

COLLABORAZIONE PASTORALE - CONCA DEL PIAVE
PARROCCHIE DI
CAORERA - QUERO - VAS - SCHIEVENIN

Contatti: don Mirko 0439.1900067 - don Romeo 366.3804266

Foglioetto N° 18 dal 19 Agosto al 1 Settembre 2024

Vademecum alla Parola – XXI Domenica del T.O.

La parola d'alleanza, che dà la vita. La **prima lettura** di questa domenica si riferisce all'alleanza stipulata in Sichem (Gs 24,1-2) e riporta il dialogo tra Giosuè e il popolo: Giosuè comunica la propria decisione di aderire al Signore e il popolo reagisce con una professione di fede entusiasta. Il Salmo 33 risponde alla lettura con un ritornello in cui si mostra che la scelta di stringere un'alleanza con Dio si basa sulla bontà divina. La **seconda lettura** presenta un famoso "codice domestico" che si fonda sull'amore attivo e creativo di Gesù Cristo che dona se stesso fino a consumarsi per la chiesa sua sposa. Il **vangelo** comincia con una nota negativa: molti discepoli si scandalizzano di fronte al discorso di Gesù. Il Maestro allora rivela che essi non hanno compreso il mistero pasquale: il Figlio dell'uomo sarà umiliato e verrà glorificato. Dopo di ciò, allude in anticipo al dono dello Spirito, capace di dare vita alla carne umana segnata dalla morte.

Vademecum alla Parola – XXII Domenica del T.O.

Carne e sangue, banchetto della Sapienza. Il passo dei Proverbi (**prima lettura**) presenta l'immagine di una donna, figura della sapienza, che prepara un ricco banchetto, invitando tutti alla sua tavola e rivolgendosi soprattutto agli inesperti. In questo modo, offre loro la possibilità di cambiare strada e di gustare il cibo succulento della grazia. Con la recita del Salmo 33 l'assemblea celebrante riconosce che l'eucaristia è proprio quella mensa in cui si può mangiare questo pane divino. La **seconda lettura** dalla Lettera agli Efesini, ricorda che il saggio sa approfittare del tempo e attraversa i «giorni cattivi», stringendosi a Gesù Cristo; egli è consapevole che solo nella preghiera sarà in grado di affrontare le prove. Nell'ultima parte del suo discorso eucaristico (**vangelo**), Gesù rivela che l'alimento essenziale per ogni creatura è costituito dalla parola di Gesù, e soprattutto dalla sua stessa persona, donata specialmente nell'eucaristia.

CALENDARIO LITURGICO

21 Agosto Mercoledì – San Pio X, Papa		
18:00	VAS	Santa Messa in chiesa grande – DF Comunità
22 Agosto Giovedì – Beata Vergine Maria Regina		
18:00	QUERO	Andreazza Luca, Ester e Santina – Benato Adriana – Specia Maria, Mazzocco Guerrino e DF
23 Agosto Venerdì		
09:30	QUERO	Santa Messa in Casa di Riposo
24 Agosto Sabato - XXI DOMENICA DEL T.O.		
16:00	CAORERA	Santa Messa per la Comunità
18:00	QUERO	Specia Antonio e Adele – Renzo, Antonio, Giovanna, Pierina, Luciana
25 Agosto XXI DOMENICA DEL T.O.		
09:30	QUERO	Zardin Fiorenza, Giacomo e Angela – Mondin Gildo e Elvira – Secco Gianna
11:00	SCHIEVENIN	Roman Giuseppe, Maria, Ornella, Gioachino, Domenico - Patrick
11:00	VAS	Cimolato Silvia e Giovanni – Mazzalovo Giulia
28 Agosto Mercoledì – Sant'Agostino vescovo e dottore		
18:00	VAS	Santa Messa in chiesa grande – DF Comunità
29 Agosto Giovedì – Martirio di San Giovanni Battista		
18:00	QUERO	Santa Messa in chiesa grande
30 Agosto Venerdì		
09:30	QUERO	Santa Messa in Casa di Riposo
31 Agosto Sabato – XXII DOMENICA DEL T.O.		
16:00	CAORERA	Santa Messa per la Comunità
18:00	QUERO	Santa Messa in chiesa grande

1 Settembre XXII DOMENICA DEL T.O.		
09:30	QUERO	Santa Messa per la Comunità
11:00	SCHIEVENIN	Spezia Attilio - don Vittorino Vedova Schievenin Clemente, Duilio, Olga, Rina, Giovanna
11:00	VAS	Santa Messa in chiesa grande - DF Comunità

Referenti per le intenzioni delle SS. Messe per i cari defunti

che vengono scritte sul bollettino parrocchiale in uscita ogni 15 giorni:

per Quero: **Fernanda Curto.** -

per Schievenin: **Rita Faccineto tel. 333.1142893**

per Vas: **Maria Grillo tel. 0439 788252** (ore pasti).

