AGID | Agenzia per l'Italia Digitale

FormezPA

Social Engineering e Cyber Security Awareness

Michele Petito, AgID

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.

Altre tecniche

Telefono

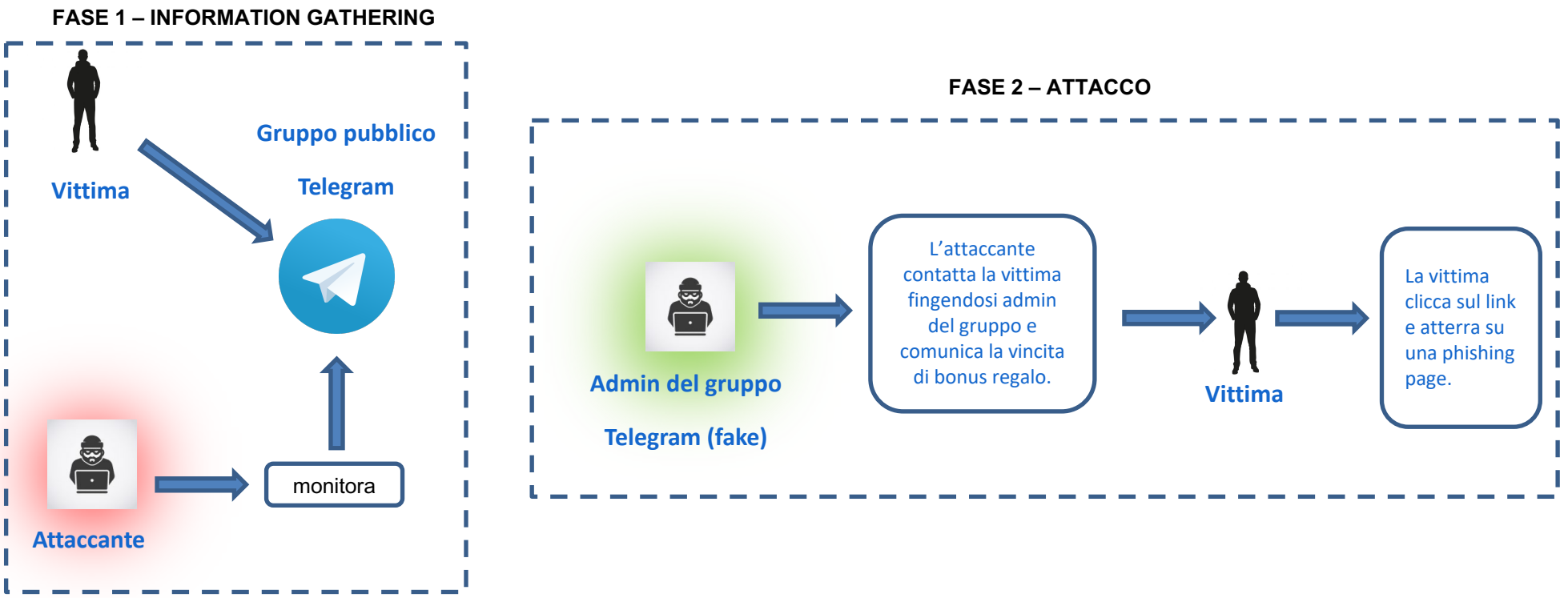
Es. Un finto amministratore di rete contatta il dipendente con la scusa di un problema tecnico e vi richiede dati personali o l'installazione per l'accesso remoto alla vostra macchina

Social

Sms

Es. L'attaccante invia un messaggio di testo contenente un link a una pagina di phishing (**smishing**)

Altre tecniche – By Social



Diffusione del phishing a livello italiano

- Anche il **Rapporto CLUSIT 2020** conferma la tendenza, classificando al terzo posto il "Phishing/Social Engineering", tra le tipologie di attacco
- Tale categoria cresce del **+81,9%** rispetto al 2018 e rappresenta il 17% del totale
- Una quota crescente di questi attacchi basati su Phishing si riferisce a **"BEC scams"** che infliggono danni economici sempre maggiori alle loro vittime .

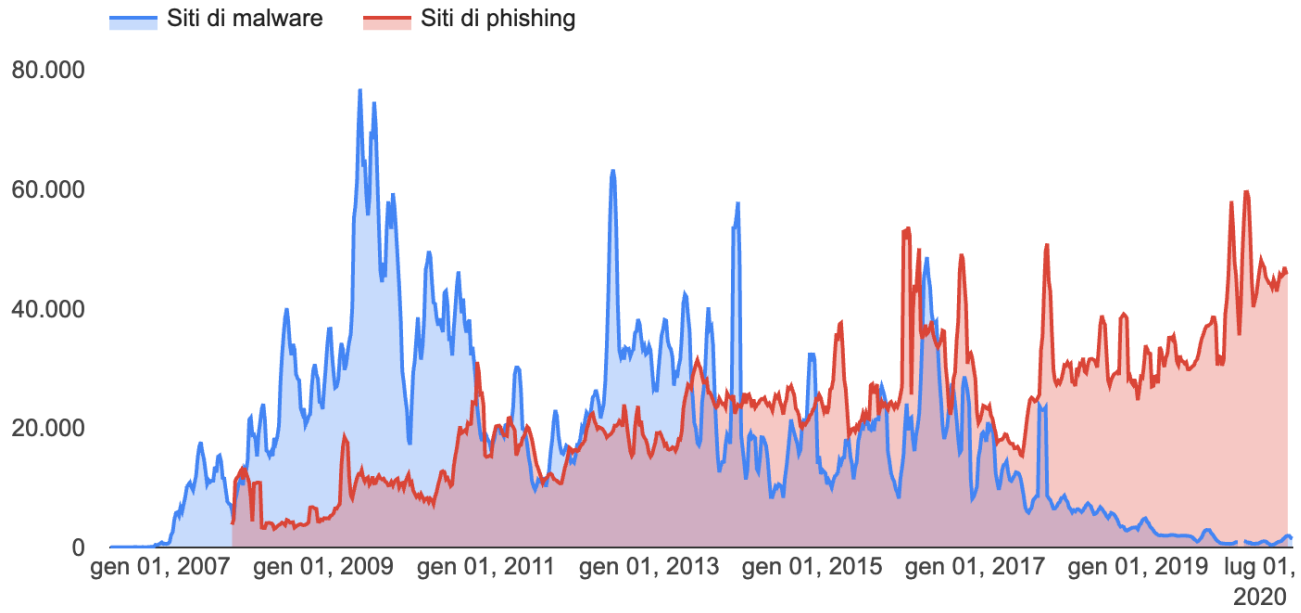
TIPOLOGIA TECNICHE DI ATTACCO	2014	2015	2016	2017	2018	2019	2019 su 2018	Trend
Malware	127	106	229	446	585	730	24.8%	↑
Unknown	199	232	338	277	408	317	-22.3%	↓
Known Vulnerabilities / Misconfig.	195	184	136	127	177	126	-28.8%	↓
Phishing / Social Engineering	4	6	76	102	160	291	81.9%	↑
Multiple Techniques / APT	60	104	59	63	98	65	-33.7%	↓
Account Cracking	86	91	46	52	56	86	53.6%	↑
DDoS	81	101	115	38	38	23	-39.5%	↓
0-day	8	3	13	12	20	30	50.0%	↑
Phone Hacking	3	1	3	3	9	1	-88.9%	↓
SQL Injection	110	184	35	7	1	1	0.0%	-
TOTALE	873	1012	1050	1127	1552	1670		

