COMANDO CARABINIERI ANTIFALSIFICAZIONE MONETARIA

COME L'AI CAMBIA LA BANCA E COME DIFENDERCI ONLINE

L'Arma dei Carabinieri nella difesa digitale dei cittadini

Magg. Roberta Mazzoni, Comandante della Sezione Analisi
Cap. Mirko Guarriello, Comandante della Sezione Criptovalute

Salone dei Pagamenti
Milano, 29 ottobre 2025

Dal falso nummario al cybercrime

LE CONSEGUENZE DEL DENARO FALSO

L'introduzione di banconote e monete false nel sistema economico ha due principali effetti negativi:

Danno Economico Diretto

Erosione della Fiducia

Dal falso nummario al cybercrime

Dal falso nummario al cybercrime

Dal falso nummario al cybercrime

Dal falso nummario al cybercrime


Il 4 ottobre 2021 nasce la
Sezione Criptovalute
per contrastare l'uso illecito delle crypto
e tutelare il sistema finanziario

- personale altamente qualificato
- disponibilità di architetture informatiche

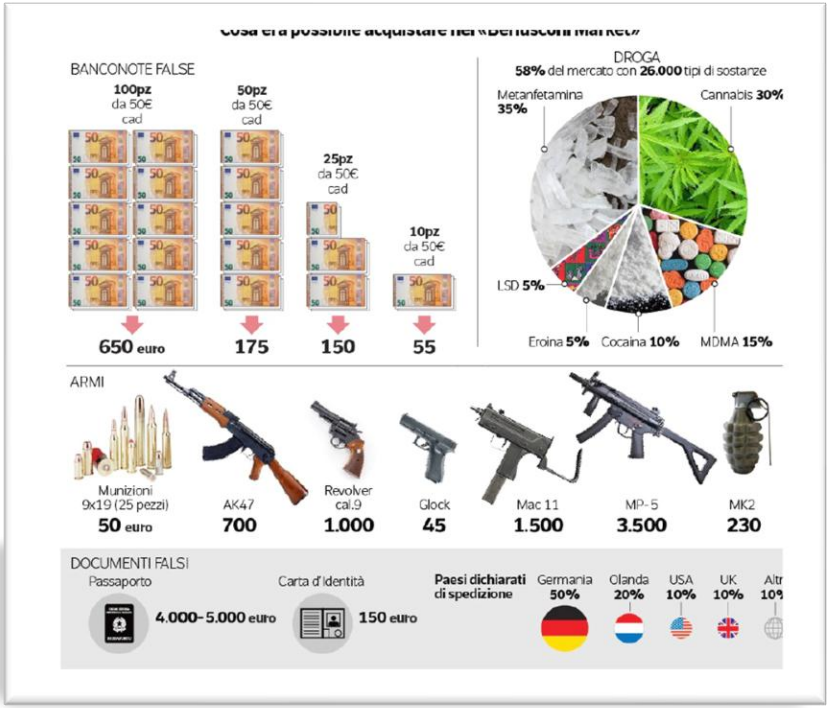

come i
CARABINIERI combattono
le MINACCE INFORMATICHE e le
TRUFFE DEL FUTURO


Comando Carabinieri Antifalsificazione Monetaria
Sezione Criptovalute
CONTENUTO ONLINE
SOTTOPOSTO A SEQUESTRO
CONTENT ACCESS INHIBITED
Questo contenuto online è stato sottoposto a sequestro a norma dell'art. 252 C.P.P. nell'ambito del Proc. Pen. n. 393/23 R.G.N.R. mod. 21 della Procura della Repubblica presso il Tribunale di Rovereto.

LA STRUTTURA DEL WEB:

Cosa si può trovare?

- Armi;
- Droghe;
- Carte di credito e conti correnti bancari;
- Denaro falso;
- Documenti;
- Farmaci;
- Pornografia;
- Gioielli falsi;
- Assassini;
- Virus informatici, botnet e servizi di hacking;
- Servizi finanziari, riciclaggio di denaro
- **Organi umani?**
- **Animali in via di estinzione?**
- **Documenti segreti?**



….ma cosa potrà mai succedere?

Navigare su internet è come girovagare in un quartiere a rischio

*Il mondo **virtuale** è*

reale

«.. In un momento di distrazione ho cliccato su un link che sembrava arrivare dalla mia banca. Poco dopo il mio conto corrente è stato svuotato»

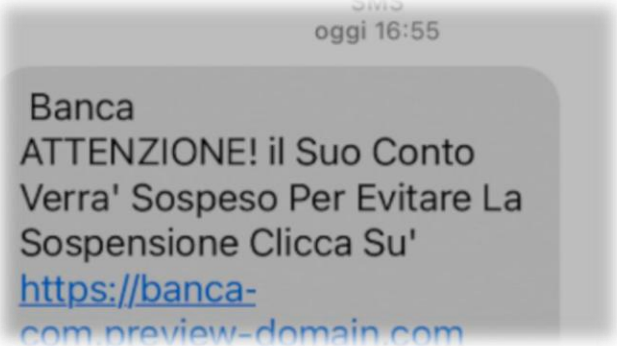
Falso Sms dalla banca sul telefonino e gli rubano 27mila euro dal conto: la truffa dello smishing

Scoperta banda delle truffe informatiche. Inviavano messaggi sui cellulari fingendo di essere istituti bancari per rubare soldi dai

Il **phishing** si riferisce a email fraudolente che ingannano i destinatari nella condivisione delle proprie informazioni personali, finanziarie o di sicurezza

Phishing, smishing e vishing

Lo **smishing** (dalla combinazione delle parole SMS e Phishing) è il tentativo da parte dei truffatori di acquisire informazioni personali, finanziarie o di sicurezza tramite SMS



Il Vishing (dalla combinazione delle parole Voice e Phishing) è una truffa telefonica in cui i truffatori cercano di indurre la vittima a divulgare informazioni personali, finanziarie o di sicurezza o a trasferire loro del denaro.

