Social Engineering e Cyber Security Awareness

Michele Petito, Agid

18/06/2021 12:45-13:20

Social engineering

- Il social engineering rappresenta **un insieme di tecniche utilizzate dai cybercriminali per attirare gli ignari utenti ad inviare loro i loro dati riservati**, infettare i loro computer tramite malware o aprire collegamenti a siti infetti.
- Il tecnica più diffusa avviene tramite l'uso della **posta elettronica**. Le-mail di phishing cercano di convincere gli utenti che esse provengono in realtà da fonti legittime, nella speranza di procurarsi anche pochi dati personali o aziendali.

Social engineering

Le varie tecniche di attacco

Social

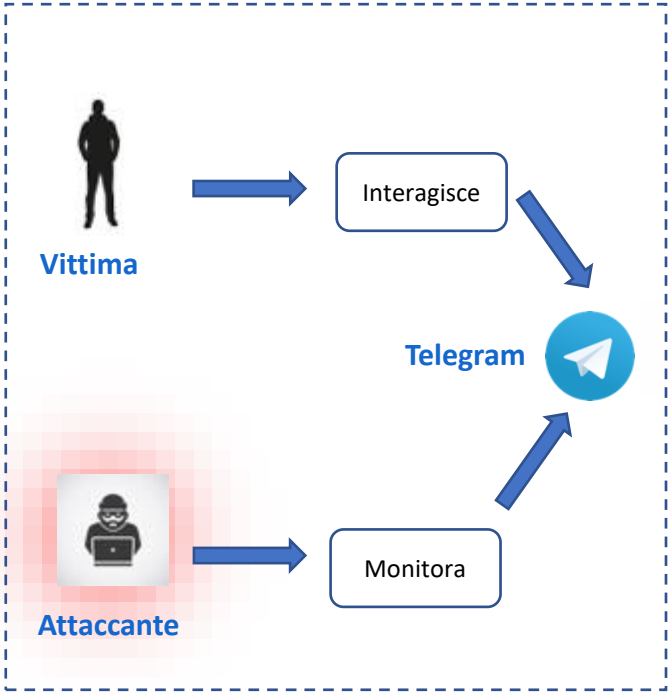
Video

Sms

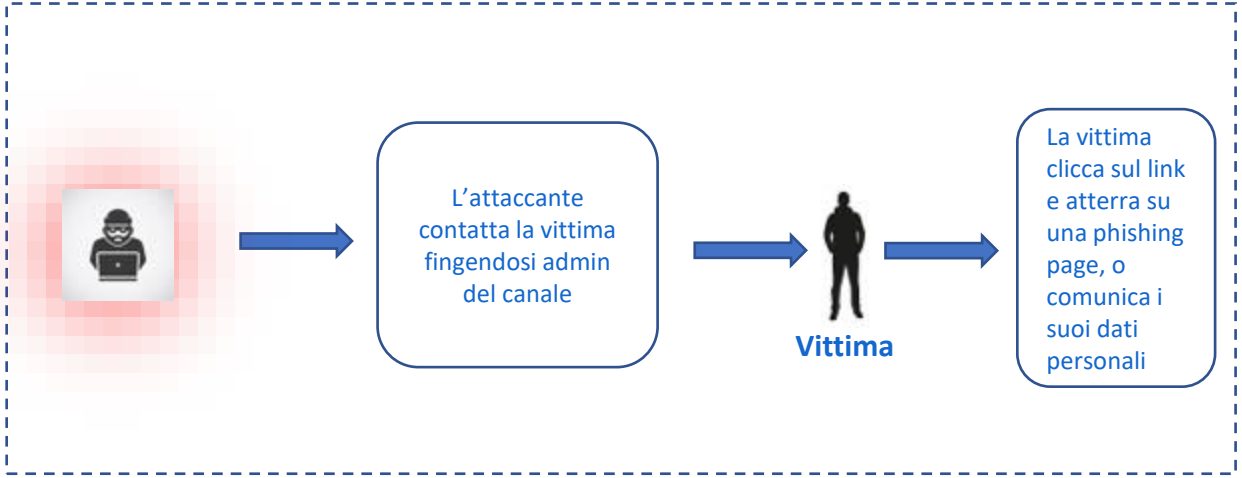
Social engineering

Via Telegram

FASE 1 – INFORMATION GATHERING



FASE 2 – ATTACCO



Social engineering

Via Whatsapp

1 Attaccante

Installa whatsapp su un altro device → Invia messaggio whatsapp → **«Ciao, scusa se ti ho inviato un codice di 6 cifre tramite SMS per errore, puoi trasferirmelo per favore? È urgente»**

2 Vittima

Riceve un sms → Your WhatsApp code: 591-059

You can also tap on this link to verify your phone: v.whatsapp.com/591059

Don't share this code with others

→ Riceve un messaggio whatsapp → Invia il codice che consente all'attaccante di attivare whatspapp

3 Amico della vittima

Riceve messaggi whatsapp dal finto amico → 

→ **«Ho comprato da internet, ma la mia carta di credito è scaduta. Posso usare la tua e ti faccio un bonifico»**

Social engineering

Via Whatsapp

Come difendersi

- **Non condividere con nessuno il codice di verifica a 6 cifre che WhatsApp** invia tramite SMS
- **In generale, non fidarti di nessuno**, neanche degli amici in rubrica, soprattutto se ti chiedono informazioni personali, codici o password
- **Abilitare la verifica in due passaggi** da «Impostazioni > Account > Verifica in due passaggi > Abilita»
- **Se disponibili, preferire l'utilizzo di app di autenticazione** (es. Google Authenticator e simili) al posto degli sms (facilmente aggirabili)

Deep fake

https://github.com/iperov/DeepFaceLab

http://bit.ly/EinsteinDF

http://bit.ly/TomCruiseDF

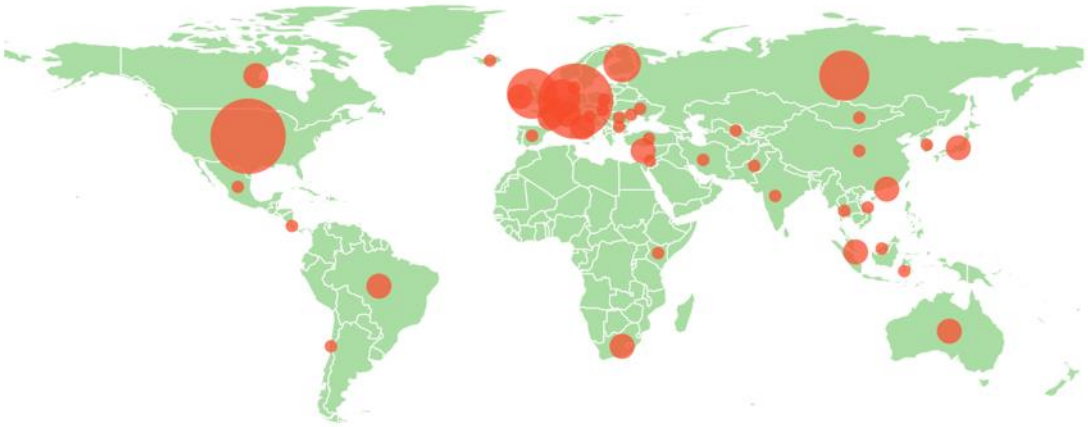
Diffusione del phishing / social engineering

- Secondo il **Rapporto CLUSIT 2021** il "Phishing/Social Engineering" si conferma al terzo posto tra le tipologie di attacco
- Tale categoria dopo una crescita del **+81,9%** rispetto al 2018, nel 2020 rimane stabile.
- Una quota crescente di questi attacchi basati su Phishing si riferisce a **"BEC scams"** che infliggono danni economici sempre maggiori alle loro vittime.

