

Lezione 22 del 27-04-2023

Le truffe

Corso android per smartphone

Sicurezza e Privacy: i domini internet



Indirizzo o url corretto ✓

https://www.cadadie.it/corsi
https://servizioclienti.poste.it
postepay.poste.it

https = protocollo
www = dominio di 3° livello
cadadie = di 2° livello (dominio vero e proprio)
it = di 1° livello (TLD = Top Level Domain)
corsi = cartelle presenti nel dominio

https://securelogin.poste.it/jod-fcc/fcc-authentication.html
http://142.250.217.68/search?q=cadadie

Indirizzo o url non corretto ✗

http://poste.cadadie.it
http://servizioclienti-poste.it
www.serviziocartedicredito-postepay.it
chebancaclienti.com
posteditalia.info
poste.com
poste-pay.eu
http://m.facebook.com_____validate____step1.rickytailk.com/sign_in.html

<https://www.emailveritas.com/url-checker>

Sicurezza e Privacy



via SMS

• Messaggistica

10:56 | 0,1KB/s

PosteInfo

PosteID - CODICE SMS: ██████████ Per autorizzare l'autenticazione di livello 2 di sicurezza, inserisci il codice indicato. Cordiali saluti. ✓

7/12/2021 15:40

Gentile cliente risulta un'anomalia sulla sua postepay eviti il blocco e completi la verifica: <https://bancoposte2> ✗

Messaggio di testo

10:22

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. ✗

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

Il tuo pacco è stato trattenuto presso il nostro centro di spedizione. Si prega di seguire le istruzioni qui: <http://██████████> ✗

Ieri • 15:18

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

Tocca per caricare l'anteprima

Sicurezza e Privacy

via WhatsApp



• Messaggistica

Buono Spesa Carrefour
Ricevi un buono di
Carrefour del valore di €
100



www.carrefour.com

Guarda: [http://mypromo.co/
carrefour/](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 ✓



ZARA

Buono 150€ Zara

Ricevi un coupon di Zara
del valore di € 150
www.zara.com

Appena presooo 😁

<http://ft3.co/zara/>

09:12



Per esempio:

Ikea (concorso con buono da 500 euro),
Zara (Coupon da 150 euro),
H&M (buono sconto da 100 euro),
Apple (iPhone 7 a prezzi stracciati),
Carrefour (buono spesa da 100 euro).

Se si clicca sul link, si accederà ad una pagina con un questionario da compilare per avere diritto allo "sconto", che ruberà i dati personali.

In altri casi verrà richiesto di inoltrare il messaggio ad almeno 10 contatti per sbloccare la promozione. Oppure potrebbe attivare servizi in abbonamento che prelevano fino a 5 euro settimanali dal credito telefonico.



Truffa del bonifico (furto di identità)

Sicurezza e Privacy



• Social



Nei **Social** la tendenza è abbassare le difese per cui bisogna prestare maggiore attenzione a:

- >inviti da presunti amici
- >offerte vantaggiose inviate
- >comunicazioni da banca, poste, provider telefonici...
- >comunicazioni in situazioni di emergenza molto diffuse mediaticamente.

Un **altro tipo di attacco** più subdolo: è l' "URL Padding" .

Un messaggio contenente un link "camuffato" così:
http://m.facebook.com-----validate---step1.rickytaylk.com/sign_in.html

sul display di uno smartphone sembrerà il link a Facebook, se cliccato indirizzerà verso un sito "fake" del tutto simile a Facebook, dove verrà chiesto di inserire le proprie credenziali Facebook.



Sicurezza e Privacy



Marketplace
€ 150 - In blocco 11 accessori PC -
Contrassegna come in sospeso

Ok compro In cambio effettuerò il pagamento tramite GLS Express Consegna espressa in una busta al ricevimento del denaro, invierò GLS a casa tua per il ritiro. In altre parole, ti mando i soldi tramite GLS in contanti, e una volta ricevuti i soldi, il servizio verrà ritirato a mie spese ricevuti i soldi, il servizio verrà ritirato a mie spese a casa tua.

Facebook search bar with the 'f' logo and a magnifying glass icon.

