Lezione 15 del 22-02-2024

Truffe

Corso android per smartphone

Docenti Dott.ssa Roberta Lai Ing. Massimo Terrosu

cadadie.it

MALWARE - porta di ingresso per le truffe

Il 96% dei mal(icius soft)ware colpisce Android,
oggi abbiamo una nuova app dannosa ogni 10 secondi

TIPI DI MALWARE

Blocca l'accesso ai dati sul dispositivo e richiede un pagamento per ripristinarlo

Ransomware

E' più utile spiare il dispositivo piuttosto che rubarlo

Spyware

Pegasus, lo spyware della società israeliana NSO, usato per spiare giornalisti, attivisti e capi di Stato.

Trojan horse

Rootkit

Remote access

Pubblicità invasive e raccolta dati personali

Adware

Worm

Virus

Per controllare figli, familiari, dipendenti...

Keylogger

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

Esempi di Truffe - via E-Mail

INPS

Gentile [redacted],

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 [redacted]mento 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'art. [redacted] delle **Condizioni Generali**.

Ti ricordiamo anche che puoi pagare comodamente da casa, evitando alcun costo aggiuntivo tramite:

- Area Servizi Clienti
- Area Pubblica, senza necessità di registrarti

Qualora non eseguiate 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.

Distinti saluti

FAKE

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 del l'#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!

Da: Intesa Sanpaolo Private Banking <contacto@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

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 inva comunicazioni che richiedano l'inserimento di credenziali o di dati sensibili.

errori di battitura

Truffe - Indirizzi Internet o URL

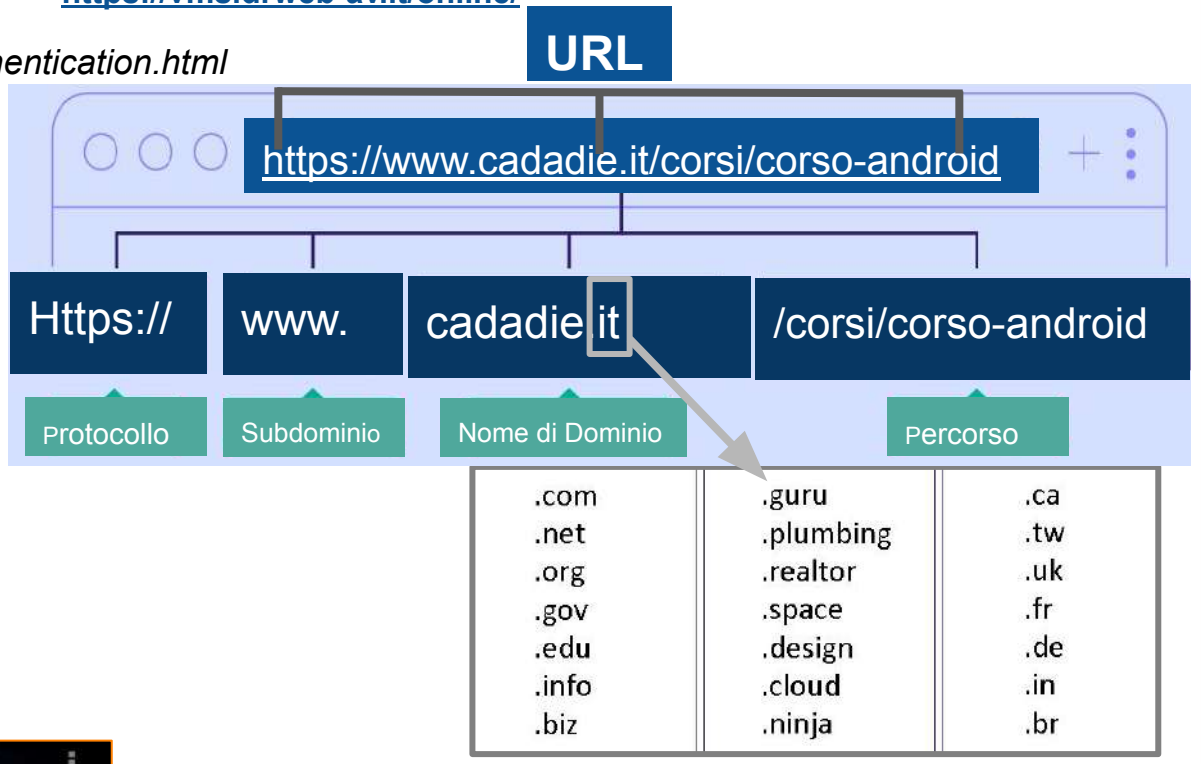
Indirizzo o url corretto

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

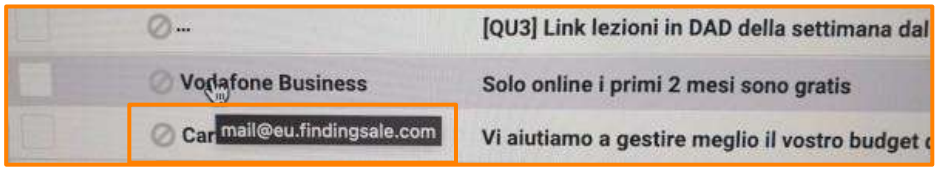
https://toolset.mrw.it/network/redirect-checker.html
https://www.emailveritas.com/url-checker
https://vms.drweb-av.it/online/