Fonte Rapporto CLUSIT 2020

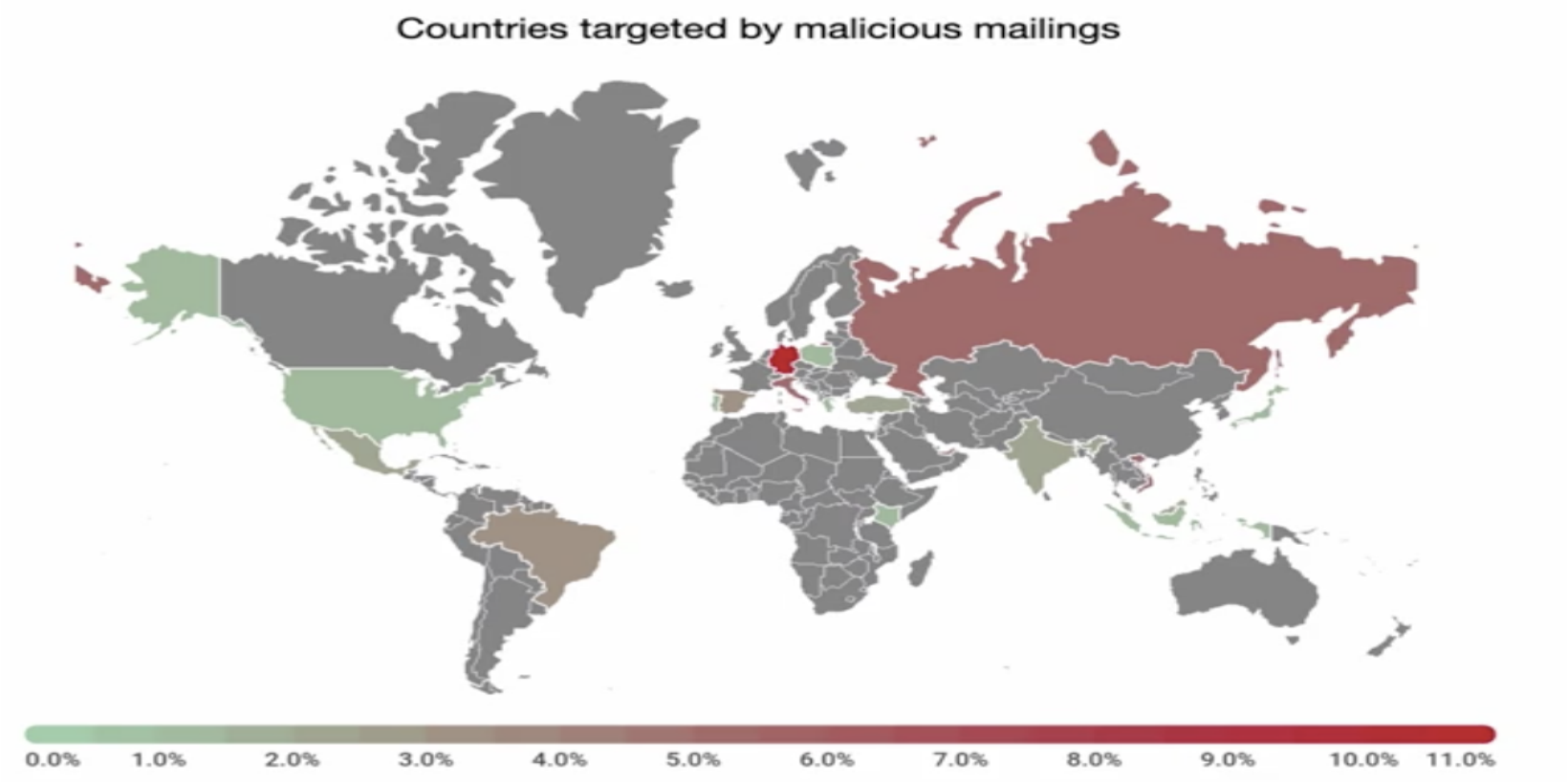
Phishing trend

https://transparencyreport.google.com/safe-browsing/overview

Inizio 21/5/2006 Fine 22/11/2020

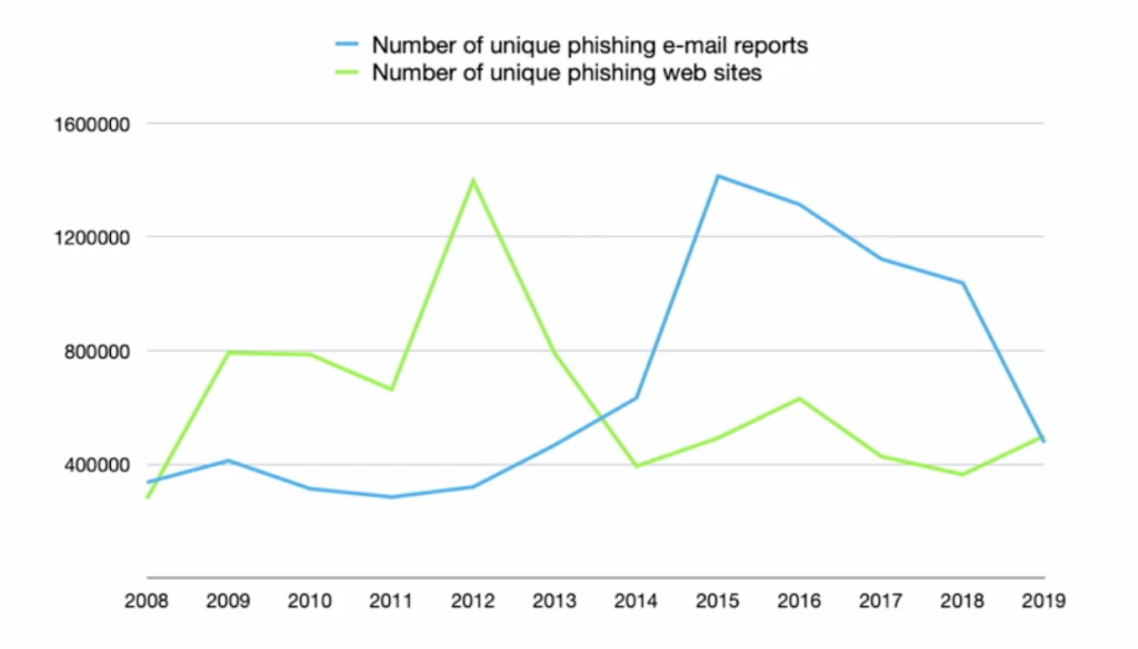


Diffusione del phishing



Fonte Securelist

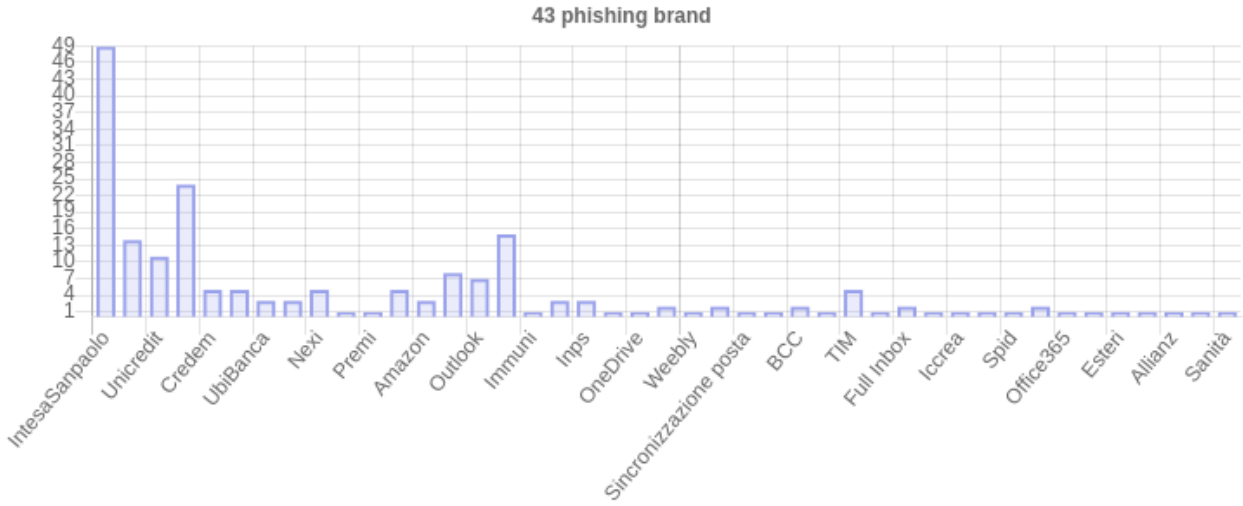
Diffusione del phishing a livello internazionale



Fonte anti-phishing working group https://apwg.org

Phishing trend - ultimo quadrimestre 2020

- Rilevate **200 campagne** utilizzate per veicolare phishing, di cui **19 smishing**
- **43 brand** coinvolti tra cui:
  - 49 **Intesa San Paolo**
  - 24 **Poste**
  - 15 **Aruba**
  - 14 **BNL**
  - 11 **Unicredit**
- **81%** delle campagne è stato a tema **banking** e **pagamenti**



