CHIESA DI PADOVA

VADEMECUM

ATTENTI ALLE TRUFFE

2024

VADEMECUM
ATTENTI ALLE TRUFFE
2024

PRESENTAZIONE

Le truffe ormai sono all'ordine del giorno. Sulla stampa si leggono con sempre maggiore frequenza casi di persone – non più solo anziani o persone vulnerabili – che vengono truffate o raggirate, da individui senza scrupoli. Purtroppo l'abilità dei criminali si affina sempre più, tanto da riuscire a raggirare davvero chiunque.
Negli anni scorsi la Diocesi di Padova aveva già focalizzato l'attenzione sulle **"Truffe all'ombra del campanile"**[1] ossia quella particolare tipologia di raggiri che potevano coinvolgere in particolare i preti o persone dedicate a quelle che in gergo tecnico si chiamano *helping profession* (professioni di aiuto), che quindi sono più predisposte a vedere le buone intenzioni, sollecitati appunto sul tasto della carità.

In quell'occasione (aprile 2021) venne anche pubblicato un **Vademecum** dal titolo ***"Soldi & carità in parrocchia"***[2] che conteneva sette indicazioni/attenzioni che il vescovo Claudio sollecitava per gestire in modo accurato anche "i soldi per la carità" ed evitare di trovarsi in situazioni piacevoli e pericolose.

Attualmente si stanno moltiplicando le truffe che utilizzano la tecnologia e gli strumenti che quotidianamente utilizziamo per comunicare – telefono, email, messaggistica – al fine di accedere impropriamente a informazioni personali e depositi bancari.

I TERMINI

TRUFFA: l'attività fraudolenta riguarda la persona. Il truffatore inganna la vittima al fine di ottenere un vantaggio ingiusto. È un reato disciplinato dall'art. 640 del Codice penale. Il reato prevedere: artifizio, raggiro, induzione in errore, danno per la vittima, ingiusto profitto per il criminale.

FRODE INFORMATICA: l'attività riguarda il sistema informatico del soggetto passivo del reato. Il criminale altera il funzionamento di un dispositivo per trarne vantaggio indebito.
Il reato è disciplinato dall'art. 640 ter del codice penale che prevede due condotte fraudolente: l'alterazione del regolare funzionamento di un sistema informatico o telematico; l'intervento non autorizzato su dati, informazioni o programmi a loro volta contenuti in un sistema informatico o telematico.

---

[1] https://youtu.be/HqlOPACron4?si=TAQppkAlv8ZognAP

[2] https://www.diocesipadova.it/soldi-carita-le-indicazioni-del-vescovo-claudio/

STRUMENTI UTILI

Alta è l'attenzione all'informazione, vigilanza e contrasto rispetto a svariati tipi di truffe e cyber truffe. Ci sono siti governativi e di istituti finanziari che forniscono strumenti utili per conoscere e riconoscere le diverse tipologie di truffe, agire per contrastarle, evitarle e denunciarle. Di seguito proponiamo una serie di link dove è possibile trovare materiali utili, filmati informativi, infografiche e grafiche che possono essere stampate e diffuse.

Sistema di informazione per la sicurezza della Repubblica

https://www.sicurezzanazionale.gov.it/cosa-facciamo/consapevolezza-digitale

Il Sistema di informazione per la sicurezza della Repubblica è l'insieme degli organi e delle autorità che, nel nostro Paese, hanno il compito di assicurare le attività informative allo scopo di salvaguardare la Repubblica dai pericoli e dalle minacce provenienti sia dall'interno che dall'esterno.

Polizia postale

https://www.commissariatodips.it/index.html

Sito gestito da personale in servizio alla polizia postale: dove qualsiasi cittadino può inviare segnalazioni riguardanti quei fenomeni che possono essere ricondotti alle "truffe romantiche". La Polizia postale pubblica periodicamente "alert" su quei fenomeni di particolare pericolosità, fornendo all'utente utili consigli.

Guardia di Finanza

https://www.gdf.gov.it/

È il sito ufficiale della Guardia di Finanza dove si possono trovare informazioni e notizie aggiornate

Consob – Commissione nazionale per le società e la borsa

https://www.consob.it/web/investor-education/le-truffe-finanziarie

È il sito dell'Autorità di vigilanza dei mercati finanziari dove si possono trovare informazioni e suggerimenti utili per evitare di cadere in truffe.