Indirizzo o url truffaldino

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

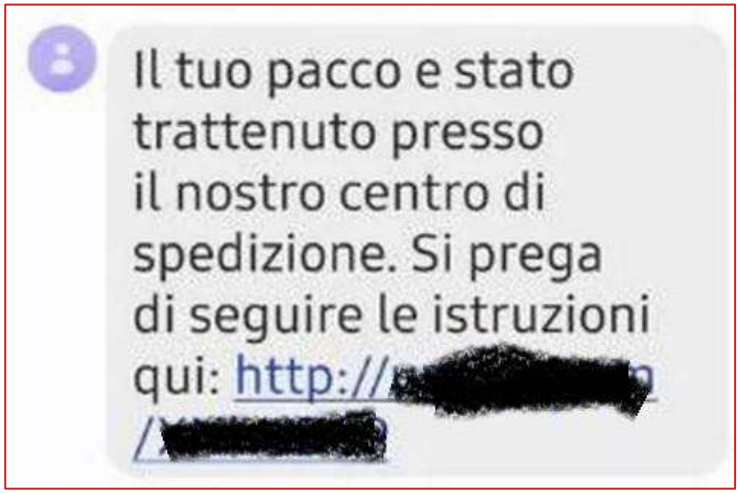


http://m.facebook.com————-validate—-step1.rickytaylk.com/sign_in.html



I domini Internet

Esempi di Truffe - via SMS



Esempi di Truffe - via WhatsApp

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)

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.

Esempi di Truffe - via Facebook

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

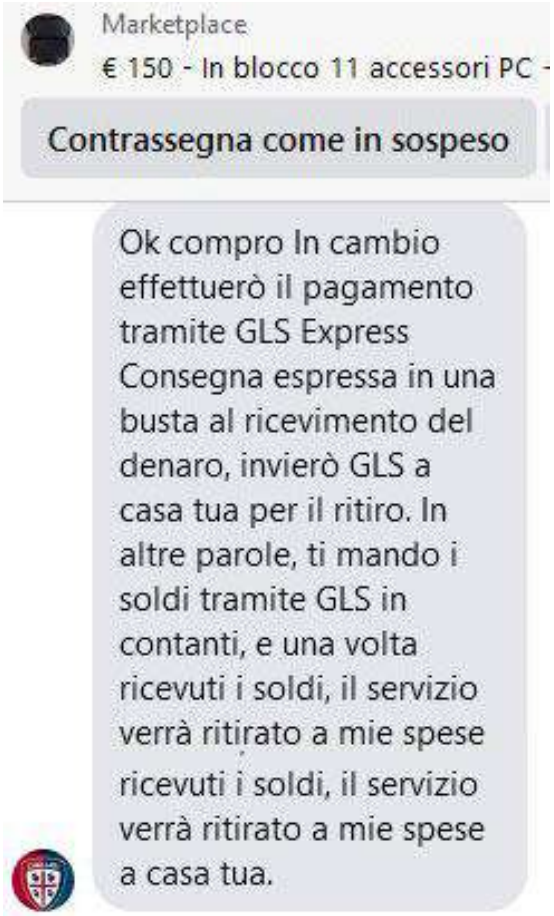
molto diffuse mediaticamente.