Fonte Cert-AgID: https://cert-agid.gov.it/news/riepilogo-delle-campagne-malevole-che-hanno-interessato-litalia-nellultimo-quadrimestre-2020/

7-Day Phishing Trend (12/01/21 - 19/01/21)

- **Rilevazione settimanale di OpenPhish**. Viene aggiornata ogni ora.
- I **brand** più colpiti:
  - **Office**
  - **Facebook**
  - **Lyloyds**
  - **Paypal**
  - **Office365**
- Settori più coinvolti: **email, social, finanziario, e-commerce.**

8,513,715	62,191	263
URLs Processed	Phishing Campaigns	Brands Targeted

Rank	Targeted Brand	Industry	Phishing Domains	Phishing URLs
1	Outlook	Email Provider	648	992
2	Facebook, Inc.	Social Networking	593	687
3	Lloyds TSB Group	Financial	265	380
4	PayPal Inc.	Payment Service	216	462
5	Office365	Online/Cloud Service	203	238
6	Amazon.com Inc.	e-Commerce	164	188
7	Halifax Bank of Scotland Plc	Financial	145	211
8	Tencent	Online/Cloud Service	107	111
9	Instagram	Social Networking	105	133
10	WhatsApp	Social Networking	87	98
11	Microsoft OneDrive	Online/Cloud Service	84	92
12	Adobe Inc.	Online/Cloud Service	72	133

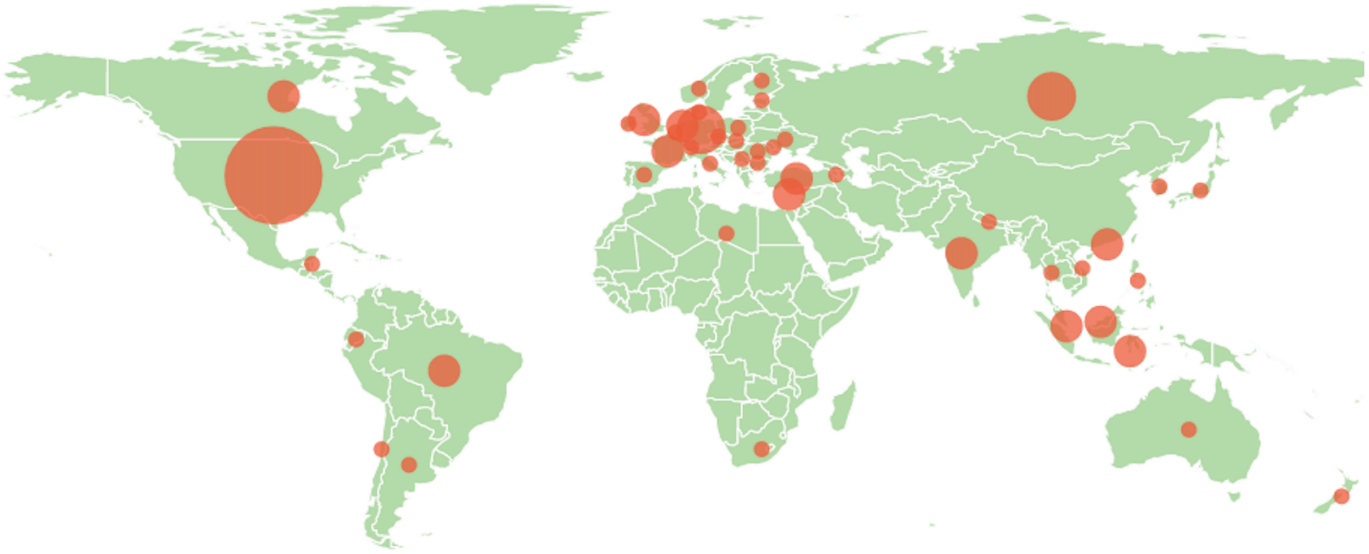
Fonte OpenPhish: https://openphish.com/

7-Day Phishing Trend (12/01/21 - 19/01/21)

13	▲ +1	Netflix Inc.	Online/Cloud Service	70	82
14	▼ -1	HSBC Bank	Financial	70	93
15		DHL Airways, Inc.	Logistics & Couriers	65	243
16		Three UK	Telecommunications	63	69
17		HM Revenue & Customs	Government	60	60
18		eBay Inc.	e-Commerce	59	95
19		Credit Agricole S.A.	Financial	56	87
20		Chase Personal Banking	Financial	55	175
21		Orange	Telecommunications	54	84
22		EE Limited	Telecommunications	51	66
23		Intesa Sanpaolo	Financial	45	45
24		O2 UK	Telecommunications	42	60
25		Apple Inc.	Online/Cloud Service	42	95

Fonte OpenPhish: https://openphish.com/

Global Phishing Activity (agg. ogni 5 min)



Top 10 ASNs

AS22612 Namecheap,...	22.2%
AS46606 Unified Layer	8.6%
AS13335 Cloudflare, I...	7.0%
AS32244 Liquid Web, ...	4.9%
AS15169 Google LLC	3.1%
AS27647 Weebly, Inc.	2.9%
AS26496 GoDaddy.co...	2.4%
AS16509 Amazon.co...	2.2%
AS51167 Contabo Gm...	2.2%
AS54113 Fastly	2.2%

Fonte OpenPhish: https://openphish.com/phishing_activity.html

Pagine di phishing italiane del 4/12/20

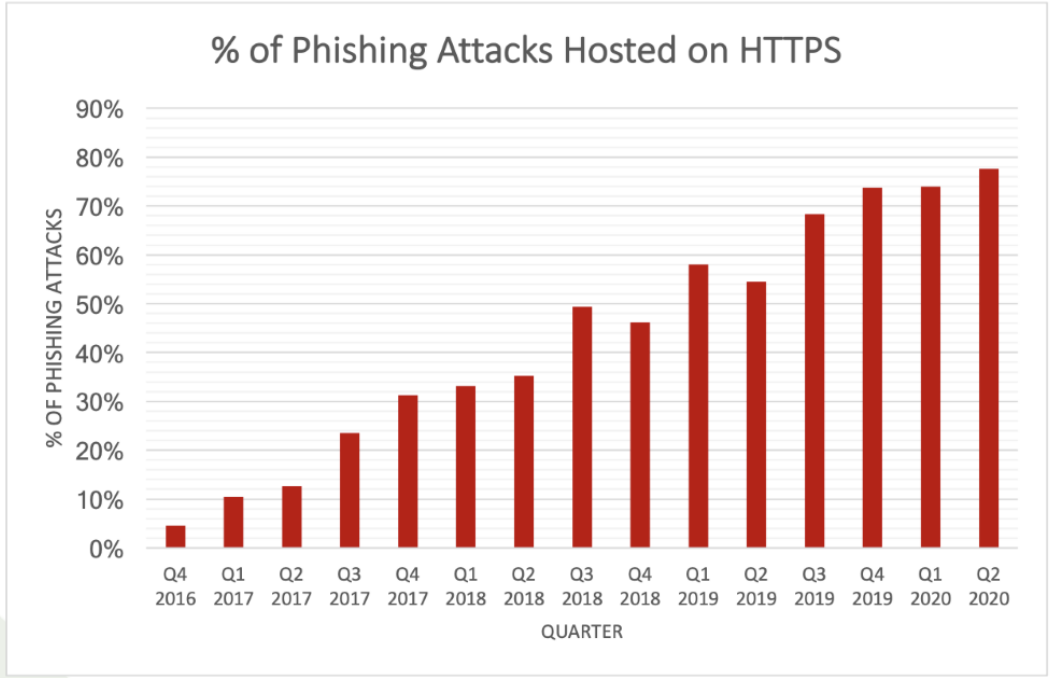
https://aggiorna-dati-conto.com/index
https://aggiornamentocertificazionedati.com/info/
https://aggiornamentosicurezza-web.com/
https://certificazionedati-aggiornata.com/info/
https://clientiverifica.cloud/
https://controllodati-anagrafici.com/
https://convalida-dati-isp.com/index
https://Informa-sicurezza-app.com/
https://Informazionesicurezza-online.com/
https://normativacertificata-dati.com/
https://normativa-europea.net/
https://portaleintesasp.com/index
https://portale-intesasp.com/index
https://portalesanpaolo.com/index
https://posterevisione.net/
https://restrizione-dati.com/index
https://sicurezza-bnl.org/accedi/

