



1



2

## PRINCIPALI ATTIVITÀ



**DIFFUSIONE**  
conoscenze e competenze di base



**AFFIANCAMENTO**  
e supporto in azienda



**MAPPATURA**  
con vari strumenti di assessment



**ORIENTAMENTO**  
verso strutture specializzate



**ANALISI**  
dei dati raccolti dagli assessment



**SOSTEGNO**  
con i voucher doppia transizione

3

## ASSESSMENT CHECKUP SICUREZZA IT

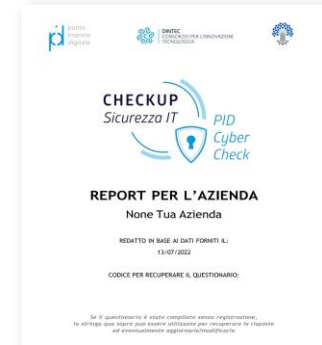
[https://bit.ly/pidcybercheck\\_bari](https://bit.ly/pidcybercheck_bari)

**CHECKUP**  
Sicurezza IT

*PID  
Cyber  
Check*

**CHECKUP**  
Sicurezza IT

*Cyber  
Exposure  
Index*



4



5



6

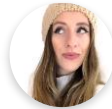
## IL TEAM DI BARI



**Alessandra Mottola**



Giurisprudenza



**Simona Lato**



Comunicazione



**Vito Macina**



Informatica

## CONTATTI



CAMERA DI COMMERCIO  
BARI

### Indirizzo

Corso Cavour 2  
Ufficio Punto Impresa Digitale  
Piano 1 – Stanza 78

### Contatti

[www.ba.camcom.it/pid](http://www.ba.camcom.it/pid)

[pid.bari@ba.camcom.it](mailto:pid.bari@ba.camcom.it)

0802174269

PIDBari

punto  
impresa  
digitale

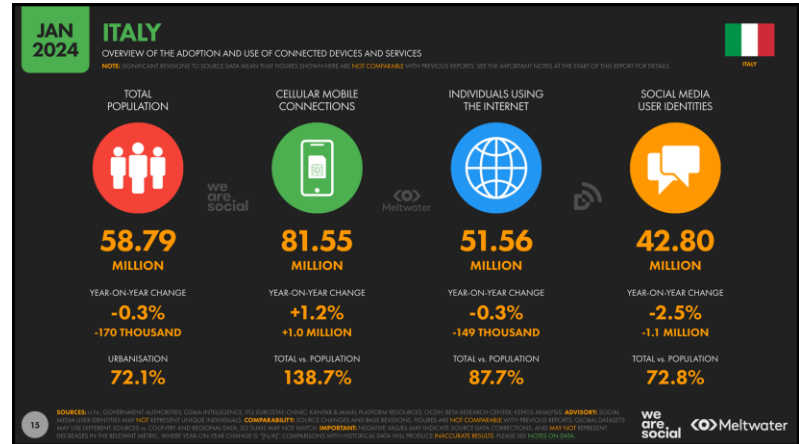

 CAMERA DI COMMERCIO  
BARI

**SERVIZI BANCARI ONLINE, APP,  
CARTE DI CREDITO E BANCOMAT:  
REGOLE DI CONDOTTA PRUDENTI  
NELL'USO PER PREVENIRE LE TRUFFE**