Scacco matto alle truffe online: consigli utili.

Prudenza, prudenza, prudenza. E stare in campana. È il consiglio di fondo da dare sempre di più a tutti, ma soprattutto agli **anziani**. Perché la truffa perpetrata con il telefono o via computer è sempre più diffusa e i truffatori inventano sempre nuovi modi per alleggerire il conto in banca altrui. Lo fa presente **Michele Fioretto, vicequestore aggiunto e vicedirigente del Cosc Veneto**, il Centro operativo di sicurezza cibernetica del Veneto. La lista delle modalità utilizzate è piuttosto lunga, ma ci sono alcune truffe che ricorrono più spesso. «Una delle più frequenti è la telefonata da parte di un interlocutore apparentemente affidabile, che si presenta come operatore di polizia o di un ufficio antifrodi della banca in cui si ha il conto corrente. Non è che il malfattore sappia in che banca abbiamo i soldi, ma citando le più diffuse sa che prima o poi farà centro; oppure è preparato per indurre l'interlocutore a dire qual è la sua banca di riferimento. Dice poi che qualcuno sta facendo operazioni sospette sul conto corrente della persona cui si telefona e che per salvare i soldi è necessario lo spostamento del denaro su un conto definito sicuro. *“Io l'ho solo avvisata”,* dirà il truffatore, *“fra poco riceverà la telefonata dell'ispettore di polizia XY o del funzionario di banca WZ, che la informerà nel dettaglio”*». E infatti in brevissimo tempo la telefonata arriva davvero e, sul cellulare del malcapitato, appare il numero della stazione di polizia più vicina o della filiale della banca presso cui si ha il conto. Questa trovata tecnologica e truffaldina – precisa il vicequestore – si chiama spoofing e consiste appunto nel chiamare da un numero diverso, facendo però in modo che appaia sul cellulare del destinatario un altro numero, ritenuto affidabile. La vittima risponde, chi è all'altro capo del telefono gli racconta di nuovo la storia che i suoi risparmi sono a rischio perché ci sono operazioni sospette e gli spiega come trasferire i soldi *“al sicuro”*. «Viene invitato a recarsi a uno sportello di un ufficio postale o a un bancomat per fare dei bonifici su conti dichiarati sicuri, che in realtà sono quelli dei truffatori». Ciò su cui si gioca è la fretta: fra la prima e la seconda telefonata passano pochi minuti, per cui la persona non fa in tempo a riflettere, a chiedere informazioni. La cosa migliore, invece, se chi ha chiamato si è dichiarato poliziotto, è cercare il numero di telefono della stazione da cui si è detto sia partita la chiamata e telefonare direttamente, sapendo che «nessuna forza di polizia chiede di spostare dei soldi da un conto all'altro, mai». Si può chiamare anche il 112 o 113 per chiedere informazioni e cosa ci sia di vero, oppure «sentire la propria filiale di banca. **E mai avere fretta**». Il secondo aspetto su cui i truffatori fanno leva è l'emozione: «Una truffa che va per la maggiore è quella del presunto incidente occorso al figlio o figlia di chi si vuole truffare. Anzi, in genere l'incidente è causato dal parente che, se non paga subito l'avvocato che dovrà difenderlo, rischia anni di galera. Normalmente il truffato è una persona fragile, specie un anziano. Lo shock emotivo, l'invito a risolvere un problema urgente entro breve termine induce la vittima a fidarsi della persona che si pre-