http://accesso-contogisp.com/index.html
http://aggiorna-app-Isp.com/gbhe8104kibr/
http://aggiornafamiglieepersone.info/tkil7604vtne
http://aggiorna-profilo-web.com/
http://aggiornapsd2-web.com/
http://assemblasicurezzaIntesa.com/
http://assistenzaappweb.com/
http://conto-controllo.com/
http://informazione-conto.com/
http://normativesicurezzeweb.com/
http://notifiche-clienti.com/
http://nuovi-dati-info.online/
http://obblighiaggiornamenti.com/
http://poste-conto.com/
http://profilobnl.online/
http://profilo-psd2-online.com/
http://riattiva-utenza-app.com/kqzu4972gvfd/
http://rinnova-loginposte.net/
http://ripristinabnl.online/

http://sicurezzaweb-Informazione.com/
http://supporto-dati.com/
https://www.info-sicuro.com/
https://www.nuovapp-psd2.info/

Attacchi phishing ospitati su https

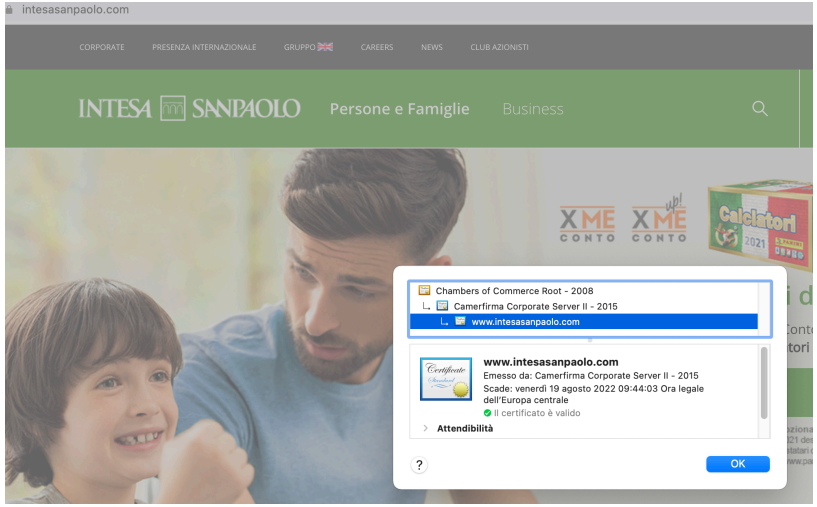
- Secondo uno studio condotto dalla società **PhishLabs**, il numero di siti di phishing che utilizzano TLS continua ad aumentare
- Il **36,2%** di tutti i **certificati** rilevati nei domini di phishing sono stati emessi dall'autorità di certificazione **Let's Encrypt** che li fornisce gratuitamente.

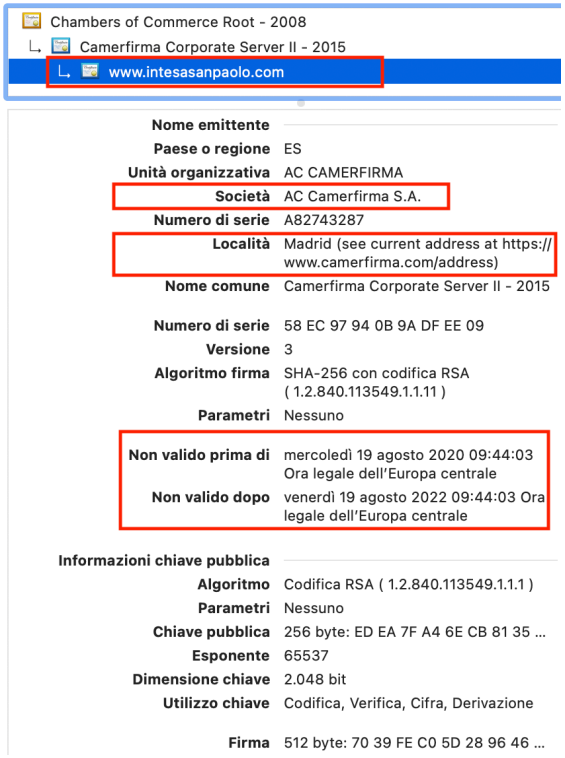


Fonte Phishlabs

Verifica del certificato

- Es. di dominio da verificare: **intesasanpaolo.com**
- Si clicca sul lucchetto e si controlla la **società che ha emesso il certificato** e la **validità**





Esempio di phishing – 1.1

Tema «Banking»

Da BNL <bnl@sicurezza.messagges.com>
Oggetto **Urgente: Conferma dati RGPD ed informazioni sulla tua privacy**
Rispondi-a noreplay@bnl.clienti.it
A cert-pa@cert-pa.it

Rispondi | Rispondi a tutti | Inoltra | Altro
30/01/20, 13:56

BNL
GRUPPO BNP PARIBAS

Gentile Cliente BNL,

Durante il 2018 e il 2019, abbiamo lavorato costantemente per aggiornare i nostri processi e la nostra sicurezza in modo da essere conformi al Regolamento generale sulla protezione dei dati (RGPD), la nuova legge europea in materia di protezione dei dati che entrerà in vigore il 1 febbraio 2020. In questo contesto, abbiamo aggiornato la nostra Informativa sulla privacy per dare maggiori informazioni sul modo in cui trattiamo i suoi dati personali.

Ti invitiamo ad accedere è verificare i suoi dati cliente: (https://www.bnl.it/it/verifica-informazioni/conto/id=001827372)

Questi cambiamenti diventeranno effettivi a partire dal 1 febbraio 2020.

Abbiamo migliorato la nostra Informativa sulla privacy in modo che sia più dettagliata e specifica, e permetta di capire facilmente come trattiamo i dati personali.

Inoltre abbiamo aggiunto alcune informazioni su privacy e protezione dei dati sul nostro centro assistenza: (https://www.bnl.it/it/vedi/privacy/id=001827372)

Cordiali Saluti.