TECNICHE DI ATTACCO PER TIPOLOGIA	2017	2018	2019	2020	2020 su 2019	Trend 2020
Malware	446	585	729	783	7.4%	↑
Unknown	277	408	317	372	17.4%	↑
Known Vulnerabilities / Misconfigurations	127	177	127	184	44.9%	↑
Phishing / Social Engineering	102	160	291	289	-0.7%	↗
Multiple Techniques / APT	63	98	65	95	46.2%	↑
Account Cracking	52	56	86	85	-1.2%	↗
DDoS	38	38	23	34	47.8%	↑
0-day	12	20	30	23	-23.3%	↓
Phone Hacking	3	9	1	3	200.0%	↑
SQL Injection	7	1	1	3	200.0%	↑
TOTALE	1127	1552	1670	1871	+12%	

Global Phishing Activity

Attività di phishing «fotografata» al 13 maggio 2021



Top 10 Targeted Brands

Facebook, Inc.	29.5%
Outlook	9.0%
La Banque postale	6.8%
Interac e-Transfer	6.4%
Office365	4.1%
Commonwealth Bank...	4.0%
Amazon.com Inc.	3.9%
PayPal Inc.	2.3%
Royal Mail	2.2%
Rabobank Nederland	2.1%

Top 10 Sectors

Social Networking	31.1%
Financial	27.9%
Email Provider	10.3%
Online/Cloud Service	9.5%
Payment Service	9.3%
e-Commerce	4.9%
Logistics & Couriers	3.4%
Telecommunications	1.6%
Government	0.7%
Cryptocurrency	0.6%

Fonte OpenPhish: https://openphish.com/

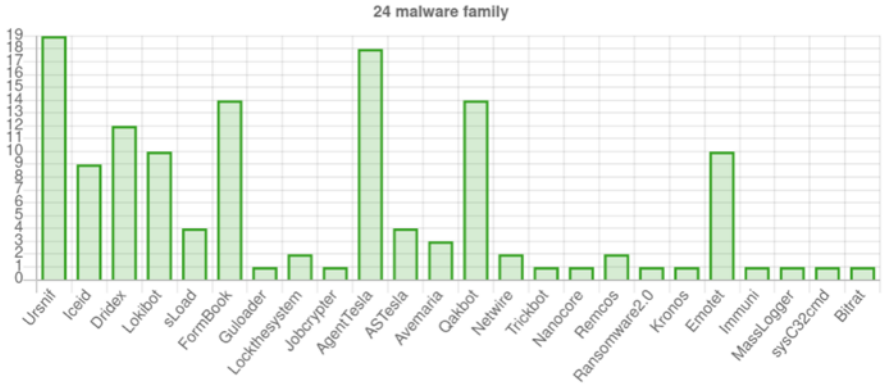
Attacchi phishing ospitati su https

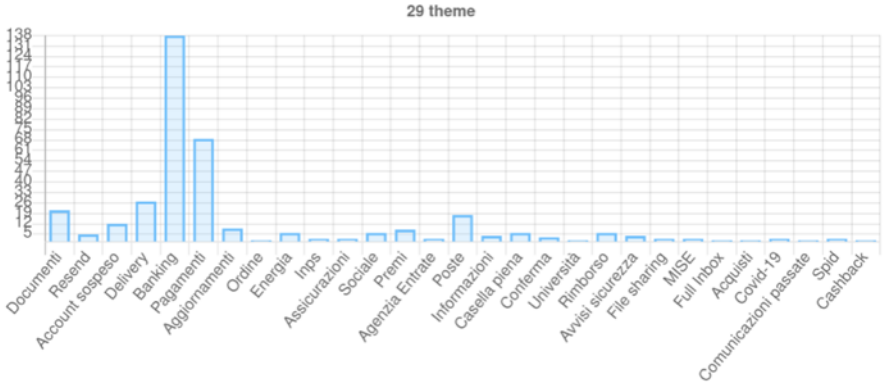
- Secondo uno studio condotto dalla società **PhishLabs**, il numero di siti di phishing che utilizzano TLS continua ad aumentare

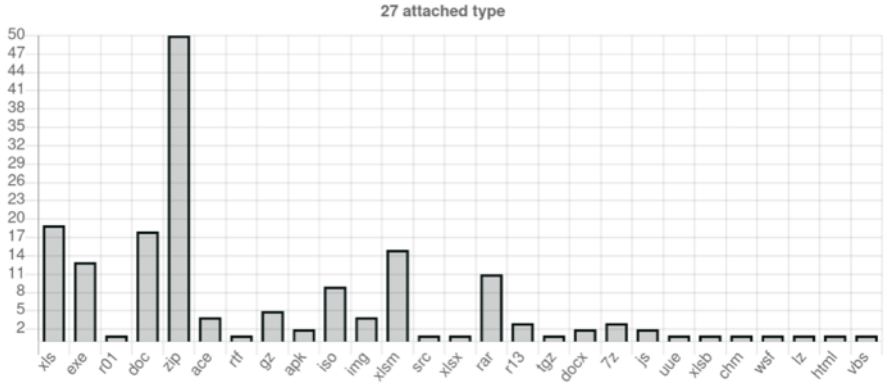
- Il **36,2%** di tutti i **certificati** rilevati nei domini di phishing sono stati emessi dall'autorità di certificazione **Let's Encrypt** che li fornisce gratuitamente.