senta come carabiniere o poliziotto». Anche in questo caso **ci si difende prendendo tempo**. Si mette giù il telefono e si chiamano i congiunti. E ancora: attenzione alla **truffa del messaggio**. Quando si riceve un sms su cui è scritto qualcosa tipo "Papà, ho perso il telefono. Questo è il mio nuovo numero, puoi salvarlo e scrivermi su WhatsApp?", è meglio telefonare al solito numero di cellulare del figlio o alla moglie o ad altri congiunti per chiedere informazioni. Anche questa, comunque, è una truffa fatta come se fosse una pesca a strascico: chi la tenta non sa se l'interlocutore ha figli, ma inviando un numero enorme di sms qualcuno ci sarà. Un'altra **truffa via WhatsApp** avviene quando si installa l'applicazione stessa su un nuovo numero: il vecchio numero riceve un messaggio con un codice che, se inserito, carica il profilo WhatsApp sul nuovo numero, scollegando quello vecchio. «La truffa funziona così: arriva un messaggio che dice *"ciao, sono X, ti ho inviato per errore un codice; per cortesia puoi reinviarmelo?"* Chi scrive è il criminale, che sta cercando di impossessarsi su un altro numero del mio profilo WhatsApp. Se io cedo quel codice, il mio profilo si sposta su quello che WhatsApp crede sia il mio nuovo dispositivo e i truffatori si impossessano del mio profilo con tutti i contatti. A quel punto le persone di cui ho il contatto ricevono dal profilo che dovrebbe essere mio, quindi ritenuto affidabile, una richiesta di aiuto e di inviare dei soldi su un determinato conto. Diffidare quindi quando si riceve il messaggio "Ti ho inviato per errore un codice": vuol dire che quell'amico è stato "bucato". «Ricordiamoci sempre che se andiamo su siti noti o di persona in un ufficio, difficilmente cadremo in una truffa. Bisogna diffidare di offerte trovate in spazi digitali improvvisati o che hanno forme di contrattazione anomale. Quando vediamo che l'interlocutore propone di "spostarsi su WhatsApp", e ci manda lì i documenti, oppure arriva una mail da un indirizzo astruso, diffidiamo. Le società di assicurazione serie hanno un loro dominio noto. [...] Il furto di dati dai depositi informatici è un reato in costante ascesa. E tocca tutti noi. Un esempio? Una persona viene raggiunta da una telefonata in cui gli dicono: "Il mese scorso hai cambiato il gestore del servizio elettrico e hai scelto noi, la società XY; abbiamo concordato che pagherai tot. Dobbiamo però fare una piccola variazione a tuo favore: sarà una società a noi collegata a fatturarti il servizio, con lo sconto. Verifichiamo insieme i tuoi dati, bancari e di fornitura?". È l'approccio di una truffa, resa credibile dal fatto che il malintenzionato al telefono conosce alcune informazioni "sensibili" e private. Come è possibile che quelle informazioni siano uscite dal "forziere" legale e finite in mani criminali? «Sempre più di frequente le società sono vittima di attacchi hacker che comportano la sottrazione di imponenti quantità di dati. Si infiltrano nel sistema che conserva i dati dell'azienda, li scaricano e poi scatta la richiesta di riscatto oppure la loro messa in vendita nel darkweb». Come ci si difende? «Facendo una campagna per accrescere consapevolezza dell'importanza della sicurezza informatica. Il che significa adottare regole di sicurezza minime come privati e sistemi di sicurezza sempre più performanti come aziende». Qualche consiglio utile? **Informarsi** per non farsi sorprendere è la prima mossa per evitare raggiri online. Un aiuto importante è il filtro anti-spam del cellulare, un sistema che raccoglie tutte le informazioni fornite dagli utenti sulle chiamate che ricevono e che aiuta a capire se la chiamata in arrivo è spam oppure no. La seconda mossa è **proteggere bene i propri dispositivi**, a partire dalle password (robuste e diverse). Verificare i siti web dove le inseriamo. E infine **riservatezza**: copriamo con la mano mentre le digitiamo. Il sito della **Polizia postale – www.commissariato.dips.it** – è un valido aiuto, sempre aggiornato e con un'ampia casistica nella **sezione Alert** dei tipi di truffe che vengono messe in atto via internet.

Attenzione all'intelligenza artificiale. La truffa del futuro è alle porte ed è figlia dell'intelligenza artificiale. È sufficiente una traccia audio o un video pubblicati online per ricreare tono, timbro e inflessione della voce. Il malintenzionato scarica quel file audio, lo lavora con un software di intelligenza artificiale e ricrea un nuovo messaggio che invia (trovandone il contatto) a un parente o amico della persona di cui ha carpito la voce. Nel messaggio c'è una richiesta di aiuto, con la domanda di soldi.

da **Difesa del Popolo**