

Lezione 20 del 10/04/2025

Truffe

Corso android per smartphone





Truffe: tipologie su smartphone

Le 3 tipologie più comuni di attacco

1

Phishing



Phishing via e-mail

2

Smishing



Phishing via SMS

3

Vishing



Phishing via telefono

COSA LE CARATTERIZZA (Ingegneria Sociale)

- ✓ Richiesta di un'azione da compiere con urgenza
- ✓ Richiesta di informazioni sensibili
- ✓ Presenza di link o allegati da scaricare

- ✓ Offerta imperdibile o intervento di sblocco
- ✓ Urgenza per non perdere l'occasione o per intervenire
- ✓ Presenza di un link che indirizza a un sito malevolo

- ✓ Chiamata dalla banca o organizzazione conosciuta
- ✓ Senso di urgenza legato a un possibile rischio
- ✓ Richiesta di informazioni sensibili, pin, numeri carte



Phishing via email

- **Mezzo di attacco:** Email che sembrano provenire da banche, servizi di consegna o altre aziende legittime, con link fraudolenti.
- **Pericolosità:** Alta, può portare al furto di credenziali bancarie e dati personali.
- **Diffusione:** Molto elevata, milioni di tentativi quotidiani in tutto il mondo.
- **Difesa:** Non cliccare mai sui link ricevuti via email, contattare direttamente l'azienda attraverso i canali ufficiali, utilizzare app di filtraggio SMS anti-spam.

INPS Istituto Nazionale per lo Studio e la Cura delle Dipendenze

Gentile **XXXXXXXXXXXXXXXXXXXX**,

ti informiamo che ad oggi non risulta pervenuto il pagamento dei contributi **INPS** dell'importo di seguito indicato:

Data Emissione	Scadenza	Numero Fattura	Importo originario €	Importo residuo da pagare €
16/01/2020	25/02/23	46638540/2022	451.90	1,90

Ti invitiamo pertanto a provvedere al pagamento di quanto dovuto entro e non oltre 2 giorni dalla presente comunicazione, ricordando che **INPS può limitare servizio sulla sua BANCA** in caso di mancato pagamento del suddetto importo, come previsto all'articolo delle **Condizioni di servizio**.

Ti ricordiamo anche che puoi pagare comodamente in casa, evitando code e **senza alcun costo aggiuntivo** tramite:

- **Area Servizi Clienti**
- **Area pubblica**, senza necessità di registrarti

Qualora non esegue i pagamenti previsti per legge, potrebbe essere sanzionato, con una multa che va dal **2.600** euro al **13mila** euro.

Il Servizio Clienti è sempre a tua disposizione.