Campagne malevole in Italia dal 01 gennaio 2021

Via Sms, Pec e Mail



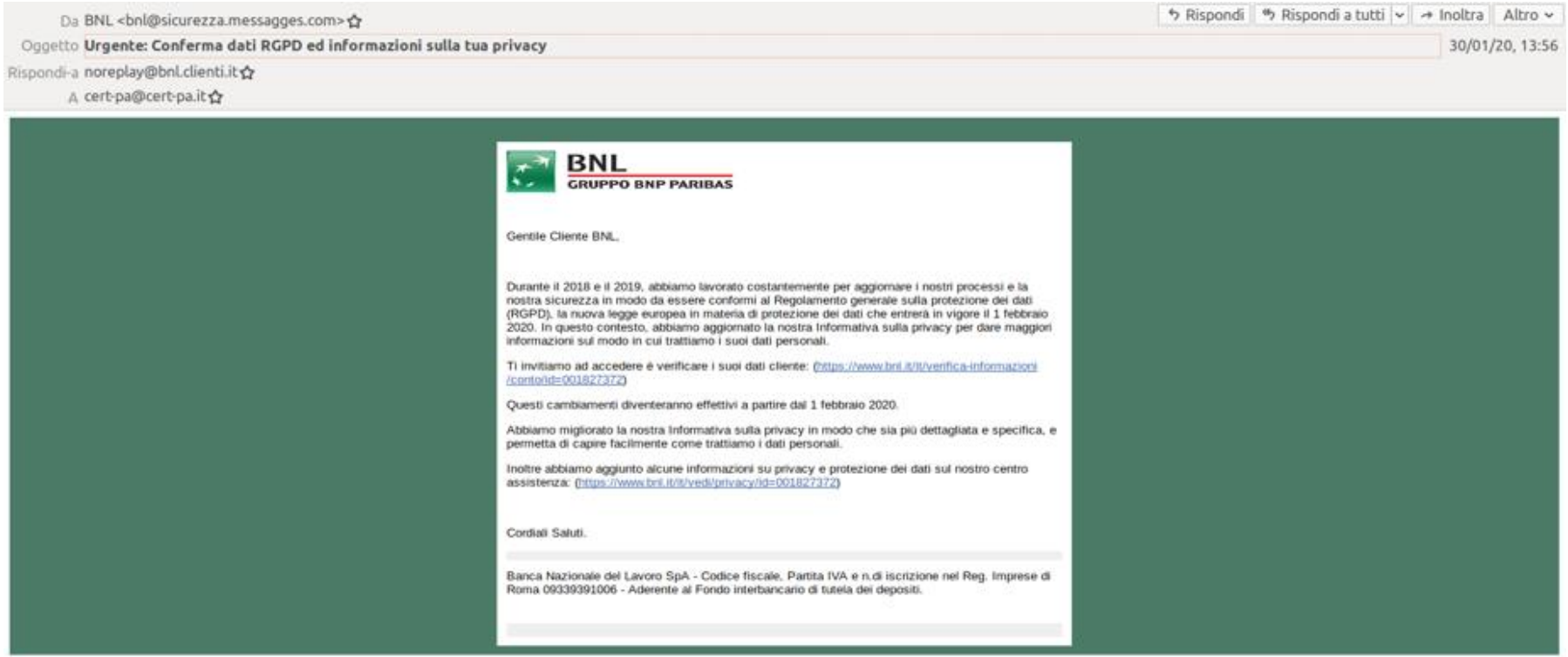




Alcuni domini phishing italiani del 1 aprile 2021

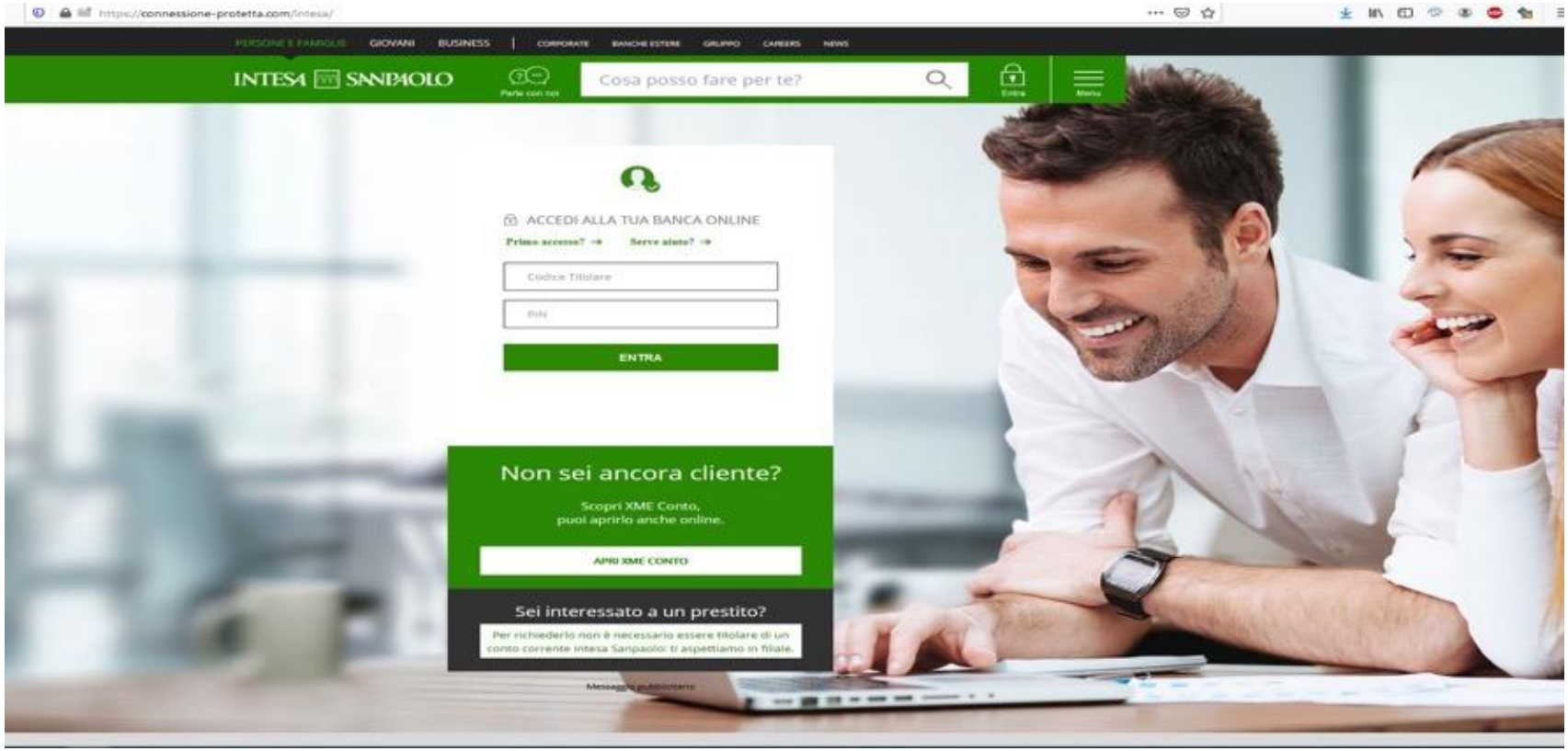
accesso-anomalo-aggiornamento.com
aggiornamento-anomali-sicurezza.com
appaggiorna.com
app-aggiorna.com
appnormativa.com
app-normativa.com
entradesso.work
evolution-postepay.com
identificazione-sicurezza-app.com
infoprivati.com
modulazione-aggiornamento-gisp.com
normativa-web-app.net
portale-info.com
portale-psd2.com
portaleweb1-Intesasanpaolo.xyz
portaleweb2-Intesasanpaolo.xyz
portaleweb3-Intesasanpaolo.xyz
protocollo-dati2021.com
psd2-italia.com
pt-italiane.com

Esempio di phishing a tema Banking - (1.1)

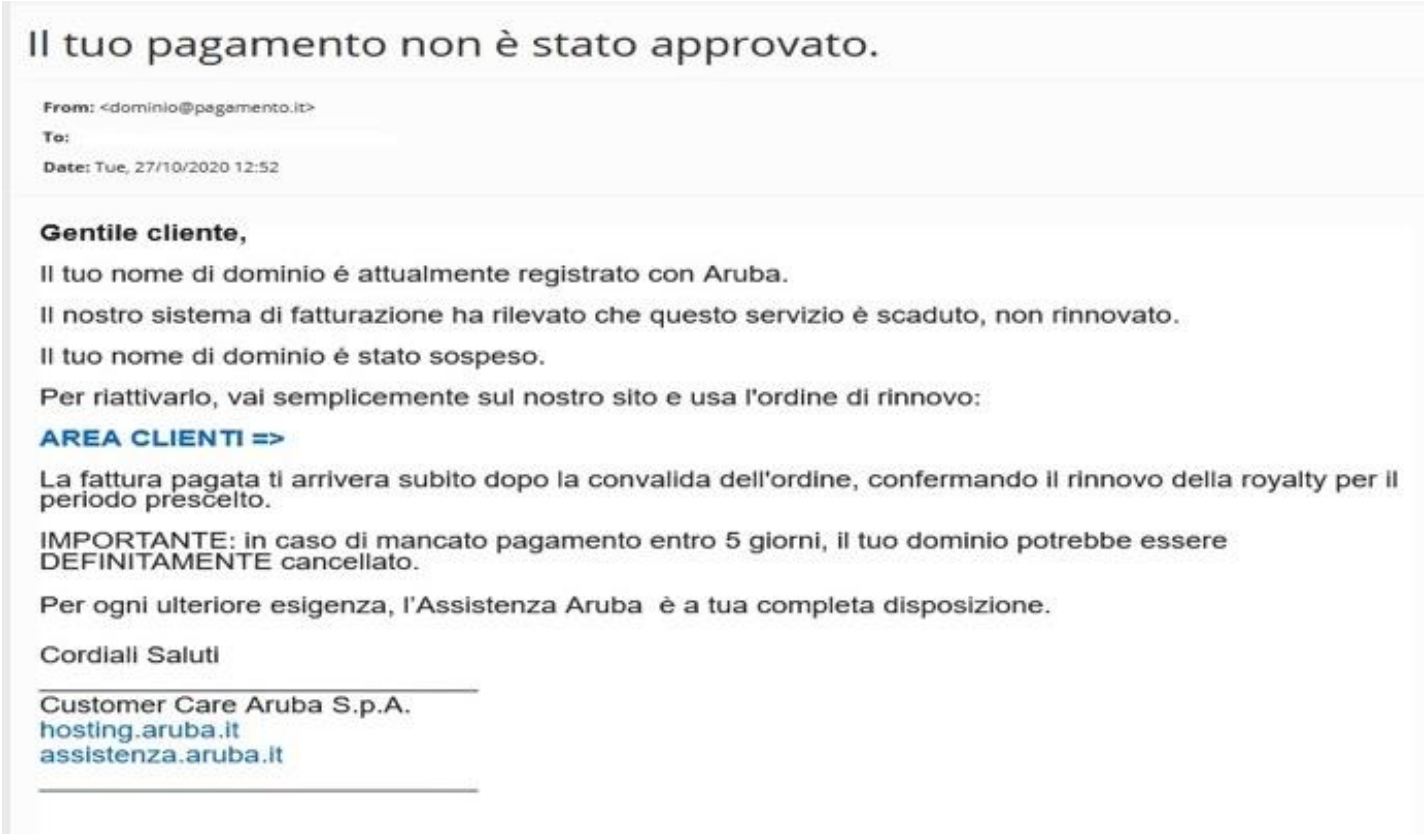


Esempio di phishing a tema Banking - (1.2)

Esempio di phishing a tema Banking



Esempio di phishing a tema «dominio scaduto»



Il tuo pagamento non è stato approvato.

From: <dominio@pagamento.it>
To:
Date: Tue, 27/10/2020 12:52

Gentile cliente,

Il tuo nome di dominio é attualmente registrato con Aruba.

Il nostro sistema di fatturazione ha rilevato che questo servizio è scaduto, non rinnovato.