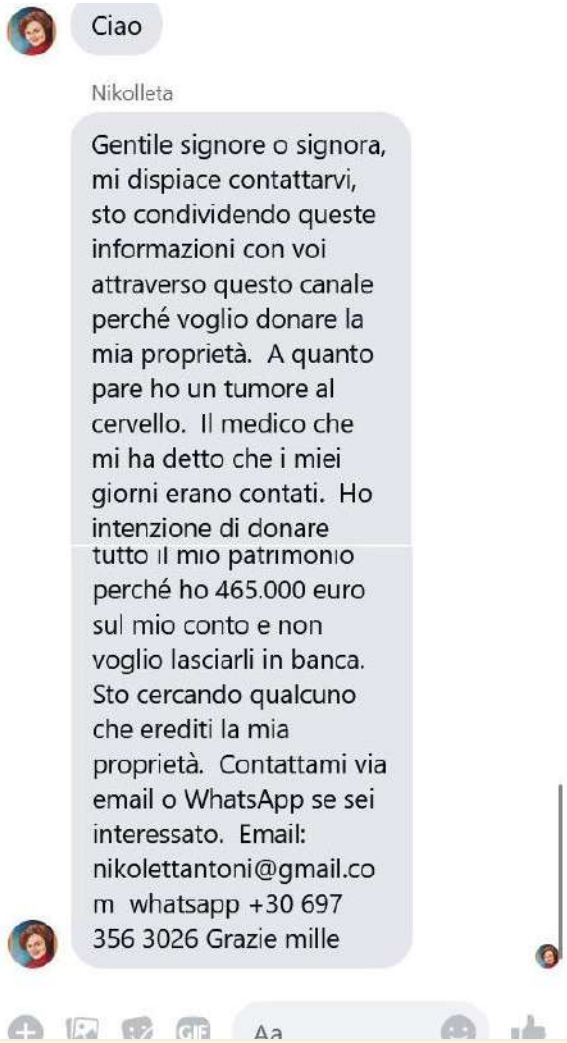
Torna sui social e sulle chat il fantomatico concorso di Pandora per sensibilizzare sul cancro al seno: l'iniziativa è però una truffa, che tramite un link può rubare dati e soldi agli utenti.
Avviene regalando charms: gioielli dall'elevato valore commerciale **a soli due euro**.La spesa di spedizione da affrontare non è altro che un modo per ottenere i dati sensibili della vostra carta di credito.

Non fidiamoci mai di promozioni "troppo belle per essere vere".
Controlliamo sempre che le informazioni che troviamo sulle piattaforme social o sul web arrivino 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!

Esempi di Truffe - via Facebook





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@gls-italy.com.**

Esempi di Truffe - via chiamate

Cagliari, finti impiegati delle Poste cercano di svuotare i conti: “Usano il numero dei carabinieri”

Di Paolo Rapeanu - 6 Febbraio 2024 - CAGLIARI

È quanto capitato a un’impiegata trentottenne residente a Cagliari, M. La donna ha ricevuto una prima **chiamata da un numero fisso e poi una, a prima vista, dal comando dei carabinieri di via Sonnino**.

“Questa persona mi ha detto che stamattina c’è stato un accesso anomalo al mio conto bancario da Bergamo e mi chiedeva se fossi stata io. Io ho detto di no, così mi è stato chiesto dove mi trovassi e ho risposto Cagliari.
Allora mi ha detto che presso la mia filiale di Cagliari era in corso un’indagine per furto di dati e che dopo questa chiamata sarei stata contattata direttamente dai carabinieri della città della mia filiale . Questa persona mi ha anche letto dei numeri e mi ha chiesto se fossero gli ultimi del mio conto, ma io ho detto che non li ricordavo. Mi ha anche detto che dovevo stare tranquilla perché il numero da cui mi chiamava era di poste italiane e che potevo verificarlo guardando in diretta con lui al telefono sul sito di poste e confrontare il numero. Mi ha anche detto che potevo fidarmi perché ci sono tanti tentativi di phishing vocale telefonico e che essendo quel numero uguale a quello del sito di Poste.
Ho infine chiamato la polizia postale dove mi hanno spiegato le dinamiche di come agiscono e attuano le truffe. Successivamente, ho ricevuto una chiamata molto strana dalla Germania a cui non ho risposto. Credo che questa chiamata fosse collegata alle due precedenti”.

Truffe - altre

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**

Le Truffe - con l'intelligenza artificiale (Deepfake)

I **deepfake** sono foto, video e audio creati grazie a software di intelligenza artificiale (AI) che, partendo da contenuti reali (immagini e audio), riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e a imitare fedelmente una determinata voce.

VIDEO FALSI

Questi video utilizzano l'intelligenza artificiale per sostituire perfettamente il volto di una persona con quello di un'altra, creando l'illusione che stia dicendo o facendo qualcosa che non ha mai fatto. Questo può essere utilizzato per impersonare amministratori delegati, politici o celebrità a scopo di lucro, ricatto o danno alla reputazione.

CLONAZIONE DELLA VOCE

L'intelligenza artificiale può essere utilizzata per creare simulazioni realistiche della voce di una persona, consentendo ai truffatori di impersonarla al telefono, nei messaggi vocali o persino nelle conversazioni dal vivo. Questo può essere usato per ingannare le vittime e indurle a inviare denaro o a fornire informazioni sensibili.

GENERAZIONE DEL TESTO

L'intelligenza artificiale può essere utilizzata per generare testi realistici e credibili, che possono essere usati per creare articoli di notizie false, post sui social media o persino email. Questo può essere usato per diffondere disinformazione, manipolare l'opinione pubblica o truffare un individuo.

Le Truffe - rimedi

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

Le Truffe - 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

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]

Improvvise 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 sovraccaricate 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