Obiettivi

- Riconoscere i segnali di un'attività sospetta.
- Evitare comportamenti imprudenti.
- Ridurre il rischio di truffe on line.

Concetti fondamentali

Identità digitale:

Insieme dei dati e delle informazioni che identificano una persona fisica all'interno di un sistema informatico.

Furto di identità:

Appropriazione indebita dei dati della persona allo scopo di sostituirsi ad essa mediante l'acquisizione delle informazioni attraverso canali internet, di telefonia mobile o sottrazione fisica di documenti cartacei.

Tipologie di truffe ricorrenti online

- Truffa su acquisti di beni su portali e-commerce o siti internet
- Truffa al venditore su portale e-commerce
- Truffa sentimentale
- Sex exstorsion
- Finto messaggio whatsapp da persona cara
- Truffa del "trading online"

NUMERI UTILI

NUMERO UNICO DI EMERGENZA **112**

PREFETTURA DI PESCARA
Piazza Italia, 30
65121 Pescara (PE)
Telefono: 085 20571
Email: prefettura.pescara@interno.it

QUESTURA DI PESCARA
Via Pesaro, 7
65121 Pescara (PE)
Telefono: 113
Email: dipps158.00f0@pecps.poliziadistato.it

COMANDO PROVINCIALE DEI CARABINIERI DI PESCARA
Viale Gabriele D'Annunzio, 149
65127 Pescara (PE)
Telefono: 112
Email: tpe20738@pec.carabinieri.it

COMANDO PROVINCIALE GUARDIA DI FINANZA DI PESCARA
Via Cincinnato, 5
65127 Pescara (PE)
Telefono: 117
Email: pe0530000p@pec.gdf.it

C.O.S.C - POLIZIA POSTALE E DELLE COMINUCAZIONI
Via Ravenna, 8
65122 Pescara (PE)
Email: dipps511.0000@pecps.poliziadistato.it

https://www.commissariatodips.it/
(anche da app per informazioni, segnalazioni e denunce)

IN COLLABORAZIONE CON

PROCURA DELLA REPUBBLICA DI PESCARA

POSTE ITALIANE

Prefettura di Pescara
Ufficio Territoriale del Governo

VADEMECUM CONTRO LE TRUFFE *online*

Accorgimenti

1 UTILIZZA SOFTWARE E BROWSER COMPLETI ED AGGIORNATI

Assicurati di avere un antivirus e un sistema operativo correttamente installati e aggiornati.

2 CAMBIA SPESSO LA TUA PASSWORD

Periodicamente modifica la tua password, non rivelandola a nessuno, combinando caratteri alfa-numerici, caratteri speciali e lettere minuscole e maiuscole.

3 CONTROLLA IL TIPO DI CON - NESSIONE E IL NOME DEL SITO

Accertati della presenza del lucchetto chiuso e che il sito utilizzi il protocollo HTTPS (la "S" indica la presenza di una connessione sicura). Verifica con attenzione il nome del dominio (sito) perché il truffatore adopera nomi molto simili a quelli autorevoli e/o ufficiali cambiando solo una lettera o inserendo un numero (es. gdf.gov.it potrebbe diventare gbf.gov.it).



4 LEGGI BENE L'ANNUNCIO

Se l'annuncio è troppo breve o fornisce poche informazioni, se il prezzo è troppo basso o il venditore chiede di essere contattato al di fuori della piattaforma di annunci avendo fretta di concludere l'affare, questi sono segnali per cui insospettirsi.

5 DIFFIDA DA CHI RICHIEDE TROPPI DATI

Per effettuare acquisti online sono richiesti pochi dati fondamentali: se venissero richiesti dati sensibili ulteriori e non pertinenti è opportuno dubitare dell'attendibilità del sito. Non entrare mai nella pagina del conto corrente attraverso riferimenti contenuti nelle e-mail ricevute

6 METODI DI PAGAMENTO PayPal

Affida il pagamento ad un servizio tracciato, come bonifici o PayPal, per consentire alle forze dell'ordine di risalire all'identità del malvivente in caso di truffa. È sicuro anche adoperare una carta di credito ricaricabile o una prepagata perché,
in caso di abusi, le somme sono solitamente contenute. Attivare o farsi attivare dai propri familiari i canali informatici della domiciliazione bancaria.

7 NON CADERE NELLA RETE DEL PHISHING E/ O DELLO SMISHING

I truffatori, attraverso mail o sms contraffatti richiedono di cliccare su un link per raggiungere una pagina web trappola e, con la promessa di un vantaggio personale, riusciranno a rubare informazioni personali (password, numeri di carte di credito) per scopi illegali. Fai attenzione a telefonate da finti call center o da interlocutori che si spacciano per qualcuno di attendibile e conosciuto dalla vittima.

8 CONTROLLA CHE IL SITO ABBIA GLI STESSI RIFERIMENTI DI UN VERO NEGOZIO

Verifica l'affidabilità del sito attraverso recensioni di altri utenti. Utilizza le App ed i siti ufficiali di Posteitaliane ovvero della propria banca digitando l'indirizzo direttamente nella barra programma di navigazione. Non rispondere a sms e non comunicare mai telefonicamente gli estremi della tua carta o il codice dispositivo dell'Home Banking. Anche per i negozi a cui fai riferimento, utilizza sempre le app ed i siti ufficiali e verifica che sul sito siano presenti gli stessi riferimenti di una sede fisica (es. Partita IVA, numero di telefono, indirizzo); i dati fiscali sono facilmente verificabili sul sito dell'Agenzia delle Entrate.