



COMUNE DI RESCALDINA

Città Metropolitana di Milano



**TRUFFE INFORMATICHE
CONOSCERLE PER IMPARARE
A DIFENDERSI**

L'Amministrazione Comunale, nell'ambito delle iniziative volte ad informare la cittadinanza sui temi delle truffe, ha realizzato questo breve opuscolo con lo scopo di dare una prima e sicuramente non esauriente informativa, rispetto alle truffe informatiche.

Il modificarsi delle abitudini che ci hanno portato ad utilizzare sempre di più la rete per portare a termine diverse attività (acquisti, gestione del conto corrente, social network ecc.), ha contribuito a rendere particolarmente appetibile questo ambito a coloro che, senza scrupoli, traggono enormi vantaggi dalle truffe informatiche.

Chiunque può cadere vittima di questi raggiri perché, chi li studia e li mette in atto, è un vero professionista in grado di trarci in inganno attraverso tranelli davvero ricercati.

A seguito di riflessioni emerse nel "Gruppo Sicurezza" del quale fanno parte anche alcuni cittadini, ci è sembrato utile ed opportuno affrontare questo aspetto delle truffe che, purtroppo, colpisce a 360° ed in modo particolare chi ha poca conoscenza degli strumenti informatici.

Ricordatevi che le forze dell'ordine sono fortemente impegnate nelle attività di contrasto alle truffe e assistono sempre le vittime di questo odioso reato pertanto è fondamentale sporgere sempre denuncia.

Per prevenire questo tipo di truffe è necessario seguire alcuni accorgimenti, facili da ricordare, che abbiamo raccolto in questo opuscolo.

La Polizia Locale ed i Carabinieri sono sempre a Vostra disposizione, non esitate a contattarli: meglio un falso allarme che una truffa riuscita!

*L'Assessore alla Polizia Locale
Gianluca Crugnola*

*Il Sindaco
Gilles André Ielo*

LE INSIDIE DELL'ERA MODERNA

La diffusione sempre più capillare di internet e la diminuzione dei costi per avere una connessione sia mobile che fissa, consente alle persone di qualsiasi età, di avere accesso a moltissime informazioni da qualsiasi parte del pianeta e l'informatizzazione globale può portare a pensare che tutto sia affidato alla



tecnologia, senza rendersi conto che dietro questa tecnologia possono nascondersi persone che, a volte, la utilizzano in maniera fraudolenta.

Internet è la primaria fonte di informazione per la maggior parte della popolazione mondiale ma, purtroppo, la rete nasconde il rischio, spesso sottovalutato od ignorato, di cadere vittime di frodi informatiche.

Naturalmente, tale rischio è tanto più elevato quanto minore è la conoscenza del computer, di internet e delle nuove tecnologie in generale.

È dunque essenziale, specialmente per chi ha poca familiarità con la rete, conoscere quali siano i possibili rischi a cui ci si espone quando si naviga in internet con il computer o con qualsiasi dispositivo mobile ed ancora più importante conoscere le strategie di base per difendersi.

Risolvere le problematiche che derivano da un furto d'identità o da un prelievo non autorizzato dal proprio conto corrente, a volte può essere davvero un calvario con strascichi che possono durare anche anni.

Per questo è fondamentale denunciare sempre, perché l'informativa alle Forze dell'Ordine permette loro di conoscere le diverse strategie utilizzate e mettere in campo azioni preventive.

COSA SONO LE TRUFFE INFORMATICHE?



Con frode informatica si intendono tutte quelle operazioni illecite e di rilevanza penale, che riguardano l'uso di apparecchiature informatiche o telematiche.

I pirati informatici o “hacker”, sono dei veri e propri specialisti informatici con una grande conoscenza in materia che studiano i sistemi di sicurezza ed i modi di violarli.

Lo scopo di una frode informatica è sempre quello di trarre un profitto personale quindi ottenere servizi gratuiti o clonare gli account degli utenti, per usufruire di determinati servizi.

Tra le frodi più comuni possiamo individuare:

- Memorizzazione dei dati delle carte di credito
- Trasmissione dei dati delle carte di credito
- Intercettazione di codici
- Dirottamento dei dati personali
- Furto di dati o credenziali

QUALI SONO LE TRUFFE PIÙ COMUNI?

Sostanzialmente le truffe informatiche si dividono in due grandi macro categorie: il furto d'identità ed il Phishing.

Furto d'identità

In generale si ha un furto di identità ogni qualvolta un'**informazione individuale**, relativa ad una persona fisica o giuridica, è ottenuta in modo fraudolento da un criminale con l'intento di assumerne l'identità per compiere atti illeciti.

Al furto di identità può conseguire sia un danno economico sia un danno morale/psicologico, correlato allo stress emotivo dovuto alla sensazione di impotenza che genera rabbia e/o paura, nonché un danno dovuto all'impegno di

tempo ed energia necessari per risolvere i problemi scaturiti alla frode, come quello di ricostruire il proprio profilo digitale.

Questa frode è in assoluto la più temibile e, purtroppo, la più diffusa perché può colpire chiunque anche chi non ha mai navigato in rete.



Le Nostre identità infatti, sono contenute in moltissimi data base anche istituzionali (contratti per utenze, carte fedeltà, sistema sanitario, amministrazioni comunali ecc.) e, talvolta, non sono protette adeguatamente permettendo agli hacker di violare i sistemi ed impadronirsi dei dati personali.

