differenza del *Man in the middle* (dal quale trae origine), in cui un soggetto si interpone nella comunicazioni on line di due persone, instaurando con loro autonome comunicazioni e creando tra loro la parvenza di stare interagendo tra loro, il *Man in the browser* sfrutta la vulnerabilità del browser di navigazione della vittima per controllare le sessioni su di esso svolte.

Ciò è reso possibile dalla inoculazione nel pc della vittima di un *malware* che resta dormiente, ma che agisce come una spia silenziosa monitorando tutte le navigazioni svolte sul browser della macchina infettata. Tale programma malevolo si attiva unicamente quando i registri di navigazione si indirizzano su siti finanziari o bancari. In quel momento, cioè l'inizio della transazione finanziaria, il *malware* si attiva rendendo possibile il controllo dell'intera operazione da parte del portatore dell'attacco.

La vittima inconsapevolmente cederà le proprie credenziali e password operative l'attaccante nella convinzione di stare risolvendo un problema di blocco all'accesso di *home banking* oppure nella convenzione di operare nel reale ambiente di un banking bancario, mentre invece si trova su di una "*fake page*" creata appositamente dal malfattore.

La pericolosità di questo attacco è rivelata, quindi, non solo dalle sue modalità operative che di fatto spiazzano la vittima non permettendogli di avvedersi della frode in suo danno in tempo reale, ma soprattutto dalla capacità di questo *malware* (appartenente alla famiglia di *Trojan*) di sfuggire ad ogni presidio antivirus presente nel pc infettato.

L'attacco descritto, di fatto, aggira il presidio di sicurezza dell'autenticazione forte in quanto agisce non sul sistema di home banking dell'istituto di credito, bensì sul browser di

navigazione, permettendo la captazione delle *one time password* inviate in sicurezza alla vittima.

Proprio il tema delle *one time password* introduce un ulteriore attacco informatico altamente aggressivo : quello del Sim swap fraud.

In questo attacco la vittima viene colpita attraverso il proprio smartphone, quale strumento deputato alla ricezione delle password autorizzative dell'operazione bancaria on-line (OTP).

Da un punto di vista operativo tale attacco aggredisce la SIM del telefono cellulare della vittima, in quanto il portatore dell'attacco attraverso un falso documento di identità richiede la sostituzione della scheda Sim della vittima al dealer di servizi di telefonia presso cui è attiva, con conseguente disabilitazione di quella in uso al soggetto colpito.

Con tali modalità esecutive, quindi, si perviene ad una sostituzione della scheda Sim in uso alla vittima, la quale totalmente ignara di quanto sta accadendo rileverà soltanto un cattivo funzionamento del proprio apparato cellulare non associando quanto sta accadendo alla violazione dei suoi dati ed alla truffa in atto.

Sostituita quindi la Sim card l'autore del reato accede all'account bancario del soggetto colpito, reimpostando le credenziali e operando disposizioni sul conto corrente on-line in piena autonomia.

La vittima ovviamente se ne accorgerà con ritardo in quanto spesso attribuisce il mancato funzionamento del proprio cellulare a problemi di connessione o a problemi di elettronica dello stesso.

Questa ultima tipologia di truffa digitale evidenzia la criticità che può determinarsi dall'invio della OTP sull'utenza cellulare del cliente.

Occorre premettere che la Direttiva 2015/2366 prima ed il regolamento delegato UE 2018/ 389 del 27 novembre 2017 poi hanno recepito la necessità di tecniche innovative per fronteggiare le minacce le sicurezza dei pagamenti elettronici indicando l'autenticazione forte del cliente come una soluzione per collegare in modo dinamico l'operazione all'importo e al beneficiario specificati dal pagatore nel momento in cui dispone l'operazione stessa.

Il suddetto collegamento dinamico è reso possibile dalla generazione di codici di autenticazione maggiormente sicuri quali password monouso e l'impiego di crittografie avanzate.

L'autenticazione forte, cioè quella multifattore, trova la sua sicurezza in precise caratteristiche che la citata normativa regolamentare europea riconosce con i seguenti termini:

- Qualcosa che solo l'utente conosce (*id* di accesso)

- Qualcosa che solo l'utente possiede (Password)

- Qualcosa che caratterizza l'utente (dato biometrico o altro)

In estrema sintesi gli elementi dell'autenticazione forte possono essere riassunti in:

- un codice identificativo di accesso di varia lunghezza (qualcosa dell'utente solo conosce);

- una password (qualcosa che solo l'utente possiede) e qualcosa che appartiene alla categoria della inerenza (e quindi qualcosa che caratterizza peculiarmente l'utente) quali ad esempio un sensore biometrico.

Ulteriore elemento di sicurezza di questo sistema è **l'indipendenza** degli elementi descritti, i quali devono tra loro essere generati separatamente quale ulteriore elemento di sicurezza dell'apparato informatico descritto.

È di tutta evidenza come l'operatività della truffa sim swap possa aggirare tale apparato, andando ad agire direttamente sulla ricezione di uno dei fattori di sicurezza descritti.

Un discorso a parte vale poi per le App dalle quali è possibile operare a distanza sul proprio conto corrente, nelle quali vi è in ipotesi una eccessiva vicinanza nella generazione dei fattori caratterizzanti l'autenticazione forte. Qualora venga compromessa l'indipendenza dei fattori descritti , infatti, cadrebbe la sicurezza stessa su cui si fonda tale metodica di autenticazione.

Non appare in ogni caso condivisibile che la ricezione del terzo fattore di autenticazione forte sia affidato alla ricezione di un apparato tecnologico di proprietà del cliente-utilizzatore di strumenti di pagamento.

Infatti l'intera sicurezza della autentificazione sull'account bancario on-line deve essere predisposta dall'istituto di credito stesso, quale contraente maggiormente in grado secondo ormai pacifica giurisprudenza di sostenere il rischio economico legato alle transazioni on-line. Spostare una parte del rischio sulla telefonia cellulare del cliente porta ad una esposizione dell'utente a rischi informatici, quali quelli del Sim swap fraud, che potrebbero essere composti ed abbattuti dalla costruzione di apparati di ricezione di tali codici OTP curati dal prestatore di servizi di pagamento all'interno dei presidi di sicurezza imposti dalla disciplina europea.