Il tuo nome di dominio é stato sospeso.

Per riattivarlo, vai semplicemente sul nostro sito e usa l'ordine di rinnovo:

AREA CLIENTI =>

La fattura pagata ti arrivera subito dopo la convalida dell'ordine, confermando il rinnovo della royalty per il periodo prescelto.

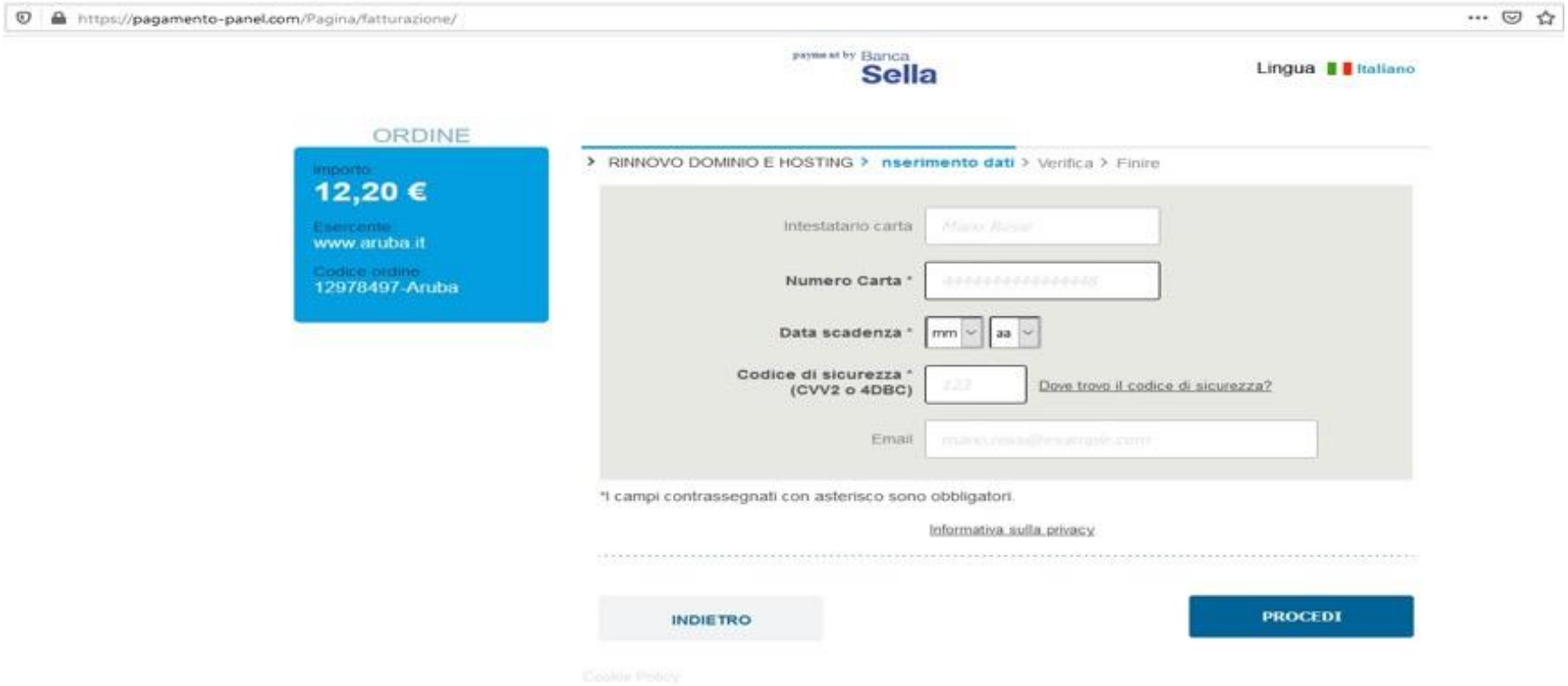
IMPORTANTE: in caso di mancato pagamento entro 5 giorni, il tuo dominio potrebbe essere DEFINITAMENTE cancellato.

Per ogni ulteriore esigenza, l'Assistenza Aruba è a tua completa disposizione.

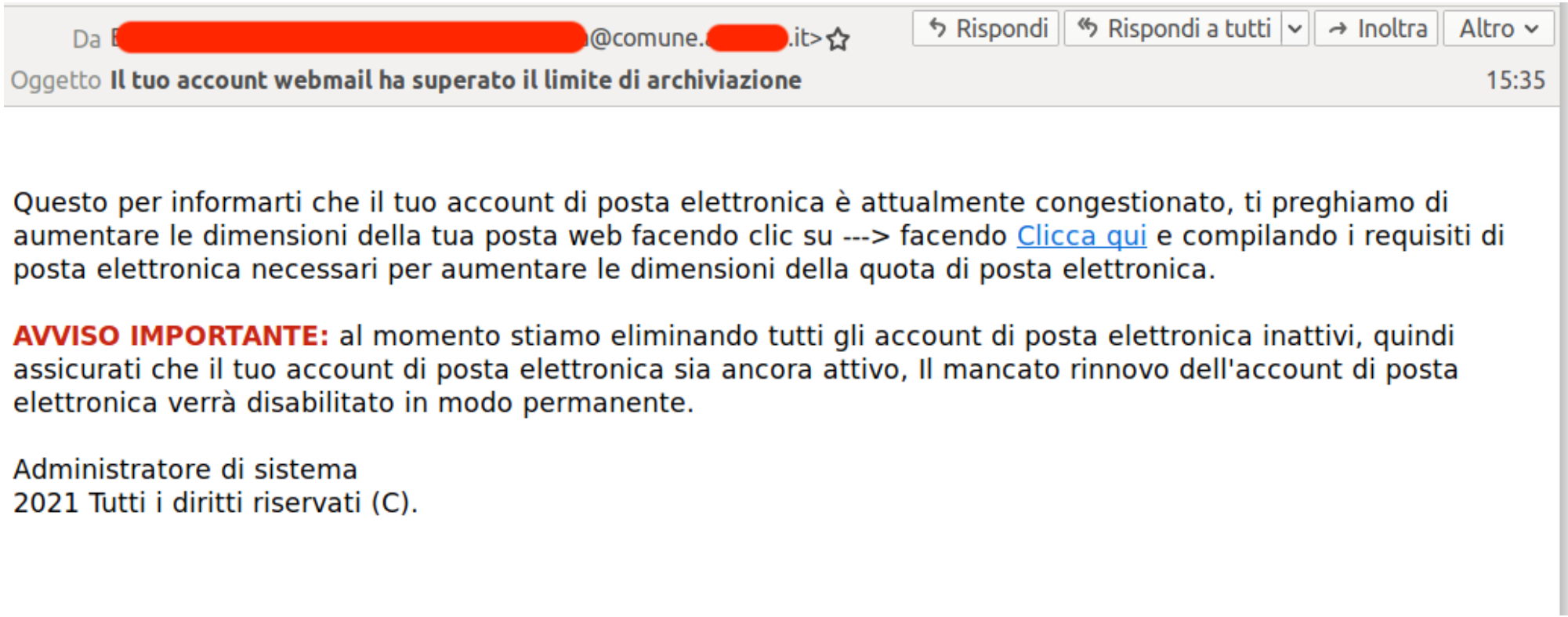
Cordiali Saluti

Customer Care Aruba S.p.A.
hosting.aruba.it
assistenza.aruba.it

Esempio di phishing a tema «pagamenti»



Esempio di phishing a tema «casella piena»



Da [redacted]@comune.[redacted].it>

Rispondi | Rispondi a tutti | Inoltra | Altro

Oggetto **Il tuo account webmail ha superato il limite di archiviazione** 15:35

Questo per informarti che il tuo account di posta elettronica è attualmente congestionato, ti preghiamo di aumentare le dimensioni della tua posta web facendo clic su ---> facendo Clicca qui e compilando i requisiti di posta elettronica necessari per aumentare le dimensioni della quota di posta elettronica.

AVVISO IMPORTANTE: al momento stiamo eliminando tutti gli account di posta elettronica inattivi, quindi assicurati che il tuo account di posta elettronica sia ancora attivo, Il mancato rinnovo dell'account di posta elettronica verrà disabilitato in modo permanente.

Administratore di sistema
2021 Tutti i diritti riservati (C).