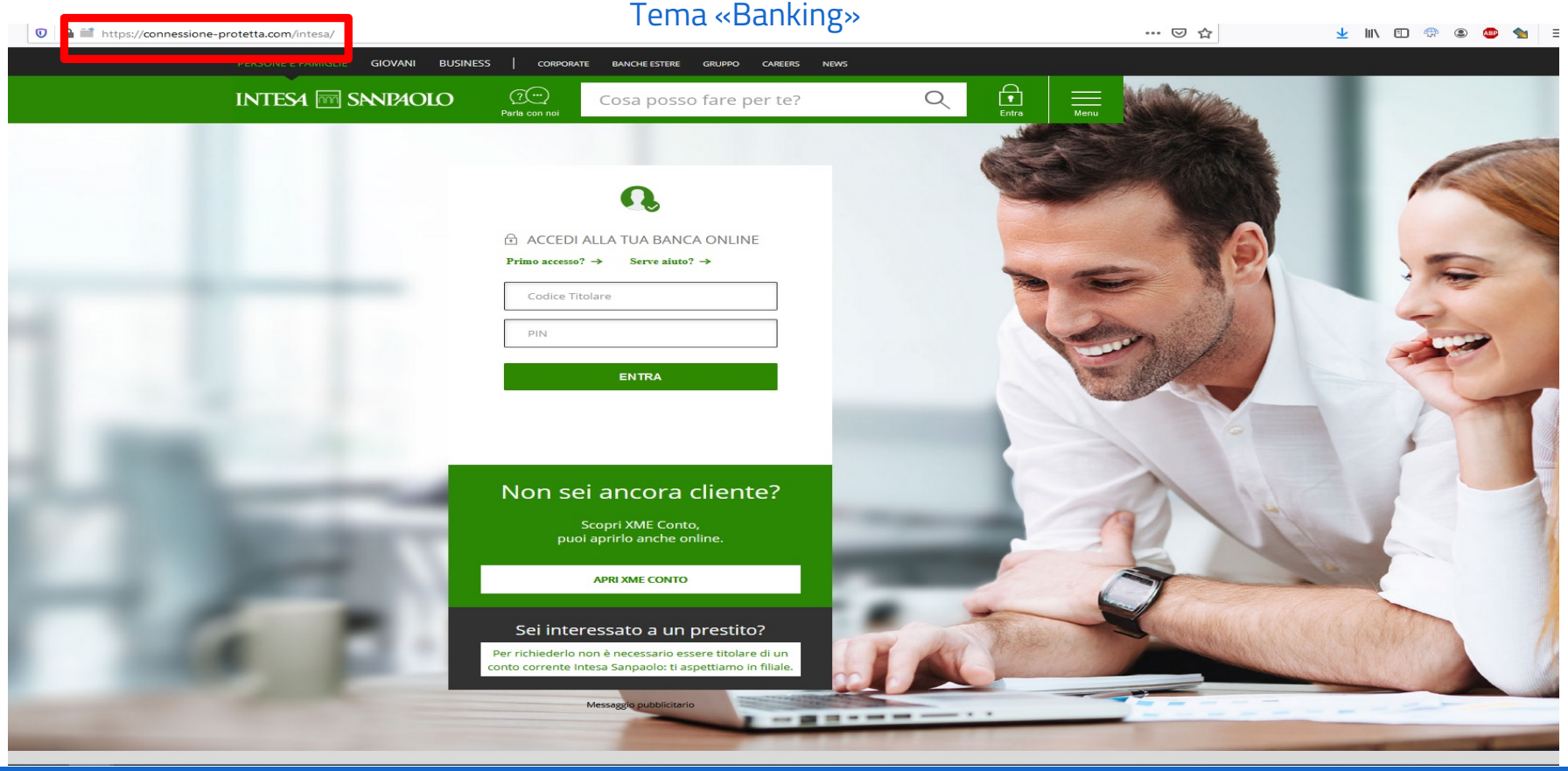
Banca Nazionale del Lavoro SpA - Codice fiscale, Partita IVA e n.di iscrizione nel Reg. Imprese di Roma 09339391006 - Aderente al Fondo interbancario di tutela dei depositi.

Esempio di phishing – 1.2

Tema «Banking»

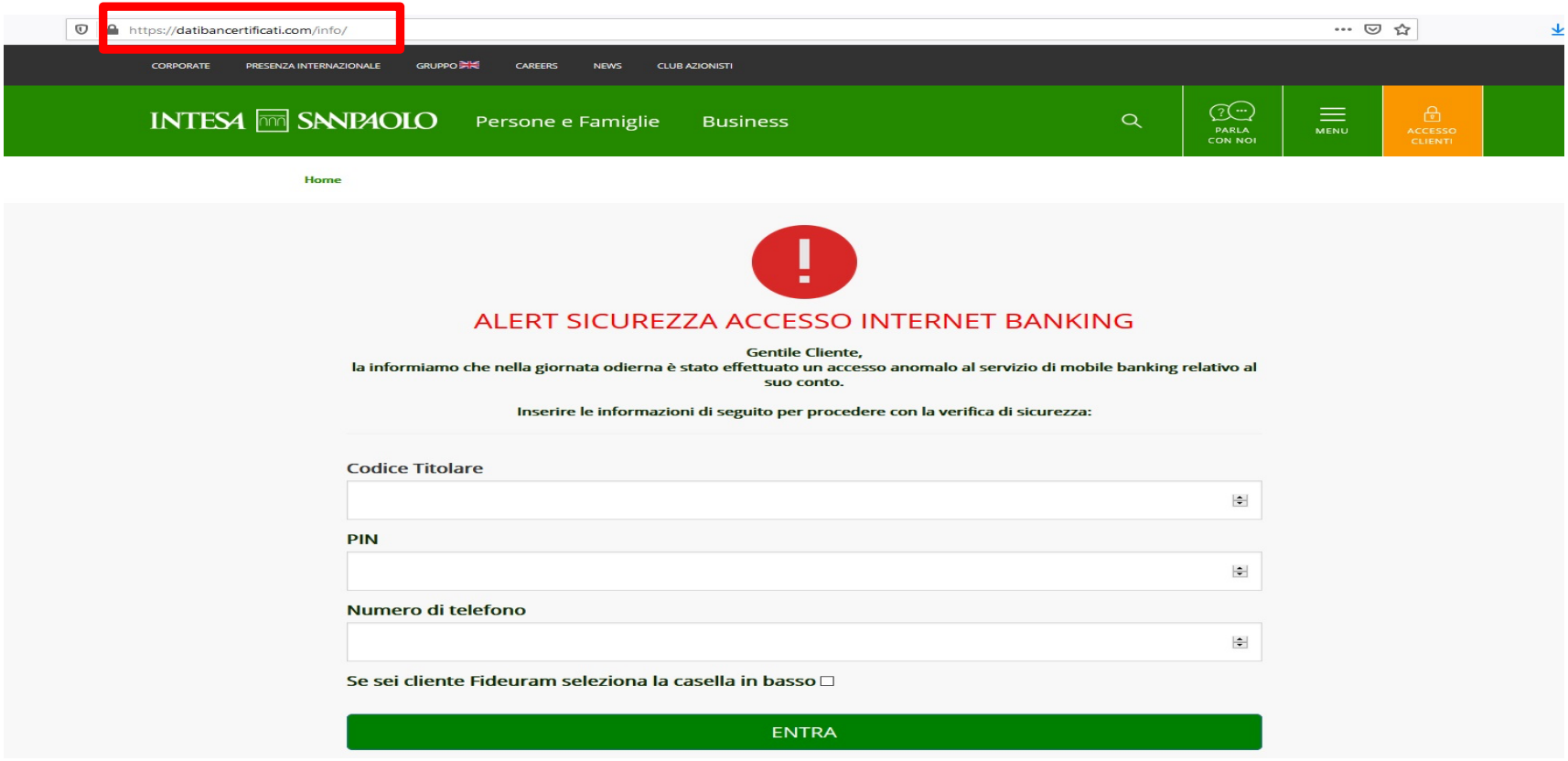
Esempio di phishing – 2

Tema «Banking»



