

Caccia ai cybertruffatori

Ogni settore della pubblica amministrazione, delle imprese e dei servizi essenziali per il Paese è oggi fortemente informatizzato. Non solo. Anche gli acquisti e le attività ludiche dei cittadini si svolgono spesso su piattaforme informatiche. La scelta quindi è obbligata, dobbiamo affidarci alle nuove tecnologie che hanno azzerato le distanze tra le persone e i servizi loro offerti e hanno permesso di fare cose inimmaginabili solo fino a qualche anno fa. Sempre però con attenzione, consapevoli delle opportunità che l'informatica offre ai cybercriminali.

«La Rete – dice Massimo Bruno, direttore della divisione dedicata al contrasto delle frodi online del Servizio polizia postale e per la sicurezza cibernetica – è oggi terreno fertile per le organizzazioni criminali. Le più recenti evidenze investigative che provengono dal territorio ci riportano una fotografia da un lato allarmante, dall'altro interessante dal punto di vista della sfida da sostenere. Oggi è più semplice realizzare una frode nel Web. Un tempo il truffatore intercettava il malcapitato per la strada e, con l'inganno, lo induceva a farsi dare del denaro. Era un'azione che richiedeva impegno, presenza sul territorio, e che comportava molti rischi perché c'era la possibilità di essere fermati mentre si compiva. Ed era un'azione limitata, poiché nell'arco di una giornata si potevano approcciare poche vittime. Oggi il mondo è completamente cambiato. Attraverso la Rete le organizzazioni criminali riescono a "gettare l'esca" verso centinaia di migliaia di potenziali vittime».

Parole confermate dai dati. Nel primo semestre di quest'anno, infatti, la polizia postale ha investigato su circa 14mila casi di truffe online e frodi informatiche perpetrate in danno di utenti, registrando un aumento del 9% rispetto all'analogo periodo dello scorso anno. Le somme sottratte, nel periodo in esame, ammontano a circa 121 milioni di euro con un incremento del 52% rispetto allo stesso periodo dell'anno scorso.

Sfida alla quale la polizia postale risponde comunque "colpo su colpo" come dimostra, ad esempio, l'*Action day* contro le truffe e gli accessi informatici abusivi del 30 luglio che, coordinato dal Servizio polizia postale e per la sicurezza cibernetica, ha coinvolto oltre 160 operatori dei Centri operativi per la sicurezza cibernetica e ha permesso di indagare 54 soggetti residenti in Campania, Puglia, Veneto, Sicilia, Calabria, Piemonte, Lombardia, Lazio, Toscana, Marche e Friuli Venezia Giulia. Le tipologie di truffe contestate sono tutte caratterizzate dall'induzione in errore della persona con la finalità di carpirne i dati personali, bancari e le credenziali di accesso ai conti correnti. Spesso, anche se parliamo di frodi informatiche, l'aspetto preponderante non è quello tecnologico ma quello psicologico. È questo il caso delle tante tecniche utilizzate nel *Social engineering* (ingegneria sociale) che permettono di carpire informazioni (password, informazioni su conti correnti e finanziarie), estorcere denaro o persino di rubare l'identità. Non vengono sfruttate debol

...

Consultazione dell'intero articolo riservata agli abbonati

09/09/2024