Marketplace

Ciao
Nikolleta
Gentile signore o signora, mi dispiace contattarvi, sto condividendo queste informazioni con voi attraverso questo canale perché voglio donare la mia proprietà. A quanto pare ho un tumore al cervello. Il medico che mi ha detto che i miei giorni erano contati. Ho intenzione di donare tutto il mio patrimonio perché ho 465.000 euro sul mio conto e non voglio lasciarli in banca. Sto cercando qualcuno che erediti la mia proprietà. Contattami via email o WhatsApp se sei interessato. Email: nikolettantoni@gmail.com whatsapp +30 697 356 3026 Grazie mille

! Gentile Cliente, in queste ore stiamo assistendo a diverse **campagne di phishing** che utilizzano il marchio di GLS Italia. Le ricordiamo che **GLS non chiede pagamenti via SMS e non utilizza mai nomi di dominio o link diversi da gls-italy.com**. Vi chiediamo di prestare attenzione anche alle e-mail con allegati sospetti, che vi invitiamo a non aprire. In caso di dubbio, vi invitiamo a segnalare le e-mail ricevute all'indirizzo **cybersec@gl-italy.com**.

Sicurezza e Privacy



via E-mail

- Messaggistica

INPS Istituto Nazionale per lo Sviluppo Pensionistico

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 il servizio sulla sua BANCA** in caso di mancato pagamento del suddetto importo, come previsto all'articolo delle **Condizioni Generali**.

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

- **Area Servizi Clienti**
- **Area pubblica**, se hai necessità di registrarti

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

Il Servizio Clienti è sempre a tua disposizione.

Diretti esultati

125 ANNI INPS

INPS_official
345.769 follower
2 giorni • 🌐

⚠️ **Attenzione!** È in corso un nuovo tentativo di **#phishing** bancario che esorta la vittima al saldo di presunti **#contributi #INPS** non pagati. Il contenuto dell'**#email** è scritto in italiano corretto e presenta il logo INPS, ma quanto indicato e le modalità suggerite non sono fornite dall'Istituto. Al momento più di 170 persone sono rimaste vittime della frode. Non cliccate sui link e non fornite nessun dato!

Sicurezza e Privacy

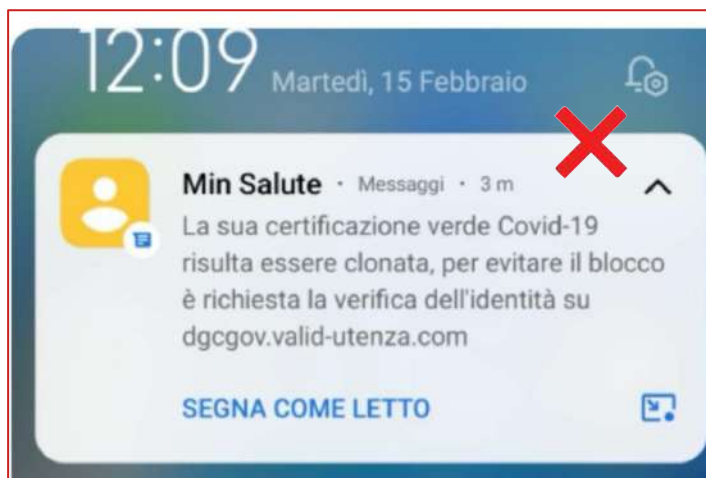


• Messaggistica

Truffe in periodo di Covid



Gli Sms che il Ministero sta inviando ai vaccinati si prestano a essere veicolo di phishing.



Il messaggio falso che circola su WhatsApp

Sicurezza e Privacy



Truffe: altri mezzi di diffusione

Truffe via Browser (pericolosi su smartphone perchè hanno schermi piccoli)

Banner malevoli (attivazione di un servizio in abbonamento) o richieste di consensi.

Truffa del Robocall rispondendo al telefono, si viene accolti da un messaggio registrato. L'obiettivo è quello di far rispondere con un "sì" a domande per autorizzare addebiti .

Truffa dello squillo riagganci dopo un solo squillo e di solito più volte al giorno .L' obiettivo è quello che l'utente richiami così da addebitargli gli alti costi di una telefonata all'estero.