CERTFin – CERT Finanziario Italiano

https://inavigati.certfin.it/

CERT Finanziario Italiano è un'iniziativa cooperativa pubblico-privata finalizzata a innalzare la capacità di gestione del rischio informatico degli operatori finanziari e la cyber resilience del sistema finanziario italiano attraverso il supporto operativo e strategico alle attività di prevenzione, preparazione e risposta agli attacchi informatici e agli incidenti di sicurezza.

Guide alla sicurezza e agli strumenti messi a disposizione dagli istituti bancari di riferimento per le parrocchie della Diocesi di Padova

Intesa SanPaolo

https://www.intesasanpaolo.com/it/common/landing/anti-phishing.html

BPM

https://www.bancobpm.it/media/2023/10/GuidaSicurezza_BBPM_set-23.pdf

Gruppo BCC ICCREA

https://stopfrodi.gruppobcciccrea.it/

TIPOLOGIE

Di seguito elenchiamo una serie di truffe, raggruppandole per ambiti.

TRUFFE INFORMATICHE

Sono le truffe di ultima generazioni, le più frequenti e subdole che riescono a ingannare davvero chiunque e su cui è importante vigilare, in quanto utilizzano spesso la tecnologia (email, sms…) o telefonate di sedicenti operatori bancari.

Ecco le più frequenti:

PHISHING

Viene utilizzato un messaggio **email (posta elettronica)** con cui si richiedono dati personali *(*nome utente, password, data di nascita, ecc.) che vengono poi utilizzati per violare account o fare operazioni bancarie non autorizzate.
Il messaggio ha tutte le caratteristiche di una richiesta legittima da parte di una fonte apparentemente attendibile e credibile (es. istituto finanziario…)
Le email appaiono identiche alle consuete corrispondenza con la banca, replicano fedelmente i loghi, il layout e lo stile, e solitamente trasmettono un senso di urgenza che induce il ricevente ad agire tempestivamente.
Il **rischio** è di considerare queste comunicazioni legittime proprio per l'apparente somiglianza visiva delle comunicazioni.

VISHING

è il *phishing* tramite **telefonata o messaggio vocale**. I truffatori chiamano spacciandosi per addetti del call center di un istituto finanziario o commerciale, o funzionari di banca e millantano un tentativo di truffa a danno della carta di credito o del conto corrente della potenziale vittima e, con questa scusa, cercano di ottenere informazioni riservati, come le OTP (one time password) password temporanee usa e getta che si utilizzano una volta sola.

SMISHING

è il *phishing* tramite **messaggio di testo** sullo smartphone della vittima. Le formulazioni sono varie:

- la promessa di uno sconto o di una promozione
- la scusa di aggiornare o riattivare il proprio account
- la richiesta di autorizzazione o di verifica di un pagamento

In tutti i casi viene chiesto di contattare un numero di telefono, di rispondere al messaggio con un sì o un no, o di collegarsi a un sito, cliccando su un link fornito, che di solito è un clone, del tutto simile a quello reale dell'istituto bancario.
L'obiettivo è impossessarsi di dati personali che possano aiutare i truffatori a rubare i soldi dai propri depositi.
Spesso *phishing e vishing* si integrano e succede che dopo aver adescato la vittima con il messaggio di testo o il link, si viene contattati da un sedicente addetto della banca o del dipartimento frodi dell'istituto bancario, che cercherà di ottenere le informazioni di accesso e i codici di autorizzazione per procedere con la truffa.

PHARMING

Si parla di *pharming* quando il traffico legittimo di un sito web viene manipolato per reindirizzare gli utenti su siti fasulli, che hanno lo stesso aspetto dei siti che si vogliono visitare, al fine di installare software dannosi sui computer delle vittime o prelevare dati personali degli utenti (password, dati bancari…)

SIM SWAP (Duplicazione Sim)

Il truffatore richiede agli operatori telefonici la duplicazione del numero di cellulare della vittima, così da ricevere codici OTP (one time password) contenuti negli sms di sicurezza inviati dalla banca.
Se il proprio numero smette di funzionare a seguito di un contatto sospetto, probabilmente il truffatore ha richiesto un duplicato della SIM.
Questa truffa spesso viene utilizzata insieme ad altre.