yvonneenovy@gmail.com

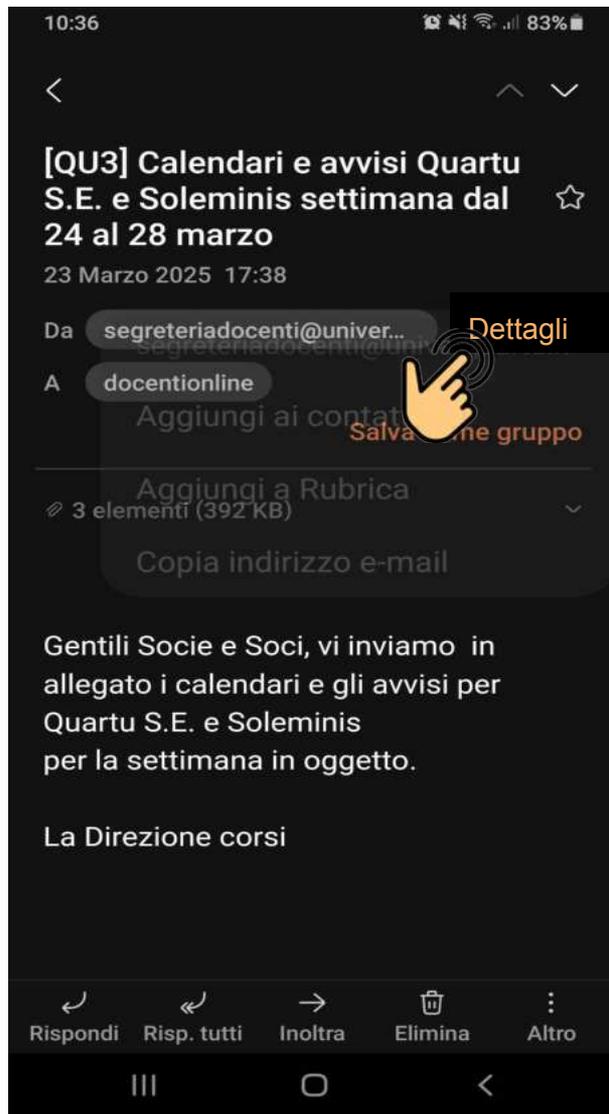
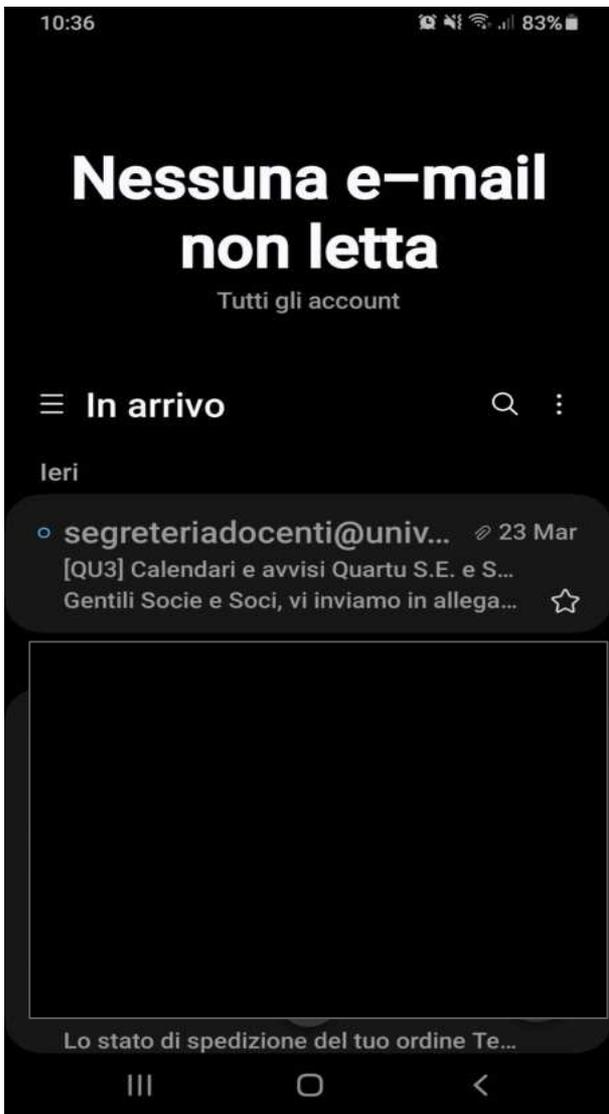
username domain TLD