Il furto d'identità ha diversi scopi:

- la clonazione dell'identità, ossia la sostituzione di persona con l'obiettivo di creare una nuova identità e un nuovo tipo di vita;
- utilizzare i dati identificativi di un individuo per ottenere crediti, prestiti finanziari, aprire conti correnti in nome della vittima;
- utilizzare i dati della vittima per compiere in sua vece atti pubblici illeciti di varia natura, come attivare nuove carte di credito o telefoni cellulari o altri account;
- servirsi dei dati personali di soggetti diversi che vengono combinati per costruire "in laboratorio", completamente o parzialmente, una nuova identità in base alle proprie necessità;
- avvalersi dei dati personali altrui per ottenere prestazioni sanitarie;
- costruzione di una nuova identità diversa da quella originaria appropriandosi di dati di una persona defunta.

Qualunque sia lo scopo del furto d'identità, il malcapitato si ritroverà a dover affrontare un percorso non privo di difficoltà, per poter "ripulire" la propria identità e poter tornare a vivere la sua vita normalmente.

Phishing



È un tipo di frode ideata per sottrarre alla vittima informazioni riservate come il numero della carta di credito, password o credenziali di accesso ad account personali e dati bancari.

Le modalità con le quali i truffatori possono sottrarre i dati sono diverse: **e-mail, siti web appositamente progettati, banner pubblicitari, messaggi ingannevoli inoltrati tramite whatsapp, messenger, Facebook od altri social.**

Normalmente il messaggio fasullo, si presenta come una notifica ufficiale proveniente da una fonte autorevole, una banca un'istituzione, un fornitore di servizi. L'hacker, con espedienti molto sofisticati, cerca di convincere il malcapitato ad effettuare azioni precise come cliccare su un link, effettuare una determinata procedura per risolvere un "finto problema" come il blocco di un conto corrente, una carta di credito o il ripristino di un account.

Se si cade nel tranello, i dati indicati vengono immediatamente trasmessi al truffatore che poi li utilizzerà per trarne profitto.

Nel corso degli anni il "Phishing" si è evoluto e trasformato diventando più "smart": i malfattori infatti, tentano di carpire i nostri dati attraverso **telefonate** od **SMS**.

Con le telefonate, il truffatore, fingendo di essere un operatore della banca, contatta la vittima di solito per avvertirla di un tentativo di truffa a suo danno e, con questo pretesto, cerca di ottenere informazioni riservate (ad es. il PIN della carta o i codici bancari).

Con l'SMS viene chiesto alla vittima di contattare un determinato numero o di collegarsi tramite un link a un sito ed ecco che un semplice clic o una telefonata possono segnare l'inizio dell'incubo.



COME POSSIAMO DIFENDERCI?

Gli hacker sono dei veri professionisti e quindi dobbiamo prestare la massima attenzione quando navighiamo o quando ci viene richiesto di fornire dati relativi alle credenziali di accesso, codici delle carte di credito o dati bancari.

Vediamo allora come possiamo difenderci.

Navigazione siti web



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 garantisce 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.



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 (www.agenziaentrate.gov.it).

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.

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.



La legge protegge comunque 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.

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 intratteni rapporti.

Più in generale custodisci le 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 assolutamente tutelata.

Consigliamo di utilizzare mail dedicate appositamente ed unicamente alle varie iscrizioni online, settare al massimo il livello privacy dei vari social network, prestare estrema attenzione alle foto ed ai dati personali che si sceglie di pubblicare: sono terreno fertile per i truffatori.



Occorre tenere sotto stretto controllo i movimenti del conto corrente effettuando frequentemente una verifica del saldo, al fine di individuare prontamente eventuali addebiti fraudolenti.

COSA FARE SE SIETE STATI VITTIMA DI UNA TRUFFA ONLINE?

1. Avisare 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.
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 ed 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 malto: sono sempre gli stessi truffatori.
8. Consultare eventualmente 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.

COME TUTELARE GLI ANZIANI



Purtroppo anche rispetto a questo tipo di truffe, gli anziani sono i soggetti da tutelare maggiormente anche perché sono spesso neofiti della rete e quindi maggiormente vulnerabili.

Per difenderli dagli hacker, la cosa migliore è assisterli sempre durante gli

acquisti on line e conoscere le loro credenziali dell'Home Banking in modo da poter controllare frequentemente i loro movimenti.

Controllate periodicamente anche la corrispondenza mail per verificare se sono vittime di “Phishing”.

Verificate anche i loro telefoni cellulari ed in particolare i messaggi SMS o Whatsapp che possono essere ricettacolo di comunicazioni ingannevoli.

Dotateli di una carta di credito ricaricabile, in modo che possano utilizzarla negli acquisti on line.

Informateli compiutamente rispetto alle frodi che appaiono sui banner dei siti internet e sono camuffate da vincite allettanti, notizie incredibili o avvisi di virus che hanno infettato il PC: queste sono le frodi nelle quali gli anziani cadono maggiormente e quindi occorre fargli comprendere che annunci troppo allettanti o avvisi troppo spaventosi, spesso nascondono delle gravi insidie nelle quali è facile incappare.

Cercate di ricordargli periodicamente quali siano i pericoli del web e le modalità con le quali i truffatori mettono in atto i raggiri tramite telefono o con le mail.

Maggiore è l'informazione e minori sono i rischi di cadere vittima di una truffa.



NUMERI UTILI



STAZIONE DI
RESCALDINA

0331 579914



POLIZIA LOCALE
RESCALDINA

0331 576676



NUMERO UNICO
DI
EMERGENZA

112



POLIZIA POSTALE
MILANO

02 43333011