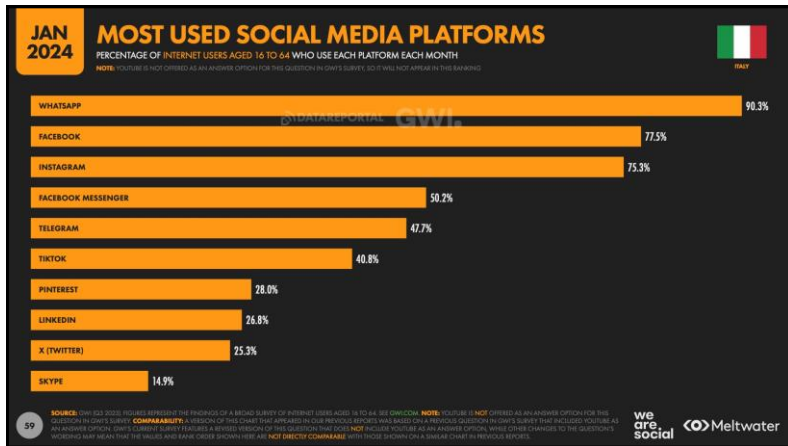

 punto  
impresa  
digitale



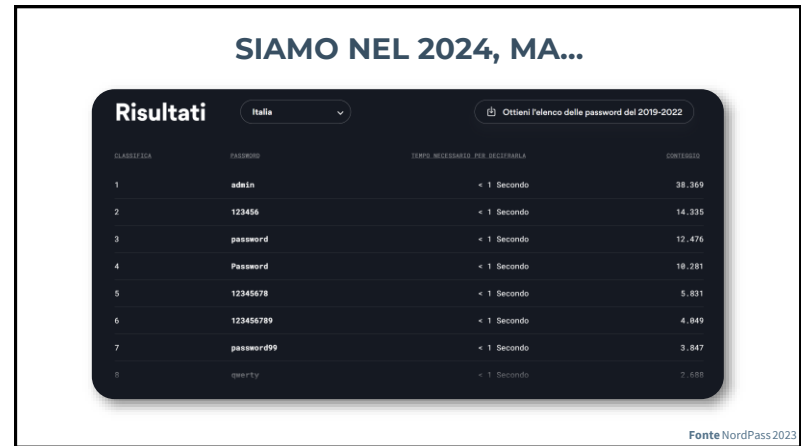
9



10



11



12

## ...NOI SIAMO LA NOSTRA MIGLIOR DIFESA



13

## REPORT POLIZIA POSTALE 2023

- Oltre 3.500 le persone deferite all'A.G. in particolare nel settore e-commerce
- Incremento degli illeciti legati al fenomeno del falso trading online  
3.360 casi trattati  
188 persone denunciate  
109.536.088 € di profitti illeciti
- Persistente diffusione di condotte predatorie  
65 grandi, medie e piccole imprese  
oltre 19 milioni di euro di profitti illeciti  
6 milioni sono stati recuperati



Fonte Resoconto attività 2023 della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica

14

## FENOMENO IN ASCESA

### INGEGNERIA SOCIALE



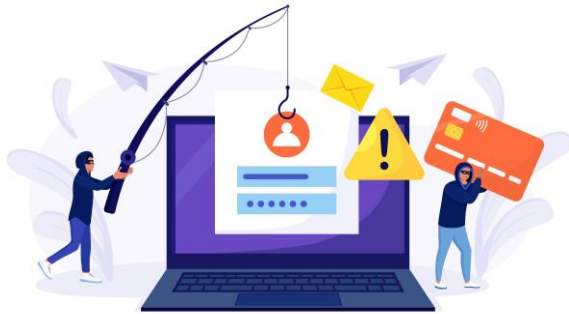
## DATI PIÙ RICERCATI

- Tutti i dati che permettono al criminale di prendere il posto della vittima (nome, cognome, numero di telefono, numero carta d'identità digitale, patente, ...)
- Credenziali d'accesso (nome utente e password, accessi dei social, carta d'identità elettronica, Spid)
- Codici bancari (informazioni per l'accesso a conti correnti o carte di credito)



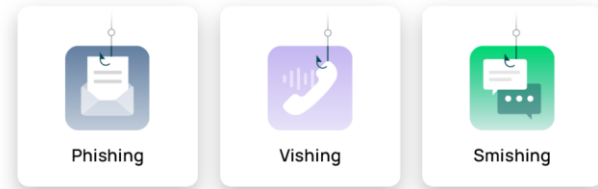


## ANDIAMO A PESCA?



17

## PESCA SEMPRE PIÙ «ABBONDANTE»



18

## PESCA SEMPRE PIÙ «ABBONDANTE»



Phishing

Email



Vishing

Voce



Smishing

Messaggi

## PHISHING

È una tecnica di frode online in cui gli aggressori inviano un'email che sembra provenire da una fonte legittima, al fine di indurre gli individui a rivelare informazioni personali, come password e numeri di carta di credito.

Queste email possono sembrare provenire da banche, fornitori di servizi o qualsiasi altra entità affidabile.



## VISHING

È una forma di phishing che si svolge tramite chiamate telefoniche. Gli aggressori possono fingere di essere rappresentanti di banche o altre organizzazioni e cercare di ottenere informazioni personali o finanziarie.

Questo termine deriva dalla combinazione di "Voice" e "Phishing".



## SMISHING

È un'altra forma di phishing che si svolge tramite messaggi SMS, WhatsApp e simili. Gli aggressori inviano messaggi di testo ingannevoli per indurre gli utenti a cliccare link dannosi o, sempre più frequentemente, a fornire informazioni personali.

Il termine "Smishing" deriva dalla combinazione di "SMS" e "Phishing".