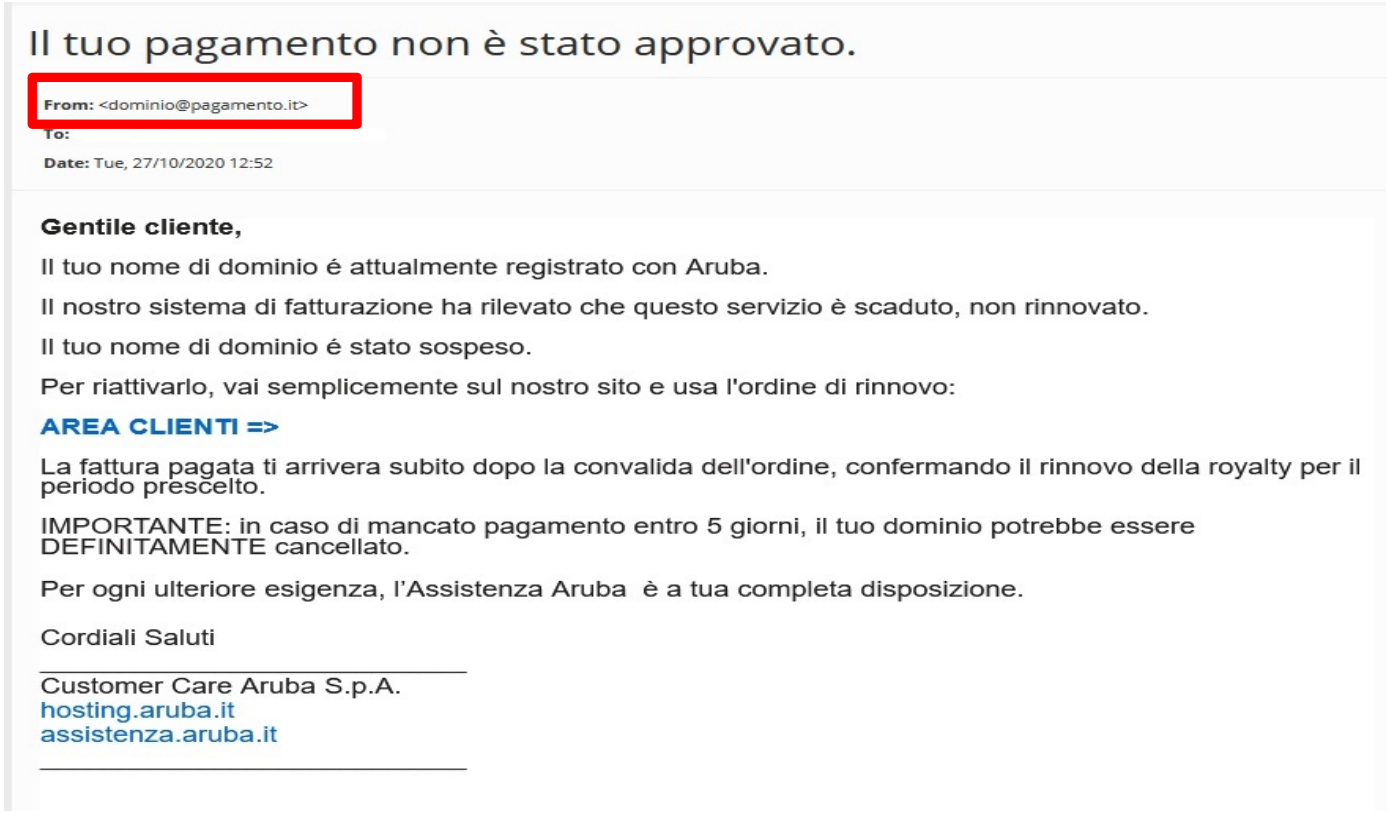
Esempio di phishing – 3

Tema «Banking»



Esempio di phishing – 4

Tema «Pagamenti»



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.

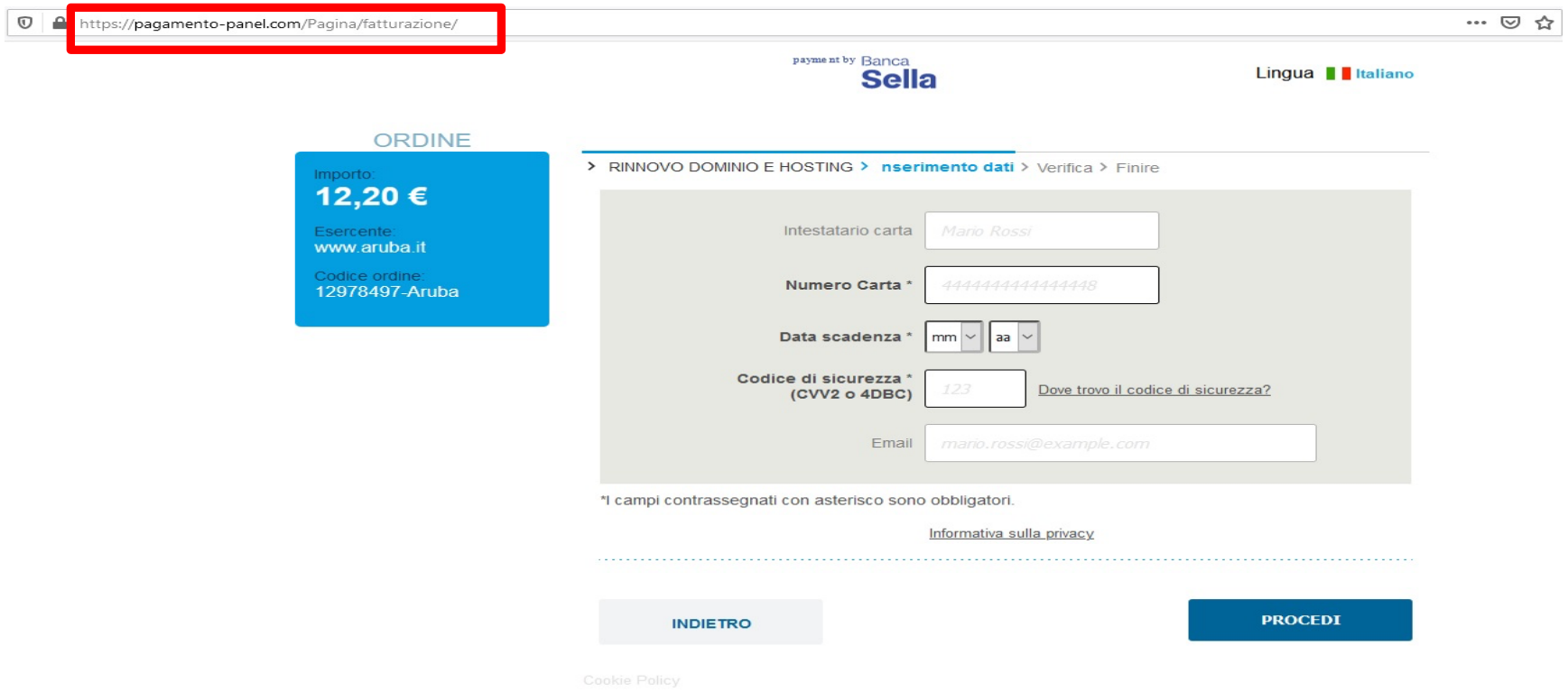
Per ogni ulteriore esigenza, l'Assistenza Aruba è a tua completa disposizione.

Cordiali Saluti

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

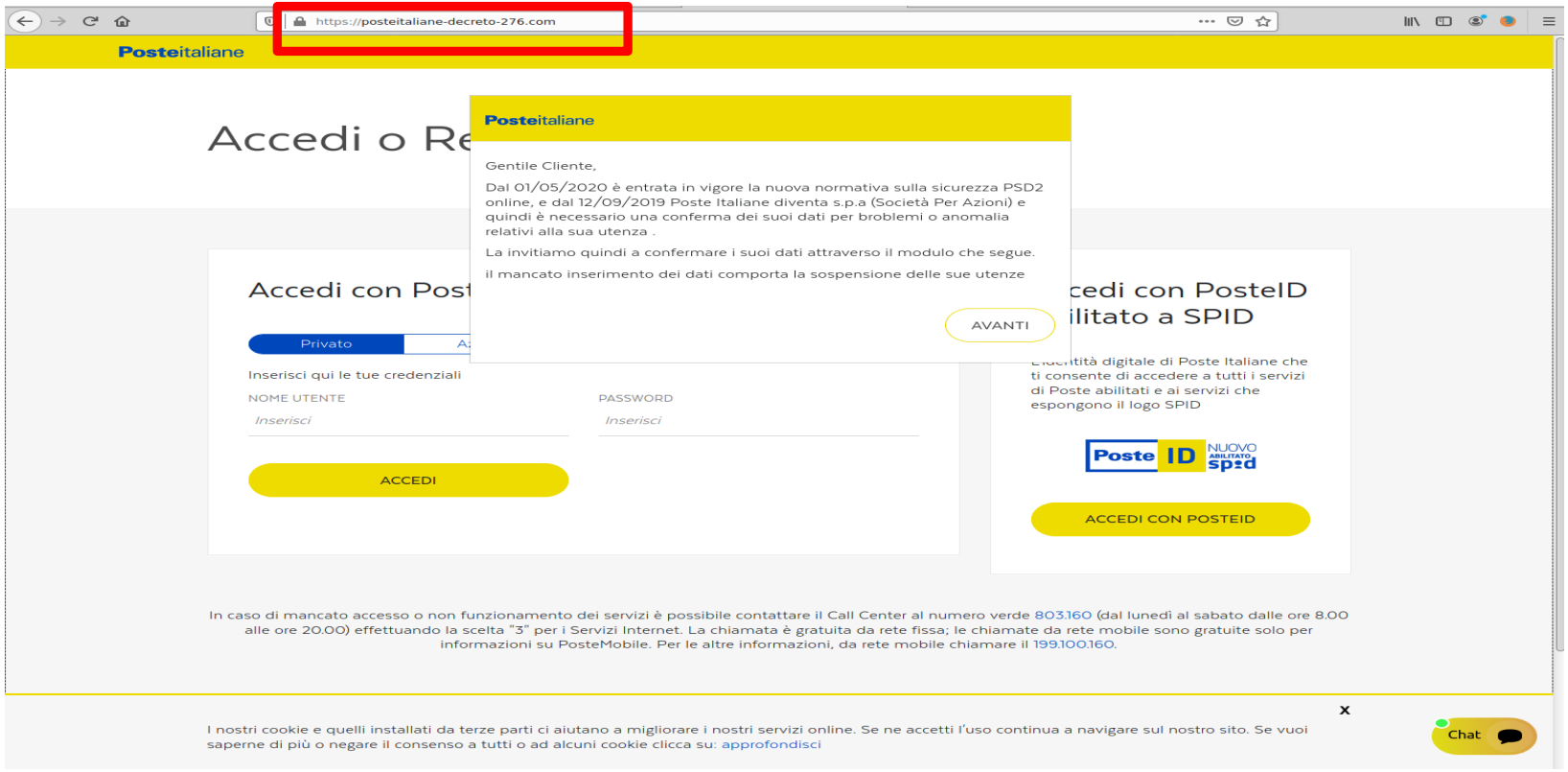
Esempio di phishing – 5

Tema «Pagamenti»



