DALLA TUA PARTE

S.O.S. TRUFFE ONLINE

I raggiri in Rete sono in aumento e i metodi utilizzati per frodare gli utenti sono sempre più subdoli, ma con l'aiuto dell'esperto possiamo imparare a difenderci

Sempre nuove e fantasiose varianti escogita la fervida inventiva dei cyber truffatori. Dal Wi-Fi agli squilli acchiappasoldi, scopriamo come difenderci grazie a Mauro Vergari, responsabile dell'ufficio studi, ricerca e innovazione per l'Associazione di consumatori Adiconsum (www.adiconsum.it).

◆ Via Pec Visto che l'elenco degli indirizzi Pec è prevalentemente pubblico, sempre più spesso oggi i malware dei truffatori arrivano proprio tramite la posta certificata che in tanti casi ha sostituito le raccomandate, confidando che la sola dicitura Pec ci induca ad abbassare la guardia. Oggi, però, chiunque può crearsi un indirizzo Pec fasullo e farsi passare per il nostro istituto di credito che sollecita: "Clicca qui per aggiornare i tuoi dati", chiedendoci per esempio di cambiare la password. Non caschiamoci! Nessuna banca ci invierà mai richieste di questo tipo, né la sigla Pec è un'assoluta garanzia di trasparenza.

◆ Wi-Fi rischiosi Per le reti di casa, o della casa di un amico, il problema non si pone. Spesso, però, capita, in giro per la città, in un ufficio o in biblioteca di agganciarci a reti pubbliche Wi-Fi gratuite del Comune, della Regione o di un'associazione riconosciuta, e lo stesso quando ci troviamo all'estero. Le reti pubbliche sono sempre meno sicure, quindi gli hacker possono più facilmente intercettare la nostra movimentazione personale e carpire dati sensibili o i riferimenti della nostra carta di credito. Usiamole solo per consultare siti Internet, ma mai per scaricare o inviare file.

◆ Telefonate senza... risposta Sempre più spesso capita di ricevere una telefonata, di solito da numeri con prefissi esteri, che dura appena uno squillo; oppure, alla risposta, non sentiamo nulla. Sono le cosiddette *ping calls* e la trappola scatta quando, incuriosite, richiamiamo per sapere chi era: non risponderà nessuno, ma il rischio concreto è che ci venga svuotato il denaro nella ricaricabile. Una variante del trucco è data dal *caller id spoofing*, telefonate che sembrano provenire da numeri italiani, ma partono dall'estero, o da numeri stranieri contraffatti: il tutto e sempre a caccia dei nostri soldi. Vediamo, di seguito, come evitare questi raggiri.

√ Non apriamo mai mail che arrivino da qualcuno che non conosciamo; se abbiamo dubbi sulle comunicazioni di una banca, prima di rispondere via web facciamo una telefonata di verifica.

√ Anche se sono più pratici, è bene non usare i programmi di gestione della posta elettronica di solito già in dotazione al pc, quali Mail e Outlook, perché non costituiscono un filtro efficiente. Meglio appoggiarci al sito Internet del server che usiamo: su Gmail, o Google, o Libero, siamo più tranquille perché la posta non è all'interno del nostro computer, ma sulla Rete: almeno sino a che non scarichiamo gli allegati.

√ Per qualsiasi operazione che comporti il trasferimento di dati o soldi, per scaricare file, controllare il nostro conto on line, usiamo solo la rete wi-fi di casa o una di cui siamo assolutamente certi. In Italia o fuori confine, il wi-fi pubblico andrebbe usato solo per leggere i giornali, navigare su Internet, consultare Google Maps o il sito di un museo.

√ Ricevendo una chiamata da un numero ignoto, in particolare dal prefisso di una città in cui non conosciamo nessuno, o con un prefisso estero mai visto (specie se non ha il + davanti), non rispondiamo né tantomeno richiamiamo. Grazie all'apposita funzione, poi, blocchiamo in tempo reale tutti i numeri sospetti o sgraditi.

Livia Pettinelli

QUELLE FALSE EMAIL

È la classica frode informatica che, anche se già nota, continua a mietere stuoli di vittime. Viene messa in atto da truffatori che, per scipparci i dati personali o le chiavi di accesso all'home banking, inviano false email, del tutto simili a quelle che si potrebbe ricevere da una banca o da una società emittente carte di credito, invitando il destinatario a collegarsi tramite un link a un sito Internet facsimile dell'originale, o a scaricare un allegato per poi inserirvi informazioni riservate. Se abbocchiamo, apriamo la porta a virus e malware e al rischio che qualcuno effettui transazioni bancarie a nostro nome o ci prosciughi la carta di credito.