INVOICE FRAUD – Truffa della fattura

Solitamente coinvolge le aziende: il truffatore contatta l'azienda telefonicamente o via email manipolando le coordinate bancarie per il pagamento delle fatture, comunicando nuovi dettagli di pagamento per le fatture in corso.
La richiesta di pagamento è spesso urgente, accompagnata da informazioni fraudolente destinate a indurre l'azienda a trasferire denaro nelle mani del truffatore.

MONEY MULING

è una pratica finalizzata al riciclaggio di denaro proveniente da attività illecite, in particolar modo frodi informatiche e campagne di *phishing*. L'approccio più comune inizia con un messaggio di posta elettronica vago, che offre un lavoro facile, ben pagato e fattibile da casa propria. Se la vittima accetta l'offerta viene richiesta la disponibilità di operare trasferimenti di denaro trattenendo una commissione: il denaro che verrà trasferito proviene da attività illegali, ricadendo nel reato di riciclaggio.

SPEARPHISHING

una truffa personalizzata basata sull'invio di comunicazioni elettroniche o email che prende di mira una persona, un'organizzazione, un'azienda specifica con falsi messaggi precisi, convincenti, che fanno leva sui punti deboli della vittima.

L'*hacker* può per esempio fingersi un collega o un conoscente, utilizzare informazioni carpite in fase di studio della vittima e attuare meccanismi di pressione psicologica.

TAB - NAPPING

È una forma di *phishing* emergente, più sofisticata. Si focalizza su utenti che aprono contemporaneamente molte schede, o tab, sul proprio browser. Poiché l'attenzione verso tutte le schede aperte è inferiore rispetto a quella dedicata alla pagina in lettura, il criminale – facendo leva sulla disattenzione – crea una scheda con una falsa pagina web, configurata per ottenere i dati personali.

QRISGHING

È una frode basata sull'utilizzo dei codici QR code. I frodatori possono modificare fisicamente i codici presenti sui manifesti e reindirizzare a siti che carpiscono informazioni.

ATTENZIONI DA AVERE

- **Diffidare** di qualunque richiesta dati relativa a carte di credito, chiavi di accesso all'home banking, pin, password, dati personali, riferimenti delle bollette delle utenze, che giungano via sms, email, telefonate.
- **Non condividere i propri dati personali se non si è certi di chi li chiede.**
- **Non cliccare mai** su link di qualsiasi tipo (sondaggi, aggiornamento dati, ecc.) che giungono via email da indirizzi bancari, tanto più se si tratta di istituti su cui non hai contratti aperti o su immagini o allegati ricevuti via sms senza prima aver verificato con attenzione l'autenticità del mittente.
- **Diffidare** di messaggi on line di cui s'ignora la provenienza (semmai verificare attentamente l'indirizzo di provenienza, quello reale non quello che si vede in apparenza).
- **Controllare** regolarmente l'estratto conto dei contratti bancari.
- Controllare sempre nella barra del browser che ci sia la scritta **HTTPS**, la "s" finale e il simbolo del lucchetto o della chiave indicano che la connessione è protetta da un certificato di sicurezza utile per identificare il mittente delle informazioni sul sito.
- **Diffidare** di chiamate sospette.
- In caso di dubbi verificare l'onestà delle richieste **contattando direttamente** con il **proprio gestore bancario, tramite i numeri** che ci sono sui siti ufficiali, non con quelli che vengono inviati
- **Fare attenzione** se il telefono associato al servizio on line smette di funzionare a seguito di un contatto sospetto.
- **Verificare** con una ricerca on line i numeri di sms o telefonate sospette: spesso se è una truffa si trovano altre segnalazioni.
- **Verificare i numeri di arrivo degli sms** se corrispondono effettivamente a quelli del proprio gestore bancario.
- **Non essere mai frettolosi**, prendersi sempre il tempo per fare i controlli appropriati, soprattutto quando si viene contattati e viene stimolata l'urgenza ad agire e se le telefonate giungono in momenti in cui solitamente gli uffici sono chiusi (sera o festivi).
- **A fronte di telefonate sospette prendere nota del numero** del chiamante e dire che si richiama. Succesivamente verificare l'identità del chiamante, **cercare il numero di telefono dell'azienda/organizzazione** (sul loro sito web o eseguendo una ricerca online) e contattarli direttamente.
- I truffatori possono trovare online informazioni su persone e attività (ad es. attraverso i social media). Non fidarsi di chi chiama perché possiede questi dati.
- **Non trasferire denaro** su un altro conto a richiesta. La banca non chiederà chiederà mai di farlo.
- Controllare le **incoerenze o la presenza di errori di ortografia o grammatica** e ciò che non ha senso in indirizzi email, numeri di telefono (spesso viene cambiata una cifra o una lettera negli indirizzi o semplicemente viene invertito l'ordine delle lettere).