23

## CASI REALI

Primo Tigota - info@fecheitalia.com  
A. Siletti - cliente  
C. Siletti - cliente

812207  
97306

**FEDEX SERVIZIO.** 04-07-2024

**Hai (1) pacchi in attesa di consegna.**

Numero di identificazione: [8815465478](#)

Pianifica ora la tua consegna:

Pianifica la consegna

Se non riceviamo una risposta entro 5 giorni lavorativi, il pacco verrà restituito.

📍 In programma per l'ufficio centrale FEDEX

Rintraccia il tuo ordine →

TIGOTA

TU SEI IL NOSTRO VINCITORE!

BRT

CONSEGNA DI PACCHI APPESI

Hai (1) pacco in attesa di consegna Usa il tuo codice per tracciarlo e riceverlo

Siamo qui per informarti che abbiamo bisogno della conferma dell'indirizzo per restituire il pacco.

⚠️ Si prega di compilare le informazioni mancanti ⚠️

24

## CASI REALI

**<#> Hai richiesto l'attivazione del Token. Inserisci il codice 911130 per proseguire o contattaci se non l'hai richiesta tu. UnsR8SLJPEC**

Ciao, il tuo Token e' ora attivo! Se avevi un Token attivo su un altro dispositivo, ora e' disattivato. Non hai richiesto l'attivazione? Contattaci subito!

14:23

Attenzione: abbiamo rilevato un'accesso anomalo al tuo mobile banking segua la procedura di verifica al seguente link <https://bit.ly/3dTuGjP>

Tocca per cancellare l'anteprima

Non siamo in grado di consegnare il **pacco** a causa dell'indirizzo non valido modificare l'indirizzo per la consegna tempestiva: <https://is.gd/djWylh>

Il tuo pacco è arrivato al magazzino ma non può essere consegnato perché mancano le informazioni sull'indirizzo. Conferma l'indirizzo nel link.

<http://business-poste.top/it>

(Rispondi Y, chiudi e riapri il messaggio di testo per attivare il collegamento oppure copia il collegamento e aprilo in Safari.)

\*I pacchi postali sono arrivati al magazzino ma non hanno potuto essere spediti a causa di un indirizzo incompleto. Si prega di confermare il proprio indirizzo tramite il link entro **le 12** ore.

<https://qrco.de/beorxA7kZa=hrT8o7etYA>

(dopo aver scritto di nuovo un SMS, la risposta ""Y"" può aprire un collegamento di attivazione tramite SMS, oppure riprodurre il collegamento in un Safari).

Il gruppo delle **poste** italiane le augura una buona giornata.

25

## AVVISI

**Attenzione alle frodi** ✕

Nessun operatore della Banca ti contatterà mai al telefono, via SMS o su WhatsApp per:

- chiederti codici o password temporanee (OTP) con il pretesto di mettere in sicurezza il conto o rivederla la tua

TORNA ALLA HOME

Non mostrare più

E-mail, SMS e telefonate sospette?

ATTENZIONE!

Potrebbe trattarsi di **phishing, smishing e vishing!**

BCC CARATE BRIANZA  
GRUPPO BCC CRODA

26

### CONSIGLI UTILI

1. Non agire mai d'impulso e prendersi tutto il tempo necessario per informarsi
2. Verificare la provenienza delle comunicazioni
3. Diffidare da proposte sospette o troppo vantaggiose (spesso fantasiose)
4. Fare molta attenzione alla gestione di dati e alle informazioni personali condivise
5. Mantenere software e credenziali aggiornati
6. Attivare sistemi di autenticazione a più fattori (2FA e MFA)

27

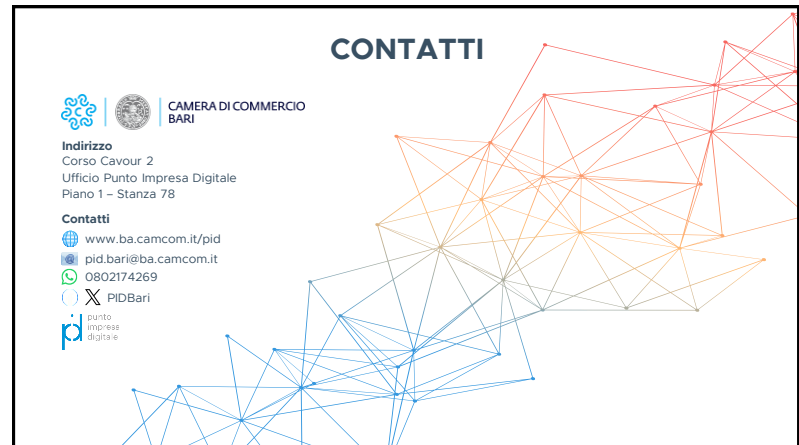
### FUTURO PASSWORDLESS



28



29



30