Esempio di phishing a tema delivery

Da DHL Customer Support <support@dhl.com>
Oggetto **DHL GST NOTIFICATION FOR INCOMING SHIPMENT ** AWB: 2352366446 Confirm your Shipment URGENT**
A Recipients <support@dhl.com>

AUTHORIZED SHIPPING CENTER

Dear Customer,

There is a package bearing your name at our local dispatch facility.

Package delivery personnel arrived at your listed address but could not find you.

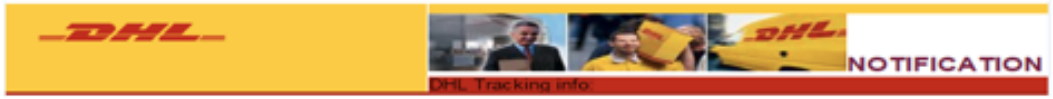
Update us with your recent address to enable swift delivery.

Find Attached To Confirm And Update Your Address And Shipping Details.

If your shipping address is not confirm within 48 hours,
your package will not be delivered.

Contact us for further help.

Best Regards
DHL Express



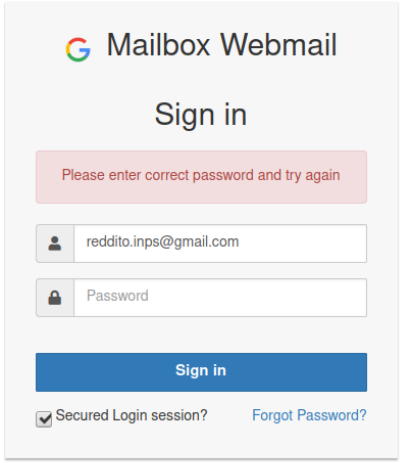
1 allegato: Shipping Doc_PDF.rar 178 kB
Shipping Doc_PDF.rar 178 kB

Phishing mail generico su storage di Amazon (S3)

PHISHING URL

https://taivonbucket56.**s3**.eu-de.cloud-object-storage.appdomain.cloud

Richiesta POST



Best practices

- Quando ricevi un'email presta la massima attenzione, verifica che la mail sia autentica**, guarda bene chi è il mittente e pensaci due volte prima di cliccare** su eventuali link o allegati

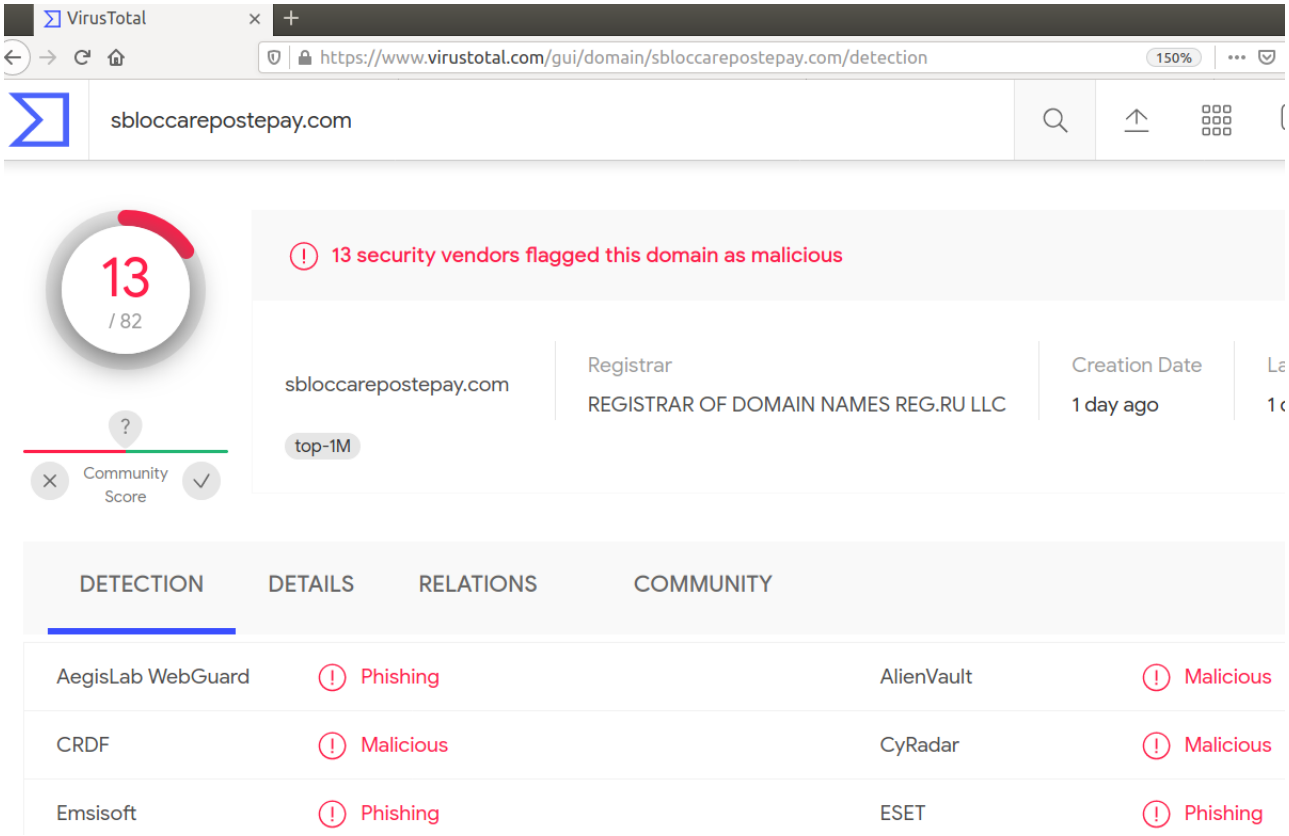
- **Non fornire informazioni sensibili a chi vi contatta di persona**, via mail o social

- Controlla bene le URL, in particolare se contiene:
  - **Dominio non correlato** con l'azienda che ha inviato il messaggio
  - **Errori ortografici**
  - **Sequenza di simboli random** nell'indirizzo internet
  - **Simboli provenienti da altre lingue** simili all'alfabeto latino

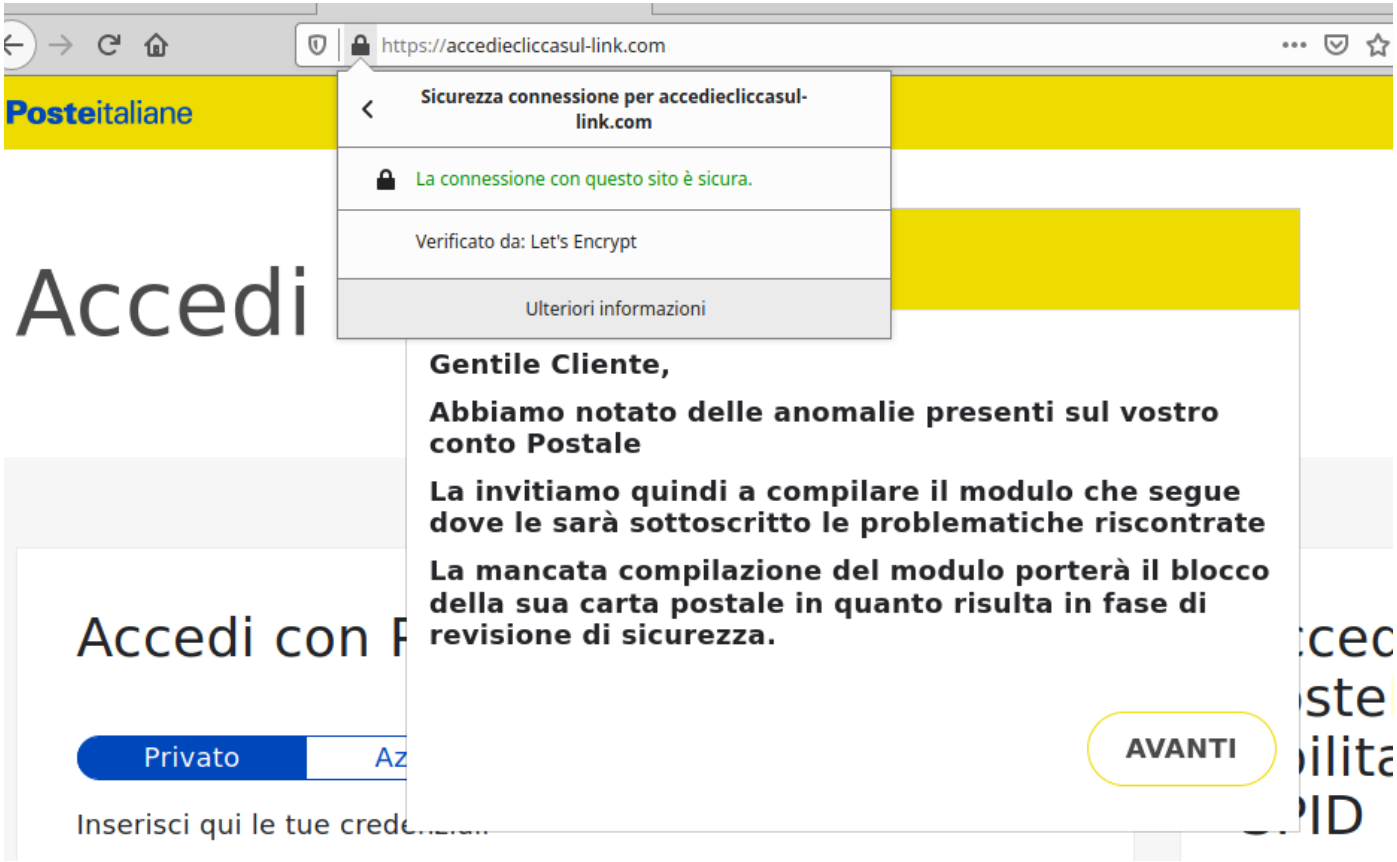
- Se non sei sicuro che una richiesta e-mail sia legittima, **prova a verificarla contattando direttamente l'azienda mittente**, tramite i contatti abituali