Lista di domini di primo livello

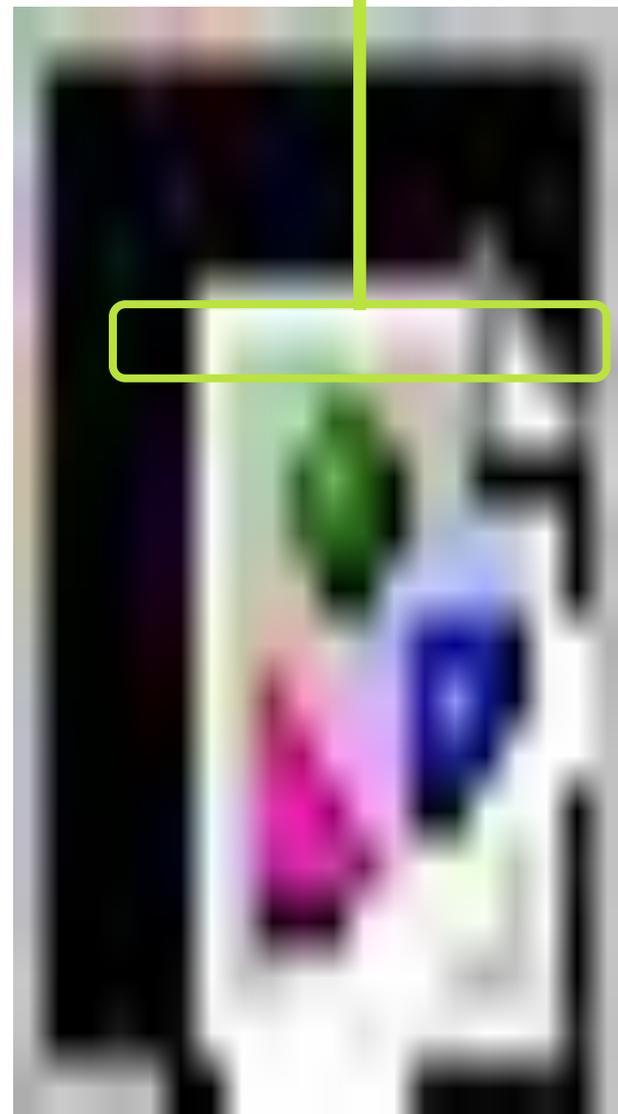




Phishing via email



Indirizzo corretto

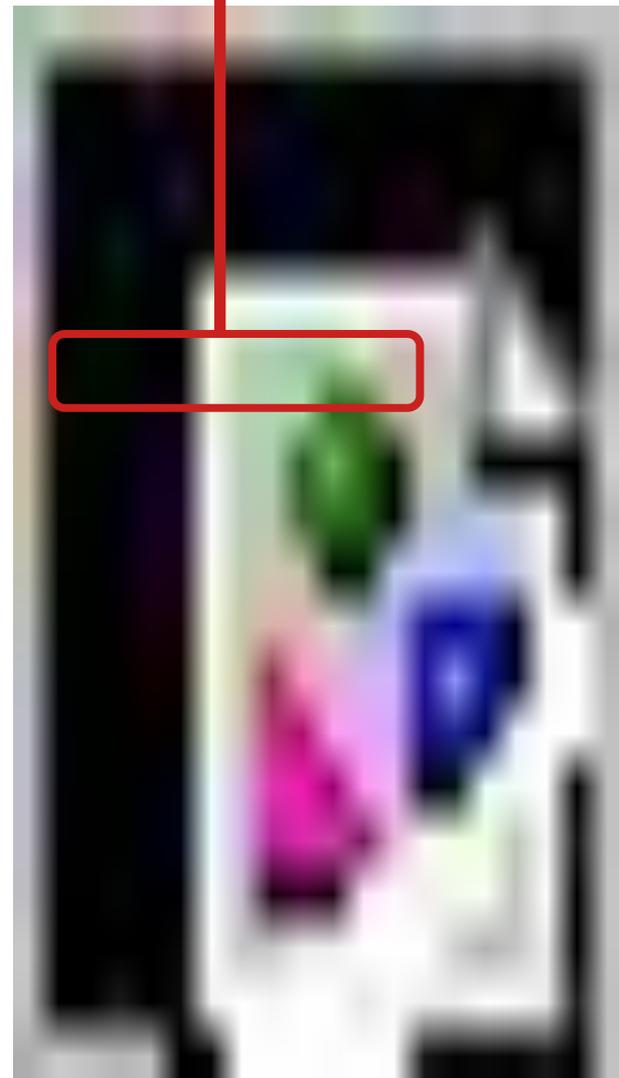




Phishing via email



Indirizzo fasullo





Truffe: indirizzi internet o URL

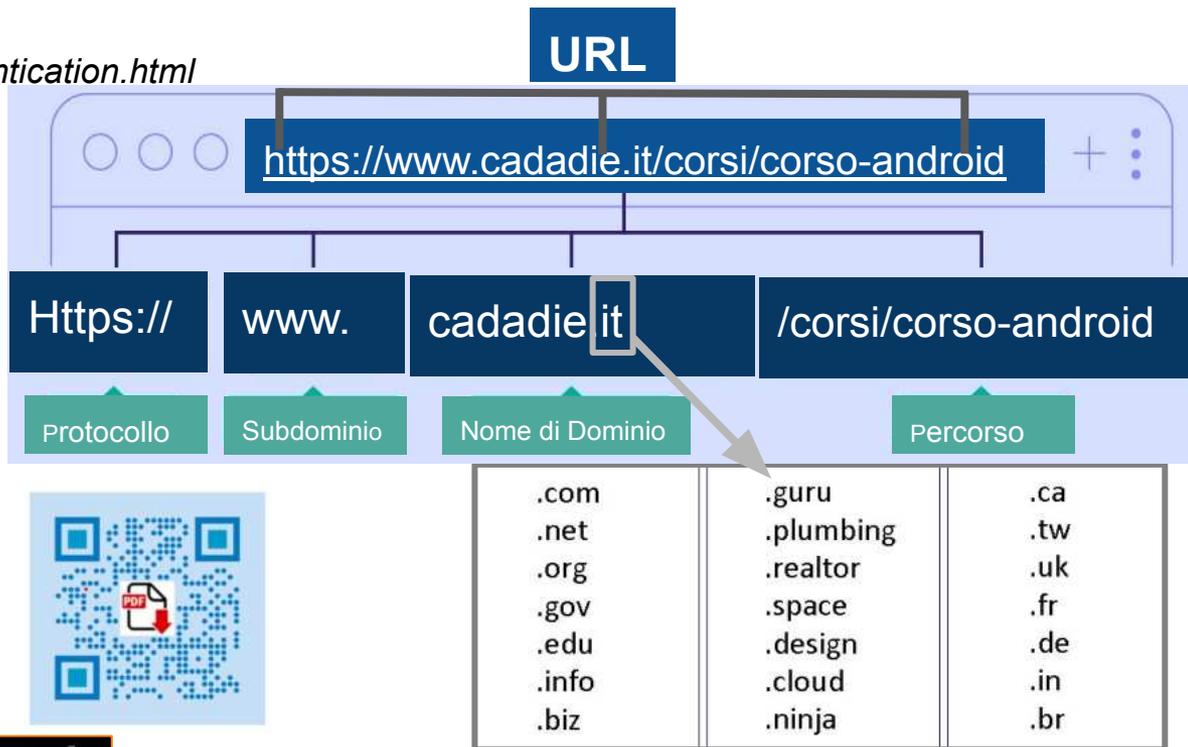
Indirizzo o url corretto

- <https://www.cadadie.it/corsi>
- <https://servizioclienti.poste.it>
- postepay.poste.it
- <https://securelogin.poste.it/jod-fcc/fcc-authentication.html>
- <http://142.250.217.68/search?q=cadadie>

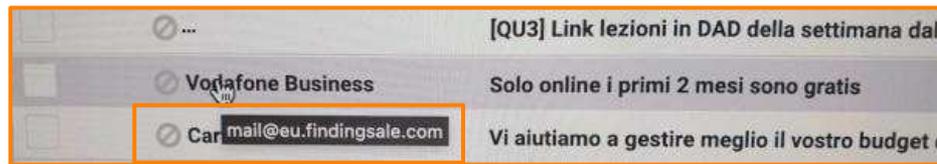
- <https://toolset.mrw.it/network/redirect-checker.html>
- <https://www.emailveritas.com/url-checker>
- <https://vms.drweb-av.it/online/>

Indirizzo o url truffaldino

- <http://poste.cadadie.it>
- <http://servizioclienti-poste.it>
- www.serviziocartedicredito-postepay.it
- posteditalia.info
- poste.com
- poste-pay.eu



<http://m.facebook.com> ————validate———step1.rickyaylk.com/sign_in.html





Phishing via SMS (smishing)

- **Mezzo di attacco:** SMS che sembrano provenire da banche, servizi di consegna o altre aziende legittime, con link fraudolenti.
- **Pericolosità:** Alta, può portare al furto di credenziali bancarie e dati personali.
- **Diffusione:** Molto elevata, milioni di tentativi quotidiani in tutto il mondo.
- **Difesa:** Non cliccare mai sui link ricevuti via sms, contattare direttamente l'azienda attraverso i canali ufficiali, utilizzare app di filtraggio SMS anti-spam.

