17 Ottobre 2108, 10:00 CEST

COMUNICATO STAMPA

Clicca qui e guarda come scompaiono i tuoi soldi – truffe informatiche del 21° secolo #CyberScams

Europol e la Federazione bancaria europea lanciano una campagna di sensibilizzazione sulle 7 truffe finanziarie online più comuni

BRUXELLES / L'AIA - **Il Centro europeo per la criminalità informatica Europol (EC3), la Federazione bancaria europea** e i loro partner del settore pubblico e privato danno il via oggi alla campagna di sensibilizzazione **#CyberScams** nell'ambito del Mese europeo sulla sicurezza informatica.

Nel corso della prossima settimana, le forze dell'ordine di tutti i **28 Stati membri dell'UE e di 5 Stati non membri dell'UE (1), 24 associazioni bancarie nazionali,** banche e molti altri soggetti che combattono la cybercriminalità, contribuiranno ad accrescere la pubblica consapevolezza in merito a questo fenomeno criminale. L'iniziativa paneuropea verrà accompagnata da una campagna di comunicazione attraverso i canali di social media delle forze dell'ordine nazionali, di associazioni bancarie e di istituzioni finanziarie.

Secondo le raccomandazioni IOCTA 2018, la difesa più efficace contro questo tipo di ingegneria sociale è l'educazione delle potenziali vittime – ossia chiunque decida di andare *online*. Aumentare la consapevolezza degli individui su come identificare le tecniche ingannevoli, contribuirà a fare sì che sia le persone sia le loro finanze siano protette.

Per questa campagna, il materiale di sensibilizzazione è stato sviluppato in **27 lingue ed è** disponibile per il download, con indicazioni sulle **7 truffe finanziarie** *online* più comuni e su come evitarle:

• **Frode dell'amministratore delegato**: i truffatori fingono di essere l'amministratore delegato o un dirigente dell'organizzazione e inducono a pagare una fattura falsa o a effettuare un trasferimento di denaro non autorizzato dal conto aziendale.

• **Frodi su fatture**: ci si finge un cliente o un fornitore e si indirizza il pagamento delle future fatture su un altro conto bancario.

• **Phishing / Smishing / Vishing:** telefonate, messaggi, e-mail inducono le persone a condividere le informazioni personali, finanziarie o di sicurezza.

• **Frodi con siti Web bancari contraffatti**: vengono utilizzate e-mail di phishing bancarie contenenti un link al sito Web contraffatto. Dopo aver cliccato sul collegamento, vengono utilizzati vari metodi per raccogliere le informazioni finanziarie e personali. Il sito ha l'aspetto di quello originale, con alcune piccole differenze.

• **Truffa "Romance" o sentimentale:** ci si finge interessati ad una relazione sentimentale. Di solito si sviluppa su siti di incontri online, ma i truffatori utilizzano spesso anche i social media o le e-mail per prendere contatto.

• **Furto di dati personali:** vengono raccolte le informazioni personali rese pubbliche attraverso i canali dei social media.

• **Scam di investimento e shopping online:** si fa credere alla vittima di trovarsi di fronte ad un investimento redditizio o ad una fantastica offerta *online*, naturalmente falsa.

Internet è diventato un canale molto interessante per i criminali informatici. I cybercriminali utilizzano sistemi sofisticati per estorcere denaro o preziose informazioni finanziarie. Gli esempi di truffe in cui si ricevono promesse di eredità da un lontano parente defunto o la "truffa del Principe Nigeriano" non sono più gli unici casi in circolazione. Le tattiche utilizzate dai criminali informatici si sviluppano più velocemente e stanno diventando sempre più difficili da individuare. Dal fingere di essere l'amministratore delegato dell'azienda in cui si lavora o simulare un interesse di tipo sentimentale, i truffatori online fanno tutto il possibile per ottenere ciò che vogliono, ossia denaro e/o le credenziali bancarie delle vittime.

Come evidenziato nella Internet Threatised Crime Threat Assessment (IOCTA) 2018, l'ingegneria sociale costituisce il motore di molti crimini informatici e il phishing è ancora la forma più frequente. I criminali usano l'ingegneria sociale per raggiungere una serie di obiettivi: ottenere i dati personali, drenare soldi dai conti correnti delle vittime, rubare l'identità, effettuare pagamenti illegittimi o convincere le persone ad effettuare qualsiasi altra attività contro il proprio interesse, come trasferire denaro o condividere dati personali. Un solo clic può essere sufficiente per compromettere i propri dati.

Ulteriori informazioni su come rimanere protetti sono disponibili sulla pagina Web dedicata #CyberScams.

Il Mese europeo della sicurezza informatica (ECMS) è una campagna di sensibilizzazione dell'UE, che promuove la sicurezza cibernetica tra cittadini e organizzazioni, evidenziando le semplici misure che possono essere adottate per proteggere i propri dati personali, finanziari e professionali.

Segui la campagna **#CyberScams su:**

Europol e EC3 Twitter, Facebook, Instagram, Youtube e LinkedIn EBF Twitter, Facebook e Linkedin

(1) **Colombia, Liechtein, Norvegia, Svizzera e Ucraina**