COSA FARE SE SE SI SOSPETTA DI ESSERE STATI VITTIMA DI UNA TRUFFA

- Se si ritiene di aver ricevuto una telefonata-truffa, segnalarla comunque alla propria banca.
- Se si ritiene di aver risposto a un messaggio di smishing fornendo i dati bancari, **contattare immediatamente la banca.**
- Denunciare alle forze dell'ordine o direttamente alla polizia postale

COME PROTEGGERE I PROPRI DISPOSITIVI

- Tenere aggiornato il software, inclusi browser, antivirus e sistema operativo sul proprio computer.
- Installare e mantenere aggiornati i software di protezione
- Installare le PATCH ("toppe di protezione) e scaricare solo gli aggiornamenti ufficiali
- installare i FIREWALL (programmi di filtraggio del flusso dei dati)
- scaricare e installare dal web solo PROGRAMMI SICURI di cui puoi verificare la provenienza
- verificare l'AUTENTICITÀ della connessione con la propria banca mediante il controllo accurato del nome del sito nella barra di navigazione (spesso i nomi sono simili, ma non uguali, presentano un cambio di lettera e comunque non sono identici)
- utilizzare quando possibile il 3D SECURE, un sistema di protezione antifrode per le carte di credito che garantisce la maggior tutela per gli acquisti online: abbina la carta di pagamento a un codice univoco e dinamico – diverso per ogni acquisto – che viene richiesto per autorizzare il pagamento online sui siti convenzionati 3DS.

TRUFFE "SOCIALI"

Le truffe e i raggiri più comuni riguardano la richiesta di soldi in nome della carità:

- c'è chi millanta spese mediche per cure a parenti lontani,
- chi sostiene la necessità di chiudere debiti improrogabili,
- chi ancora si spaccia per assistente sociale del comune e chiede l'urgenza di bonifici o contanti per aiutare situazione di singoli o famiglie urgentemente, solitamente l'approccio è telefonico e viene simulata anche una diretta conoscenza del problema da parte del sindaco del paese.

COSA FARE

- ricordare che i soldi della parrocchia sono della comunità e per le azioni caritative vanno utilizzati seguendo le disposizioni stabilite insieme al Consiglio pastorale parrocchiale
- far riferimento alle indicazioni "Soldi & carità in parrocchia"
- affrontare le diverse situazioni con gli organismi di comunione
- verificare sempre alla fonte (sindaco o assessore preposto) nel caso si tratti di sedicenti assistenti sociali o funzionari del comune, non fidandosi di voci al telefono che possono millantare altre identità

TRUFFA "D'ONORE"

Una delle forme più "antiche" di raggiro vede come vittime i sacerdoti anziani, avvicinati da donne o uomini che, coadiuvati da complici pronti a fotografare, creano situazioni apparentemente compromettenti, con cui ricattano poi il malcapitato, minacciando di diffondere le immagini. Solitamente la persona anziana, sebbene completamente innocente rispetto a qualsiasi situazione disonorevole, prostrata dalle possibili conseguenze della divulgazione di foto, cede al ricatto.

COSA FARE

- superare la paura del disonore e denunciare il fatto
- non cedere al ricatto
- parlarne con qualcuno, nel caso di sacerdoti, con i diretti superiori, per essere aiutati

Accanto a quelle elencate ci sono tutta una serie di truffe a danni di anziani e persone vulnerabili a partire da quella del falso incidente e delle telefonate di finti avvocati o finti rappresentanti di forze dell'ordine che chiedono soldi in cambio del rilascio di un proprio congiunto trattenuto a causa di altrettanto inventati incidenti.

Nota

Le informazioni contenute in questo Vademecum sono state raccolte dai siti segnalati tra gli "Strumenti utili". Per praticità si è dato un "nome" alle diverse tipologie di truffe.

A cura di
Servizio amministrativo
Ufficio stampa diocesano