COME DIFENDERSI

- Fai attenzione alle chiamate telefoniche indesiderate.
- I truffatori possono trovare le tue informazioni di base online (ad es. attraverso i social media). Non presumere che chi chiama sia autentico solo perché possiede questi dati.
- Non cliccare su link, allegati o immagini che ricevi da SMS indesiderati, senza prima verificare il mittente;
- Non condividere il numero PIN della tua carta di credito o di debito oppure la password del tuo online banking.
- La tua banca non ti chiederà mai tali dettagli. Non trasferire denaro su un altro account a richiesta. La tua banca non ti chiederà mai di farlo;
- Presta particolare attenzione se un'email 'bancaria' ti richiede informazioni sensibili (ad esempio, la password del tuo conto bancario online).

«.. era in possesso delle mie credenziali di accesso ai social network ed è entrato sui miei account dove sono presenti tutti i miei dati personali»

«.Qualcuno ha rubato i miei dati personali e ha creato dei documenti personali falsi. Con quei documenti sono stati aperti conti correnti su cui sono state addebitate delle somme di denaro. Mi ritrovo indagato senza sapere perchè»

Un cybercriminale che ci ruba l'identità può, ad esempio: comprare qualsiasi cosa con la nostra carta di credito, **creare nuove carte di credito a nostro nome**, **attivare utenze telefoniche**, dell'**energia elettrica o** del **gas a nostro nome** e persino spacciarsi per noi in caso d'arresto. Insomma, l'impatto del **furto di identità online va ben oltre la realtà della Rete e potrebbe causarci problemi non di poco conto anche nella vita reale**.

COME DIFENDERSI

NON CONDIVIDERE I PROPRI DATI ONLINE

Fai molta attenzione alle informazioni personali

usare **password robuste**;

usarne **una diversa per ogni sito o account**;

evitare accuratamente di collegarsi a reti Wi-Fi pubbliche.

usare **l'autenticazione a due fattori,** ma non usare mai il numero di telefono come secondo fattore: clonare un numero telefonico è possibile e sempre più alla portata di mano dei truffatori.

«abbiamo cominciato a chattare. Siamo entrati in confidenza. Dopo qualche mese mi ha chiesto di mandarmi qualche foto. Ho accettato di spogliarmi in chat e ha cominciato a ricattarmi»

Adescato in un sito internet e ricattato

L'incubo è finito dopo la denuncia e gli arresti

e una agli arresti domiciliari, nei confronti di un 24enne e di un 56enne. Ai due i militari dell'Arma sono risaliti dopo la denuncia della vittima

spacciato per l'avvocato dell'inesi stente ragazza ritratta in foto nel sit di incontri: avrebbe richiesto ricari che settimanali periodiche di un

CARABINIERI

Pubblicano una foto di donna su un sito di incontri e adescano un giovane, poi lo minacciano per ottenere denaro: due arresti

Dopo aver raccolto foto e video intimi della vittima, i due avrebbero alzato il tiro minacciando di morte anche la moglie della vittima qualora non avesse ripreso i pagamenti e non avesse acquistato loro uno scooter

Truffe sentimentali e «sextortion»

I truffatori prendono di mira le vittime sui siti di incontri online, ma possono utilizzare anche i social media o le email per prendere contatto.

COME DIFENDERSI

- Fai molta **attenzione alle informazioni personali** che condividi sui social network e sui siti di appuntamento;
- **Fai attenzione ad errori di ortografia e grammatica,** ad incongruenze nelle loro storie e a scuse quali la fotocamera che non funziona;
- Non **condividere materiale compromettente** che possa essere usato per ricattarti;
- Non trasferire denaro per conto di qualcun altro: il riciclaggio di denaro è un reato penale

*«sono stato contattato tramite Facebook Messenger da tale …. che mi ha proposto un'**opportunità di investimento in criptovalute**, assicurandomi che investendo delle somme di denaro avrei ottenuto significativi margini di guadagno in breve tempo»*

«convinto dalle sue promesse e dalla documentazione che mi aveva mostrato, ***convincevo anche altri miei conoscenti ad investire in criptovalute****, dietro la promessa di una percentuale per ogni amico che avrei convinto ad investire»*

10 REGOLE PER LA SICUREZZA WEB

1. proteggi sempre il tuo PC con **antivirus e aggiornamenti**:
   installa software sicuro ed originale
2. non **fornire i tuoi dati personali** a nessuno
3. utilizza **password sicure e** distinte sui tuoi account: tienile **segrete**
4. è **facile mentire on-line**: nomi, foto, video potrebbero non essere reali
5. attenzione ai **falsi**, alle **truffe**, ai **siti a pagamento**, alle **facili offerte**
6. attenzione ai **messaggi istantanei** ed agli **allegati**
7. non fare su chat, forum, blog, social network ciò che non faresti nella vita reale: **mantieni una «netiquette» esemplare**
8. bada a **quello che pubblichi** su internet, forse rimarrà lì per sempre
9. tutela la tua **identità digitale** sulla rete
10. osserva sempre **la barra degli indirizzi** per sapere dove navighi

GRAZIE PER LA VOSTRA ATTENZIONE.

BUONO STUDIO! BUONA VITA!