



Tiratura: 849.940

Data: 21/03/2026 | Pagina: 31 | Autore: di Giovanna Venditti

Categoria: Settore Credito



Truffe online, la Rurale punta a prevenire

L'iniziativa

L'evento ha coinvolto forze dell'ordine ed esperti di psicologia per spiegare come far fronte ai tentativi di imbroglio più comuni

di Giovanna Venditti

PERGINE «La prevenzione passa dalla conoscenza - dichiara il direttore della Cassa Rurale Alta Valsugana Mauro Pintarelli - Con questa serata vogliamo offrire alla nostra comunità un momento di approfondimento e aggiornamento sui rischi sempre più diffusi e sofisticati che si celano nel mondo digitale. Il nostro obiettivo è fornire strumenti concreti per riconoscere e prevenire le principali tipologie di truffe, rafforzando la sicurezza di tutti. Sul palco si alternano gli esperti di neuroscienze Roberto Patricolo, Veronica Patron, Cyber Security Operations Mario Baracchetti, Allitude Marco Grasso, Vice Brigadiere Gennaro Zambigli del Comando di Pergine». Il tema è caldo, tutti più o meno ne hanno avuto sentore o conoscenza,

indipendentemente dall'esserci cascati o meno. I dati del fenomeno sono implacabili: le truffe online in Italia sono in costante aumento. I truffatori contattano fingendosi centri di assistenza, forze dell'ordine o addirittura la propria banca o un familiare. Alcune tecniche di utilizzo fra le truffe più comuni: Phishing, tramite e-mail fraudolente i truffatori chiedono di scaricare allegati, cliccare su un link o chiamare un numero con un pretesto. Smishing, messaggio fraudolento che invita a cliccare su un link o chiamare con un pretesto quale un'offerta vantaggiosa o l'alert di un pagamento. Vishing, truffa telefonica in cui il truffatore, con un pretesto, chiede di fornire dati personali o finanziari o trasferirgli del denaro facendo leva sul senso di urgenza o paura.

Durante la serata sono stati dati alcuni suggerimenti: Diffidare dalle richieste urgenti: Le organizzazioni legittime non richiedono mai dati sensibili, password o l'accesso remoto al computer tramite chiamate non sollecitate. Verificare l'autenticità: se si riceve una chiamata sospetta da un presunto ente ufficiale o dalla propria banca, interrompere la comunicazione e contattare direttamente l'organizzazione utilizzando i canali ufficiali (numeri di telefono trovati sul sito ufficiale o sul retro della propria carta di credito). Non fornire informazioni personali o finanziarie:



La serata | relatori che hanno partecipato all'evento di formazione



Il teatro | il pubblico presenta alla serata sulle truffe online

non condividere mai codici personali, Pin o numeri di conto tramite telefono a meno che non si sia assolutamente certi dell'identità del destinatario. Utilizzare password sicure: Proteggere la propria segreteria telefonica e tutti gli account online con password complesse e uniche, non salvarle sul browser, attivare, eventualmente, l'autenticazione a due fattori, cioè una misura di sicurezza che richiede due metodi di verifica distinti per accedere a un account: solitamente una password e un codice temporaneo inviato via Sms o app.

Tra i giovani di età compresa tra i 18 e 24 anni, il 61% è consapevole del phishing, mentre questa percentuale sale al 76% nella fascia di età tra i 35 e 44 anni. Il reddito e il tipo di occupazione influenzano allo stesso modo il tasso di consapevolezza sul tema del phishing. Tra le persone con un reddito più alto, il 79% dice di essere al corrente dei rischi, a differenza del 58% di soggetti con un reddito più basso. Inoltre, l'80% dei freelance e lavoratori autonomi dice di conoscere il phishing, rispetto al 55% di chi si occupa delle faccende di casa.

© RIPRODUZIONE WEGALIA