- Leggere la pillola informativa sul phishing: https://cert-agid.gov.it/download/Phishing-Cert-PA.pdf

Verifica di link e allegati

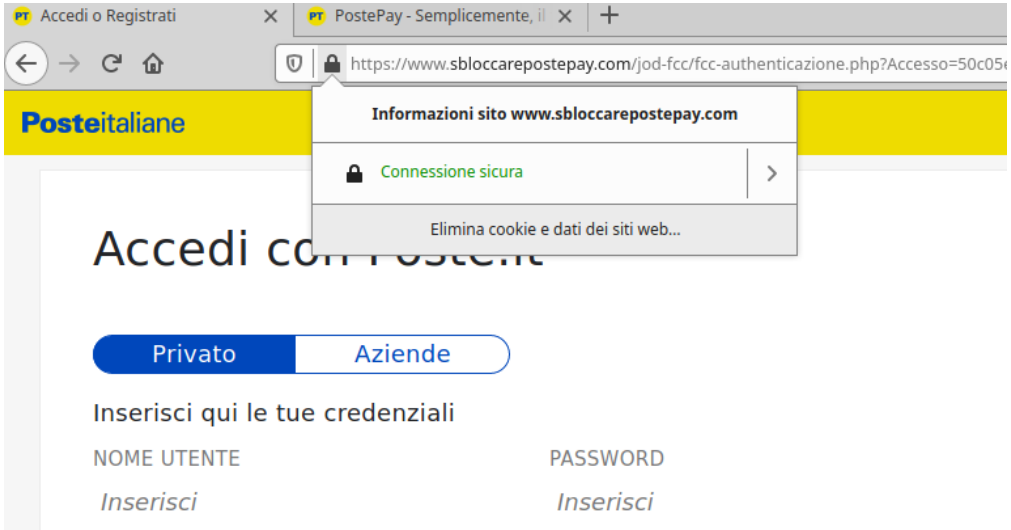


Verifica del certificato

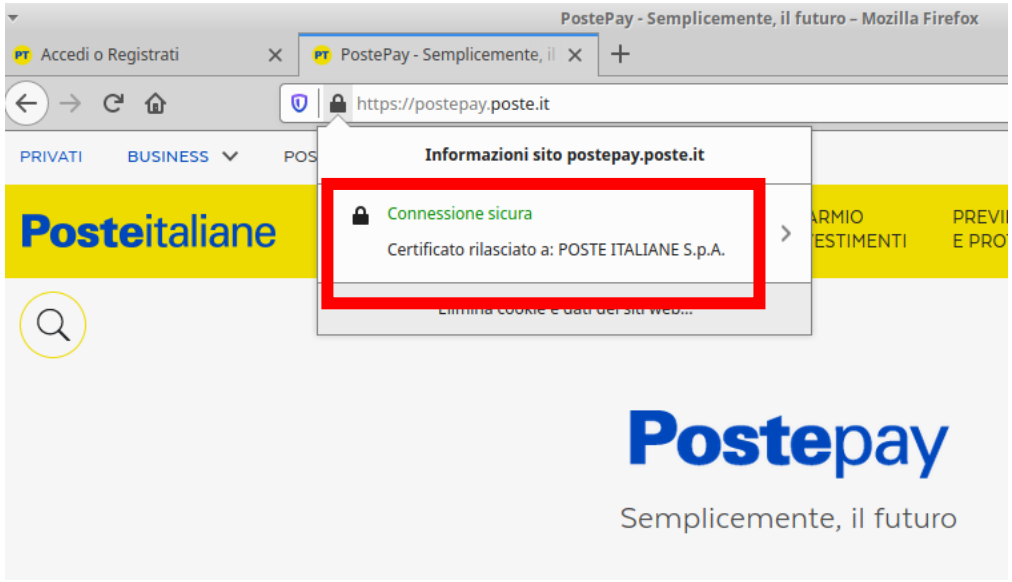


Verifica del certificato

Sito Fake



Sito legittimo



Segnalare un Phishing

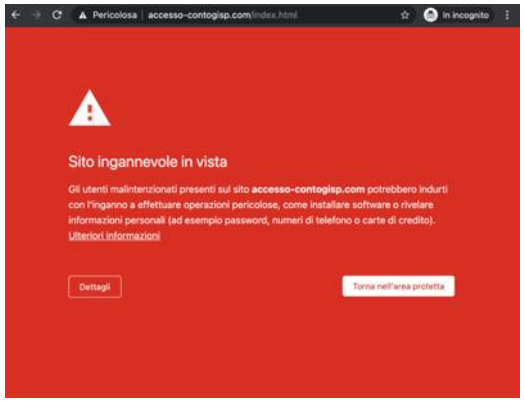
La collaborazione degli utenti è fondamentale per combattere il phishing e bloccare le URL più velocemente.

Alcuni canali per segnalare questi siti fraudolenti :

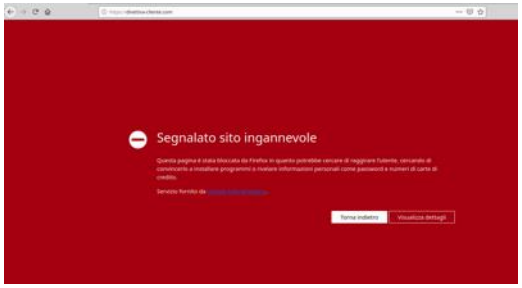
- **Cert-AgID** – malware@cert-agid.gov.it
- **Google** - https://safebrowsing.google.com/
- **Phishtank** - https://www.phishtank.com/

Blocco automatico delle pagine sospette

Chrome



Firefox



Firewall

La miglior difesa è la formazione

> Si possono investire milioni di dollari per i propri software, per l'hardware delle proprie macchine e per dispositivi di sicurezza all'avanguardia, ma se c'è anche solo un unico dipendente della nostra azienda che può essere manipolato con un attacco di ingegneria sociale, tutti i soldi investiti saranno stati inutili

Kevin Mitnick

Simulazione di campagne phishing all'interno della PA

- **Gophish** è un phishing framework **Open Source** che **permette di simulare campagne di Phishing**;
- **Consente l'invio delle email fraudolente**, la creazione della finta pagina web che dovrà carpire le informazioni sensibili e di monitorare la campagna.
- Ottimo per simulare all'interno della propria organizzazione una campagna di Phishing e **individuare il personale più vulnerabile e da formare**.
- Gophish è uno strumento **multi piattaforma**, sviluppato in Go, utilizzabile su Linux, MacOS e Windows.