SMS
oggi 10:20

Gentile Cliente, la sua carta PostePay è stata bloccata. Visiti <http://poste.it-securelogin-job-fcc.com/> e segua la procedura guidata.

Il tuo pacco è stato trattenuto presso il nostro centro di spedizione. Si prega di seguire le istruzioni qui: [http://\[redacted\]](http://[redacted])

Messaggio di testo • SMS
ieri 13:04

Abbiamo provato a contattarla diverse volte. E prego di chiamare al numero [89349067](tel:89349067). Per delle questioni che la riguardano

IntesaSP. >

SMS
lunedì 15:05

Il suo conto è in fase di blocco per prelievi sospetti se disconosci chiama il numero: [3514600014](tel:3514600014)

Venerdì 22 Gennaio 2021

Gentile Cliente, Poste Italiane per motivi di sicurezza la invita a convalidare i suoi dati al seguente link: <https://bit.ly/3iCbEPJ>

14:30

ieri • 15

Ordine di bonifico dall'INPS con identificativo 001489 non riuscito, Correggi i tuoi dati: <https://bit.ly/3bPIIT2>

In data odierna è stato rilevato un accesso anomalo, se non è stato lei acceda al seguente link: <https://accesso.dati.79-137-207-161.cprapid.com/ital-1/>

17:58

Messaggio di testo • SMS
oggi 06:40

INPS: Per proseguire con l'erogazione di 280a, sul tuo conto controlla i dettagli: <https://inps.multiscreensite.com/its>

Grazie alla tua fedeltà Poste Italiane ti regala 50 euro di credito telefonico Gratuito vai sul sito www.bancopostaitaliana.it completa l'operazione in 24 ore

lunedì 3 aprile 2023

In data odierna è stato rilevato un accesso anomalo, se non è stato lei acceda al seguente link: <https://accesso.dati.79-137-207-161.cprapid.com/ital-1/>

17:58



Esempi di truffe via Whatsapp

Buono Spesa Carrefour
Ricevi un buono di
Carrefour del valore di €
100
www.carrefour.com



Guarda: <http://mypromo.co/carrefour/>

Un buono Spesa di 100€
Carrefour .
Stanno celebrando il loro
60esimo anniversario e
sono in quantità limitata. Io
già l'ho preso. ❤️❤️

13:05 ✓✓

Furto di account WhatsApp

Prende il via da un messaggio che l'utente riceve da un suo contatto WhatsApp:

“Ciao, scusami, ti ho inviato per sbaglio un codice, potresti rimandarmelo?”

Pochi istanti dopo, alla vittima viene recapitato un secondo messaggio contenente il presunto codice, questa volta da parte di WhatsApp. Convinto che non ci sia nulla di cui preoccuparsi, l'utente segue la richiesta e, in maniera del tutto inconsapevole, commette l'errore. Appena la sequenza numerica viene inviata ai truffatori, l'account è irrimediabilmente perduto.



Truffa del bonifico (furto di identità)

Sono io mamma ho perso il telefono, questo é un nuovo numero lo puoi salvare e scrivermi su whatsapp? <https://wa.me/+39328> [redacted]

Non fidiamoci mai di promozioni “troppo belle per essere vere”.

Controlliamo sempre che le informazioni che troviamo sulle piattaforme social o sul web arrivano direttamente dai canali ufficiali delle aziende in questione.

Ricordatevi che se un prodotto viene proposto a prezzi regalo vuol dire che il prodotto siete voi!