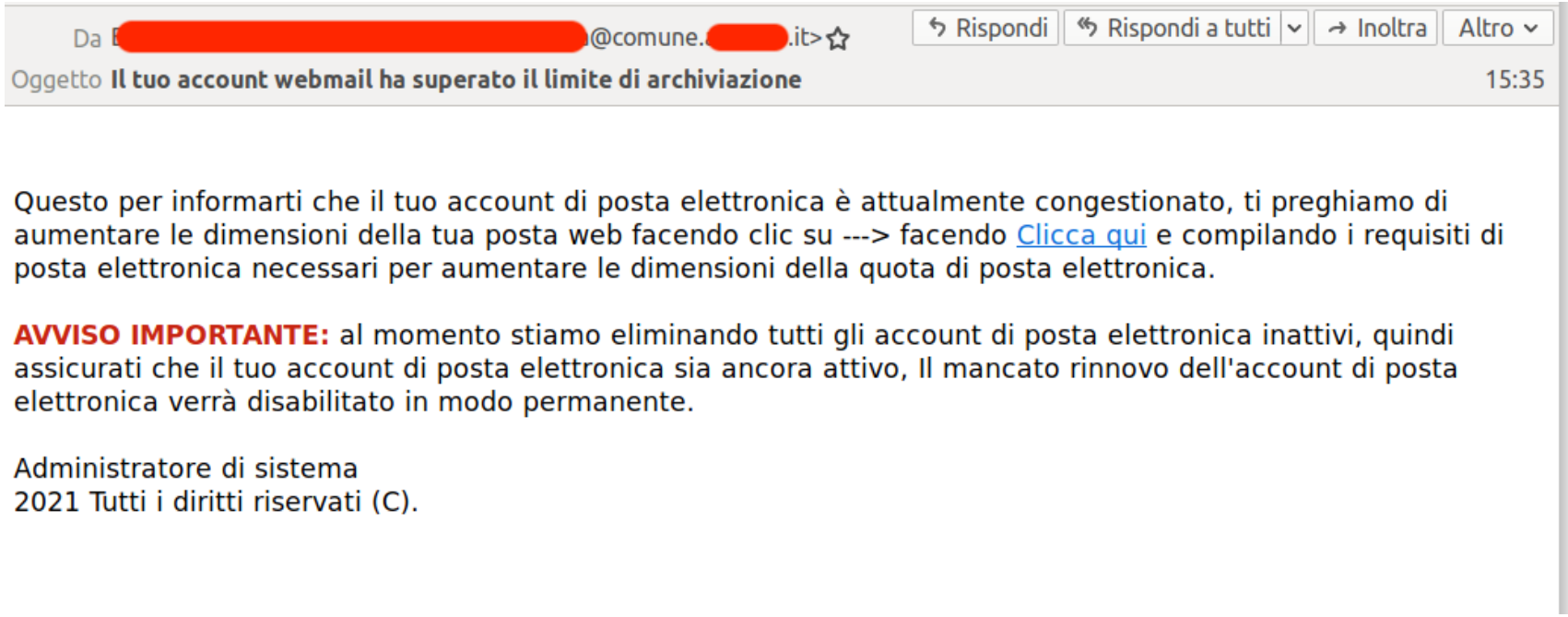
Esempio di phishing – 6

Tema «PSP2»



Esempio di phishing – 7

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 –

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

Esempio di phishing –

Tema «Delivery»

Reale dominio di provenienza

Header

```
Received: from hj0.321.zrami.ml (hj0.321.zrami.ml [159.65.221.182])
    by pecfe8.telecompost.it (Postfix) with ESMTPS id EB9E9C000073
    for <[redacted]>; Mon, 18 Jan 2021 01:19:04 +0100 (CET)
Content-Type: multipart/mixed; boundary="==========0867356116=="
MIME-Version: 1.0
Subject: DHL GST NOTIFICATION FOR INCOMING SHIPMENT ** AWB: 2352366446 Confirm your
 Shipment URGENT
To: Recipients <support@dhl.com>
From: "DHL Customer Support" <support@dhl.com>
Date: Sun, 17 Jan 2021 16:18:52 -0800
Message-Id: <20210118001904.EB9E9C000073@pecfe8.telecompost.it>
X-TransactionId: 21b37a8f-a100-48f3-9439-3a733b9dcb8f
X-PM-Type: peo
```

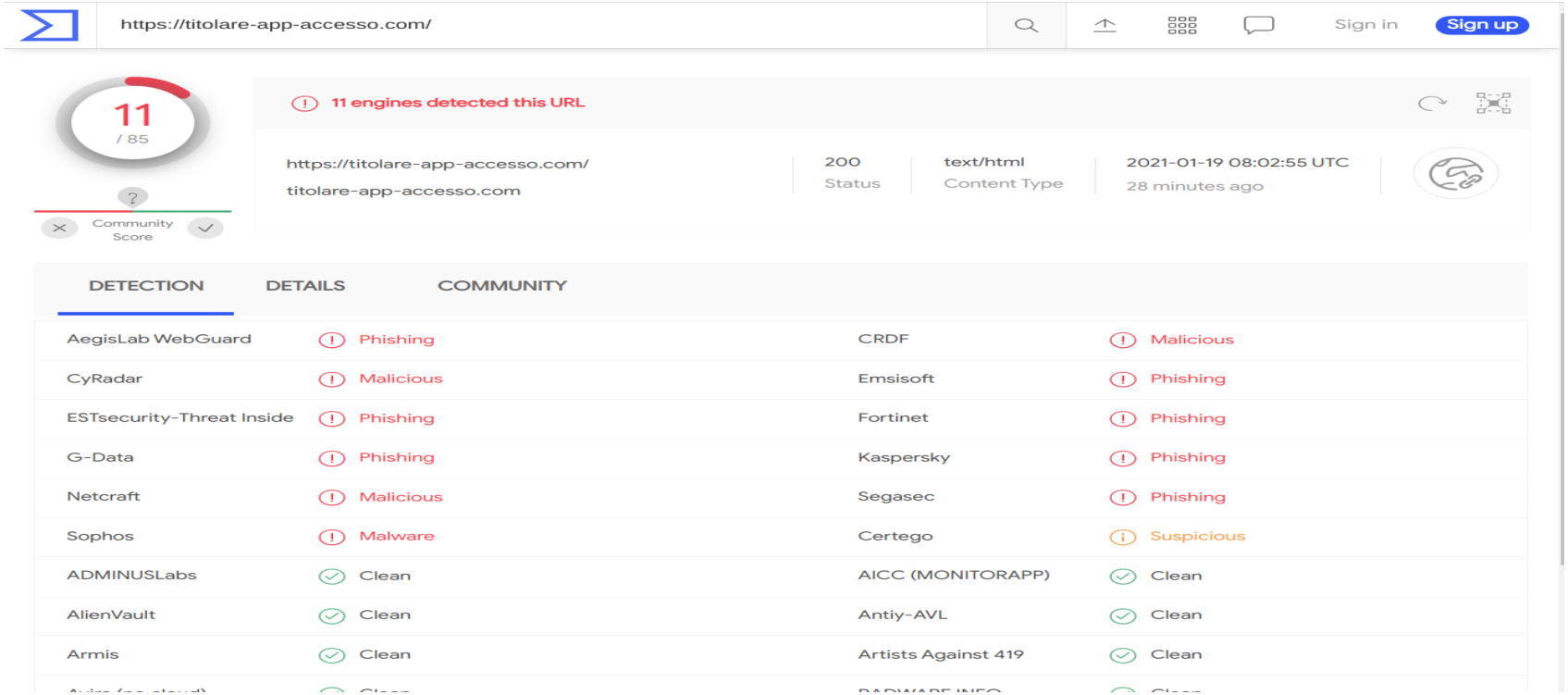
Best practices

- **Non aprire link / allegati contenuti** contenuti in e-mail provenienti da mittenti sconosciuti
- **Non fornire informazioni sensibili** a chi vi contatta di persona, via mail o social