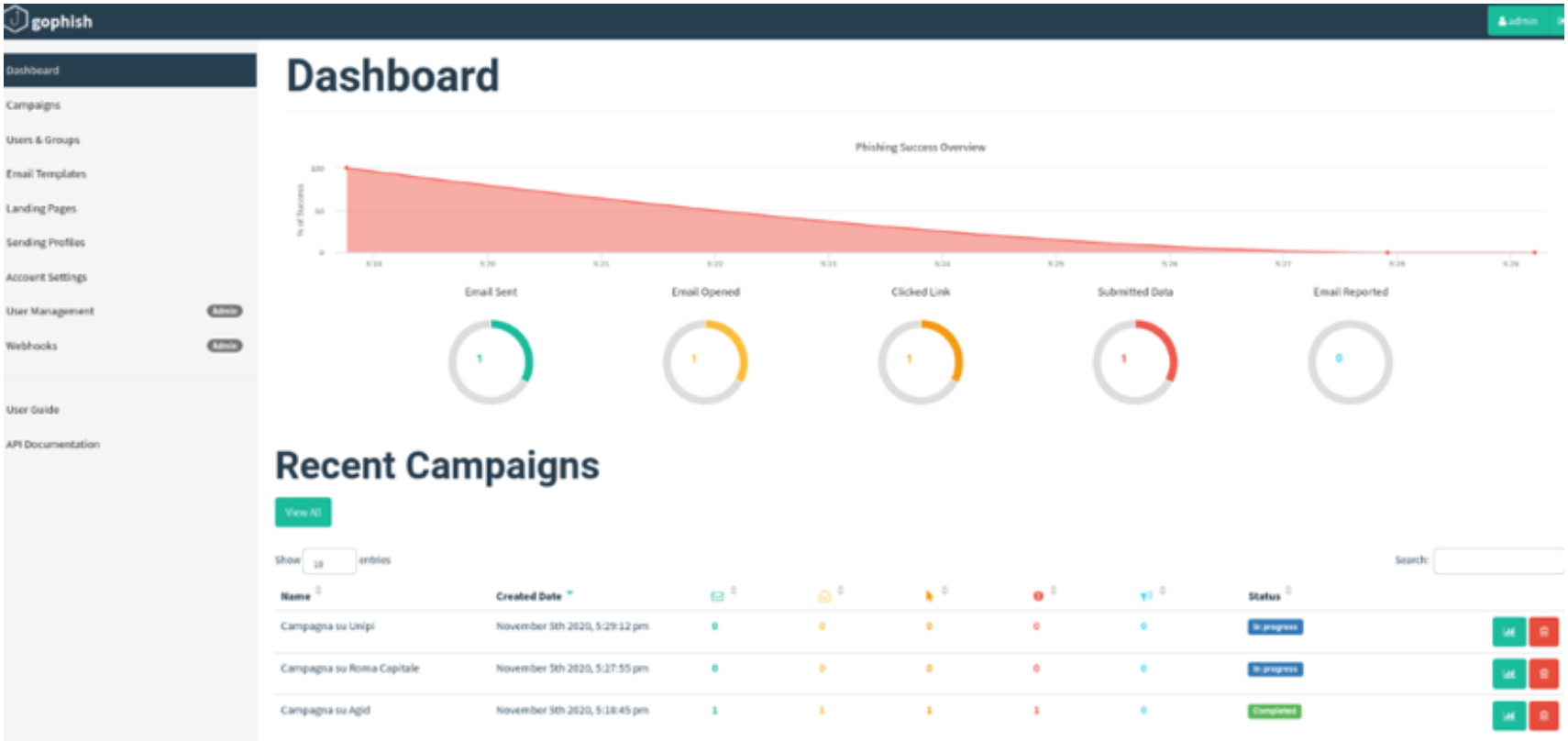
Creare una campagna di phishing con OpenPhish

Processo semplice (5 step)

- **STEP 1**: configurazione di un account mittente (SMTP server)
- **STEP 2**: creazione della phishing mail
- **STEP 3:** creazione della phishing page
- **STEP 4:** avvio della campagna
- **STEP 5**: monitoraggio real-time e report finale

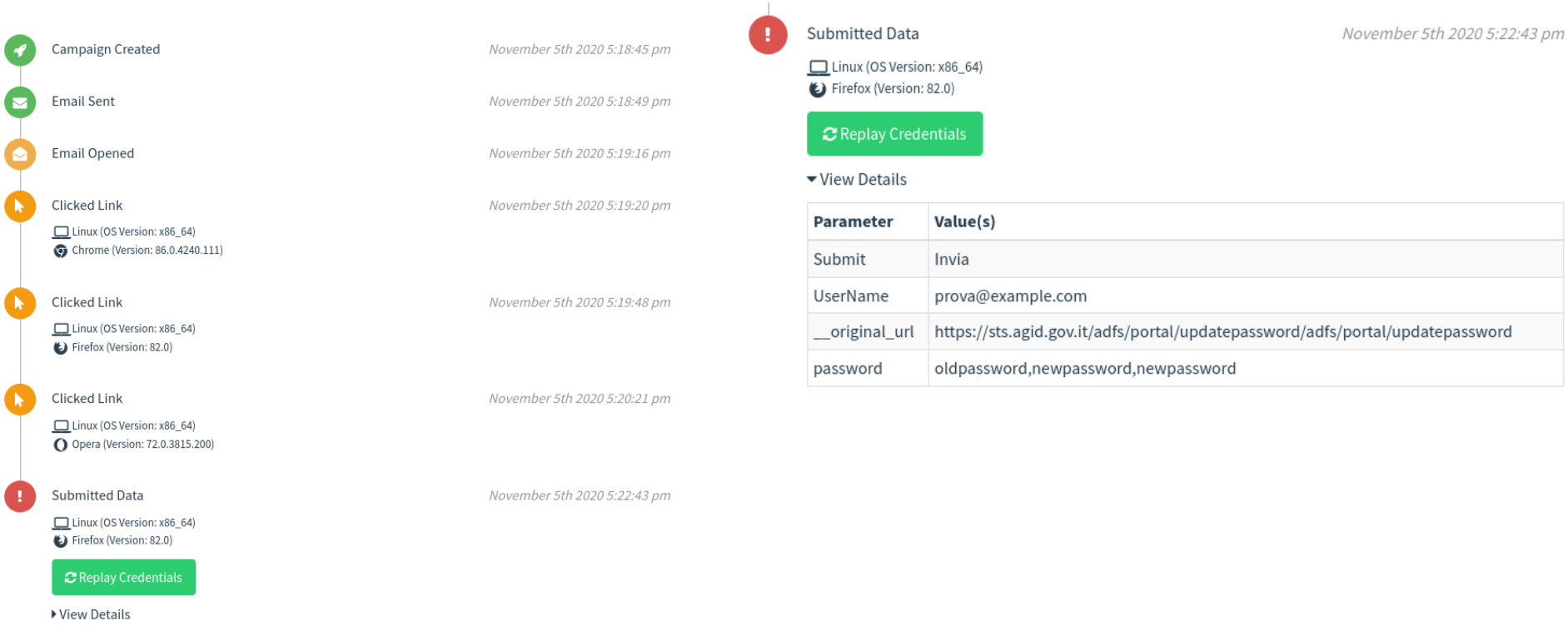
OpenPhish

Monitoraggio della campagna



OpenPhish

Monitoraggio dei risultati



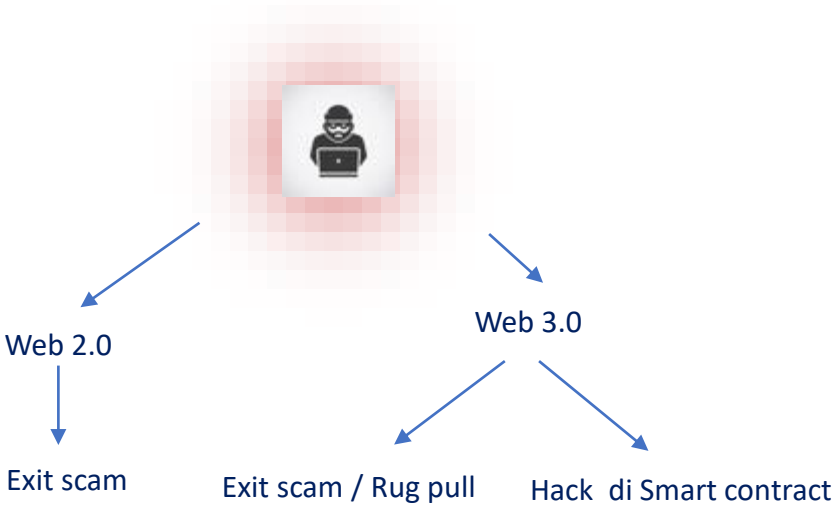
I benefici delle campagne simulate all'interno delle organizzazioni

