Gruppo spagnolo tenta la truffa telematica all'Isisc di Siracusa, arrestata una 32enne

Una donna di 32 anni è stata arrestata in Spagna nell'ambito di una inchiesta coordinata dal procuratore capo, Francesco Paolo Giordano, e dal sostituto Davide Lucignani. L'accusa è di avere truffato, attraverso internet, l'Istituto Internazionale di Scienze Criminali di Siracusa (Isisc) oggi noto come "The Siracusa International Institute for Criminal Justice and Human Rights".

Il meccanismo della truffa è quello dello spoofing: un gruppo criminale studia il sito internet di un'impresa e ne acquisisce l'organigramma, quindi si inserisce nelle dinamiche aziendali e mediante una sostituzione di persona, attraverso l'invio di un messaggio di posta elettronica falsificato con l'identità del presidente dell'Istituto, induce il tesoriere a effettuare un determinato pagamento verso un conto corrente creato ad arte per appropriarsi del denaro.

Questa volta però, il gruppo criminale è stato sfortunato due volte: in primo luogo perché ha truffato un Istituto specializzato nella repressione dei reati, che ha saputo immediatamente sporgere denuncia fornendo agli investigatori i dati necessari alle indagini; e poi perché a Siracusa la Procura della Repubblica è dotata di un gruppo investigativo altamente qualificato nelle indagini telematiche, il N.I.T. – Nucleo Investigativo Telematico.

Dopo avere ricevuto la dettagliata denuncia da parte del direttore dell'Istituto che era stato truffato, ha effettuato tutti i tracciamenti informatici utili a risalire a ritroso alla reale ubicazione dei criminali e dopo avere avuto contezza che si trattava di persone operanti dalla Spagna ha

allertato la Guardia Civil attraverso il servizio di Europol, che ha immediatamente ottenuto i dovuti riscontri e ha quindi eseguito l'arresto di una cittadina spagnola che nel frattempo aveva incassato il denaro.

La tecnica usata dai criminali, conosciuta come "email spoofing", sta diffondendosi sempre più nelle sue molteplici varianti, sia nella versione della sostituzione di persona, sia in quella della falsificazione del codice Iban e di altre ancora.

La migliore tecnica di difesa che può essere adottata per difendersi da simili attacchi informatici è quella di dotarsi di efficaci procedure per la gestione della posta elettronica, nell'ambito di semplici ma costantemente aggiornate misure di sicurezza informatica, nonché di applicare alcuni semplici controlli di congruità e di coerenza prima di effettuare qualsiasi pagamento.