Truffa del QR code (Quick Response) può contenere stringhe alfanumeriche

QR per pagamenti online tramite app bancarie (poche verifiche)

QR come URL (contengono link a siti web di phishing)

QR come numero di telefono fake



Usare app tipo **QR Code Reader and Scanner di Kaspersky Lab Switzerland**



Sicurezza e Privacy



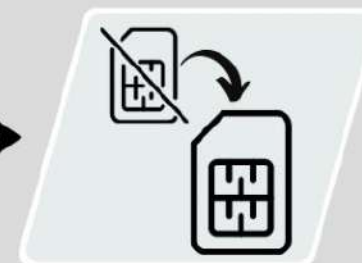
Truffa dello SIM swappig



Il truffatore ottiene i dati personali dell'utente tramite phishing



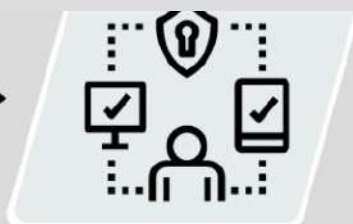
Il truffatore chiama l'operatore telefonico e, con tecniche di persuasione, ottiene il trasferimento del numero (SIM)



L'operatore telefonico trasferisce il numero dell'utente sulla SIM del truffatore



Il truffatore adesso riceve gli SMS e le chiamate della vittima che è ignara fino all'uso del telefono



Il truffatore bypassa facilmente la 2FA



Il truffatore ruba i soldi e cancella tutto

Sicurezza e Privacy



Truffa dello SIM swappig approfondimento

La **SIM** crea una corrispondenza univoca tra la nostra “identità fisica” (la SIM) e la nostra “identità digitale” (il numero di telefono). La terminologia “**SIM swapping**” si riferisce all’atto di **trasferire da una SIM card a un’altra questa corrispondenza** con il nostro numero di telefono. Tale trasferimento può essere effettuato solo tramite operatore telefonico (con imbroglio, corruzione, documenti o dichiarazioni false etc...)

Prima del Sim Swapping è necessario catturare tutte le informazioni sensibili relative al cliente, al fine di ricevere **sul loro telefono il codice di autenticazione dell’operazione di bonifico**.

Queste possono essere reperite con falsi sms, false telefonate, ricerche sui social e quantaltro precedentemente descritto

I sintomi che dovrebbero metterci in allarme e cosa fare:

il cellulare, improvvisamente, non è più in grado di connettersi,
chiamare immediatamente il Customer Service del nostro gestore telefonico ed eventualmente **blocca lo scambio della SIM**.

✗ Chiamate da un presunto operatore telefonico che ti informa che ci sono problemi di linea

Non farci caso

✗ Potresti ricevere molte chiamate fastidiose che ti spingono a spegnere il telefono per non essere disturbato.

Non farlo

✗ potresti ricevere un SMS con la stessa informazione

Non fare niente ma:

controlla i tuoi conti online

contatta il Servizio Clienti della tua banca e blocca l’operatività temporaneamente



Sicurezza e Privacy

Come difendersi da un attacco approfondimento

- > Non utilizziamo il nostro numero di telefono per processi di autenticazione a due fattori che prevedano come modalità di ricezione del secondo fattore di autenticazione l'invio di un SMS.
- > Usare solo altri sistemi one time password (via app).
- > Se la banca lo consente meglio utilizzare una verifica via email su casella protetta.
- > Se la banca lo consente configuriamo l'accesso sicuro a due fattori tramite l'app della banca, che può usare l'impronta digitale del telefono o un PIN segreto per autorizzare tutti gli accessi e le transazioni, rendendo di fatto obsoleto l'invio via SMS.
- > Controlla sempre

Da: Intesa Sanpaolo Private Banking <contatto@intesasanpaoloprivate.com>
Data: 1 Maggio 2019 ore 11:5
A: [il tuo indirizzo email]
Oggetto: Aggiornamento del numero di cellulare [il tuo numero]

ATTENZIONE AL MITTENTE
email non ufficiale

INTESA SANPAOLO PRIVATE BANKING

Gentile Cliente

Come annunciato in precedenza, tutti i clienti avranno presto bisogno di confermare i bonifico tramite SMS o tramite notifiche PUSH sull'applicazione mobile.

Per confermare i bonifico il codice O-Key saranno disattivate dal 4° maggio 2019.

Per accertarti di poter confermare i bonifico, controlla le impostazioni per verificare che il tuo numero di cellulare sia aggiornato. Una volta inserito il numero di cellulare corretto, il servizio inizierà a funzionare automaticamente.

CLICCA QUI

non ti chiederemo mai di confermare via mail le tue credenziali

errori di battitura

Banco Intesa Sanpaolo Private Banking lavora continuamente per migliorare la sicurezza della sua piattaforma online. Contribuirà a mantenere i nostri clienti al sicuro tramite SMS e notifiche push. Per favore si assicuri che i dettagli siano corretti per poter confermare i bonifico tramite SMS o tramite l'applicazione prima del 4° maggio 2019.