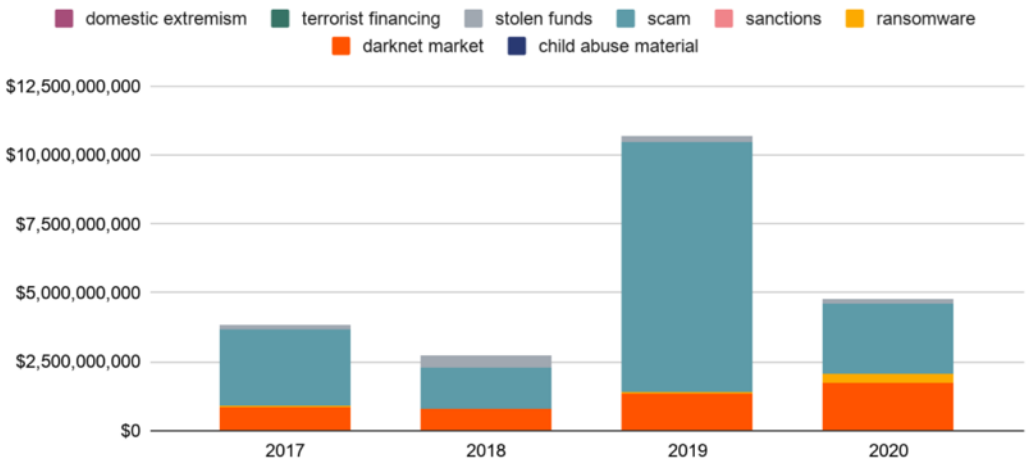
Maggiore consapevolezza dei dipendenti sui rischi cyber legati al phishing

Riduzione dei costi: le PA possono condurre questi test in totale autonomia senza ricorrere a costosi servizi esterni

Formazione mirata: il tool tiene traccia di tutta l'attività effettuata dai dipendenti (lettura mail, apertura della phishing page ecc). Questo potrebbe quindi consentire di definire quali utenti formare e a che livello.

Scam, hack nel mondo delle criptovalute



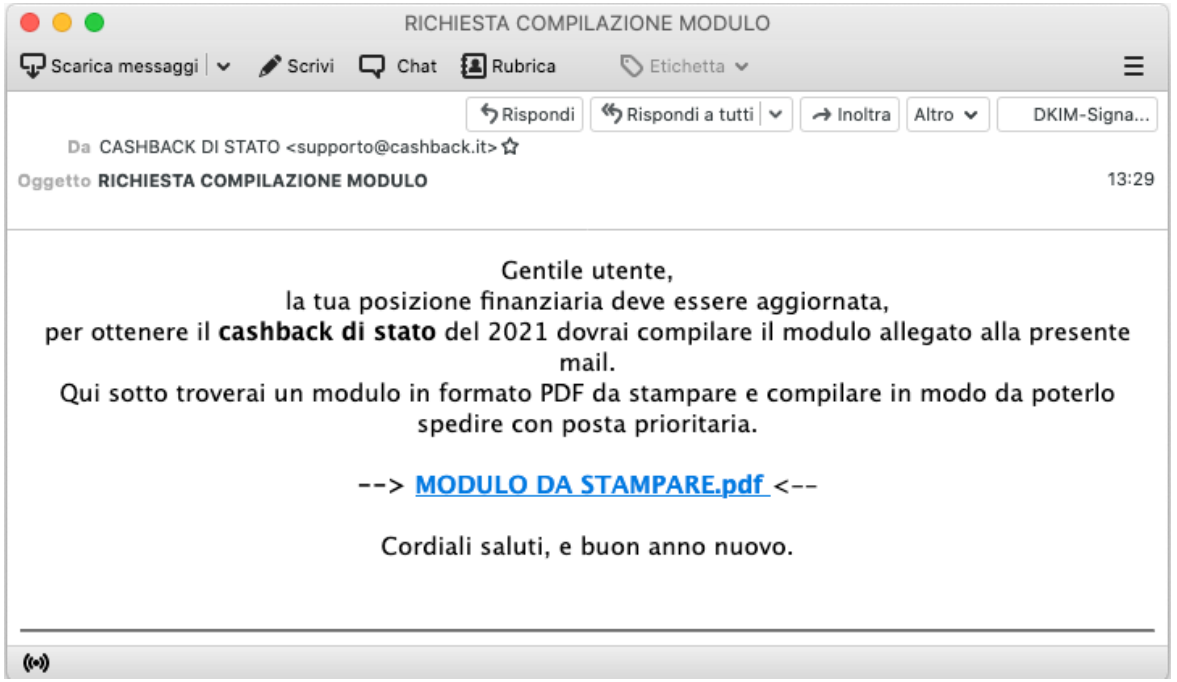


Rif. https://cert-agid.gov.it/news/scam-hack-e-scenari-reali-nel-mondo-delle-criptovalute/

Alcune delle campagne rilevate (1/2)

05/01/2021 - Falsa comunicazione Cashback di Stato veicola malware

- Mail fraudolenta con **allegato pdf**
- In realtà il file non era un pdf ma un **eseguibile scritto in Visual Basic** 6 con doppia estensione (.exe.pdf)
- Il malware utilizzata un **server FTP** su Altervista per lo scambio di informazione con l'attaccante
- Oltre alla persistenza, il malware copia la **home dell'utente** e scarica un **keylogger**
- Molte evidenze fanno pensare che l'autore sia un hacker **italiano non professionista**



https://cert-agid.gov.it/news/malware/falsa-comunicazione-cashback-di-stato-veicola-malware/

Alcune delle campagne rilevate (2/2)

14/04/2021 - Pericolosa campagna Flu bot veicolata anche in Italia via SMS

- Malware già diffuso in Spagna, Germania, Ungheria, recentemente ha iniziato a colpire pure l'Italia
- Sfruttato il tema «spedizioni», l'utente viene spinto a cliccare sul link riportato, dove viene proposto di scaricare e installare un DHL.apk
- L'attacco non sfrutta le vulnerabilità di Android ma la ben nota tecnica del servizio di «Accessibilità» che dovrà essere abilitata dalla vittima
- Tra le azioni principali abbiamo quella di visualizzare una finta pagina (Activity) di verifica Google Play Protect che richiede l'inserimento delle carte di credito e pagine di phishing di Gmail, Whatsapp e simili.
- L'applicazione è in grado di **inviare SMS, recuperare i codici 2FA, disinstallare app, aprire pagine web arbitrarie** ed **eseguire codici USSD.**

https://cert-agid.gov.it/news/campagna-flubot-veicolata-anche-in-italia-via-sms-prende-di-mira-i-dispositivi-android/

Android è sicuro?

- Android ha una **quota di mercato dell'85**% a livello globale → maggiore diffusione = più attacchi
  - Ma più diffusione non significa più vulnerabile o meno sicuro, anzi…
- Android ha **meccanismi di sicurezza forti anche più di iOS**
  - vedi ricerca Gartner *Mobile OS and Device Security: A comparison of Platforms* del 2019 (1) e nostro PDF tecnico su SELinux in Android (2)
- Android offre anche una serie di **vantaggi chiave per gli utenti aziendali** che non sono disponibili con altre opzioni OS
  - **open source**, quindi può essere customizzato per un utilizzo enterprise
  - **consente di adeguare la sicurezza alle policy aziendali**
  - supportare una **vasta gamma di casi d'uso specifici**:
    - maggiore **isolamento delle app** dal sistema operativo
    - **limitazione delle app installabili**
    - **limitazione dei dati** accessibili dalle app
    - limitazione della connettività wifi, cloud pubblici, blootooth, gms ecc
    - utilizzo di schermi sensibili al touch con guanti
    - accesso tramite smart card
    - tastiera personalizzata con supporto di vocabolario unico dell'organizzazione
    - supporto di strumento per lettura tag RFID

(1) https://www.gartner.com/en/documents/3913286
(2) https://cert-agid.gov.it/whatisit/selinux-ed-i-meccanismi-di-isolamento-delle-app-in-android/)

Smart working:
il vademecum per lavorare online in sicurezza

AGID | Agenzia per l'Italia Digitale

https://cert-agid.gov.it/news/smart-working-il-vademecum-per-lavorare-online-in-sicurezza/

GRAZIE PER L'ATTENZIONE!

petito@agid.gov.it