Banco Intesa Sanpaolo Private Banking si preoccupa della tua sicurezza e non ti invia comunicazioni che richiedano l'inserimento di credenziali o di dati sensibili.

Sicurezza e Privacy



Come difendersi da un attacco approfondimento

il mittente è corretto
MA... Attenzione!!!!

SMS autentici 

SMS fraudolento (smishing) 

ora i frodatori possono utilizzare il nome corretto "Gruppo ISP" per mimetizzarsi tra gli SMS ufficiali

ATTENZIONE AL LINK numero non ufficiale



Gruppo ISP >

Messaggio
Jun 29 apr, 17:32

O-Key SMS - Usa [453959](#)
per entrare nel sito della tua banca online

mar 30 apr, 17:06

O-Key SMS - Usa [423857](#)
per autorizzare

mer 1 mag, 17:10

Intesa Sanpaolo: Gentile Cliente invitiamo a mettersi urgentemente in contatto con il nostro ufficio prevenzione frodi chiamando il numero verde [800940828](#)

Messaggio

Verificare che il numero VERDE non sia un fake

Sicurezza e Privacy

Prevenzione contro gli SPYWARE

- Autenticazione a due fattori (2FA)

Concetto di fattore:

qualcosa che conosciamo (Password e/o domande di sicurezza)

qualcosa che abbiamo (token OTP...)

qualcosa che possediamo (impronta digitale, viso)

dove siamo (localizzazione smartphone)

- Scaricare e installare applicazioni solo da app store ufficiali come Google Play

Scaricare con attenzione qualunque tipo di app.

Verificare:

il numero di download

le recensioni (<https://it.trustpilot.com/>)

i permessi richiesti (non dare permessi non congrui con la tipologia di app)

il nome dell'autore.

- Non eseguire mai il “root” dei dispositivi

- Installare tempestivamente gli aggiornamenti del sistema e delle applicazioni

- Effettuare il log out dalle applicazioni, specialmente bancarie

- Cambiare spesso la password dell'account Google e delle Banche



Sicurezza e Privacy



Cosa fare qualora per sbaglio o intenzionalmente si sia cliccato sul link:

1 formattare il dispositivo dal quale hai cliccato e ripristinare le impostazioni di fabbrica

2 informare tutti i contatti in rubrica di cestinare i messaggi provenienti dalla propria utenza

3 modificare tutte le password utilizzate nel dispositivo relative al sito poste italiane o della propria home banking

4 se però hai fornito i tuoi dati bancari devi assolutamente bloccare le carte e sporgere denuncia presso la polizia postale

Sicurezza e Privacy



SEGNALI CHE IL TUO SMARTPHONE HA UN VIRUS



Consumo anomalo del traffico dati



Un virus potrebbe generare un elevato traffico dati. Oltre alle info fornite dal sistema operativo è possibile farsi aiutare in questa analisi da app specifiche [[click qui](#)]



Addebiti fraudolenti



Le app malevole potrebbero effettuare acquisti in-app o iscrizioni ad account premium non desiderate. Scopri come verificare [[click qui](#)]



App che si chiudono da sole con regolarità



A causa di un virus le nostre APP potrebbero avere dei malfunzionamenti e chiudersi spesso da sole. Scopri come verificare il problema [[click qui](#)]



Improvvisi aperture di Popup



Uno dei problemi più fastidiosi, indicatori della presenza di adware nel telefono da rimuovere. Scopri come verificare il problema e se possibile ripulire [[click qui](#)]



Durata molto limitata della batteria



Uno dei segnali più forti è proprio una improvvisa riduzione della durata della batteria. Scopri come verificare il problema [[click qui](#)]



La presenza di APP fake o sconosciute



Scopri come controllare lo stato di certificazione delle APP e visualizzare l'elenco delle app che possiedono i privilegi di amministratore [[click qui](#)]



Un elevato surriscaldamento del telefono



Il virus potrebbe sovraccaricare di lavoro la nostra CPU del telefono o la RAM e generare il problema del calore eccessivo. Scopri come verificare il problema [[click qui](#)]



Rallentamenti dello smartphone



Improvvisamente il telefono è lentissimo. Se avete android per escludere che si tratti di un problema di memoria piena potete verificare con un [[click qui](#)]



Email di spam nella posta inviata



Fate attenzione alle email che vengono inviate nella vostra posta. Un controllo ogni tanto è davvero importante. Andate nella posta inviata e verificate la presenza di email che non vi appartengono