Porre attenzione a:

- A **domini non correlati** con le aziende che inviano messaggi
- **Errori ortografici**
- Sequenza di **simboli random** nell'indirizzo internet
- Simboli provenienti da altre lingue simili all'alfabeto latino

Verifica di link e allegati



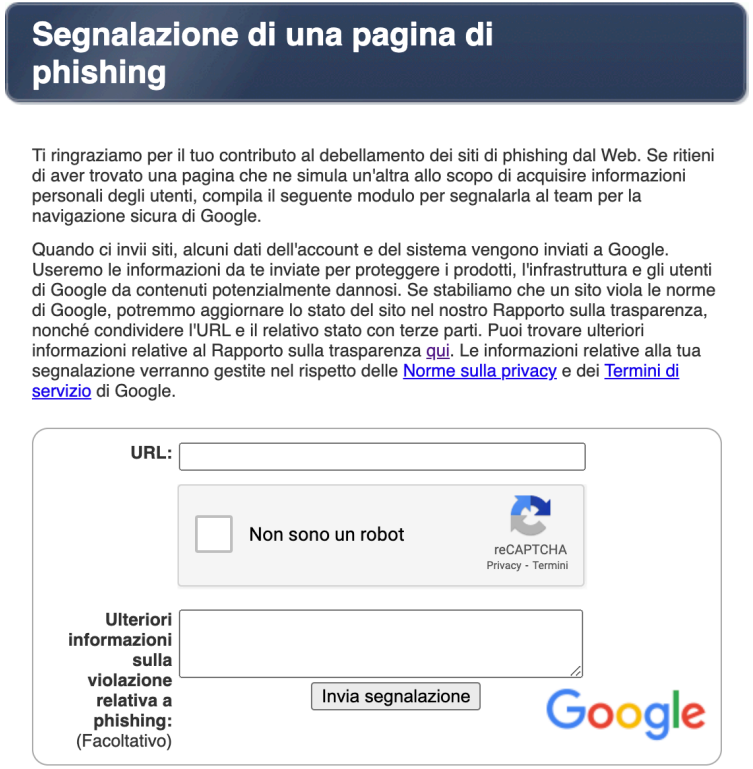
Fonte VirusTotal: https://virustotal.com/

Come segnalare il phishing?

- La collaborazione degli utenti è fondamentale per combattere il phishing e bloccare le URL più velocemente. Esistono diversi canali per segnalare questi siti fraudolenti :
  - **Google** - https://safebrowsing.google.com/
  - **Phishtank** - https://www.phishtank.com/
  - **Netcraft** - https://www.phishtank.com/ -
  - **Cert-AgID** – Inviare una mail a info@cert-agid.gov.it

Google surf browsing

https://safebrowsing.google.com/safebrowsing/report_phish



Segnalazione di una pagina di phishing

Ti ringraziamo per il tuo contributo al debellamento dei siti di phishing dal Web. Se ritieni di aver trovato una pagina che ne simula un'altra allo scopo di acquisire informazioni personali degli utenti, compila il seguente modulo per segnalarla al team per la navigazione sicura di Google.

Quando ci invii siti, alcuni dati dell'account e del sistema vengono inviati a Google. Useremo le informazioni da te inviate per proteggere i prodotti, l'infrastruttura e gli utenti di Google da contenuti potenzialmente dannosi. Se stabiliamo che un sito viola le norme di Google, potremmo aggiornare lo stato del sito nel nostro Rapporto sulla trasparenza, nonché condividere l'URL e il relativo stato con terze parti. Puoi trovare ulteriori informazioni relative al Rapporto sulla trasparenza qui. Le informazioni relative alla tua segnalazione verranno gestite nel rispetto delle Norme sulla privacy e dei Termini di servizio di Google.

URL:

Non sono un robot

reCAPTCHA
Privacy - Termini

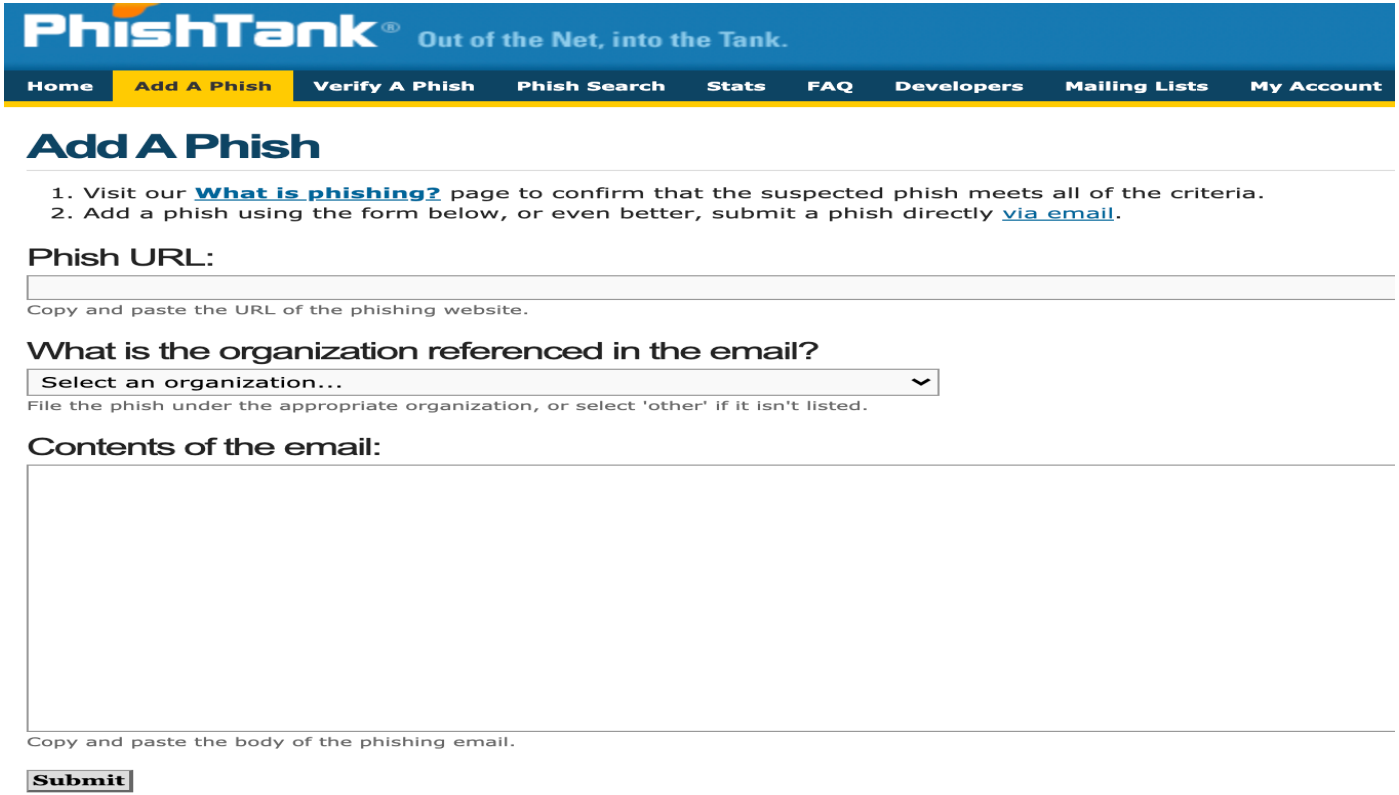
Ulteriori informazioni sulla violazione relativa a phishing: (Facoltativo)

Invia segnalazione

Google

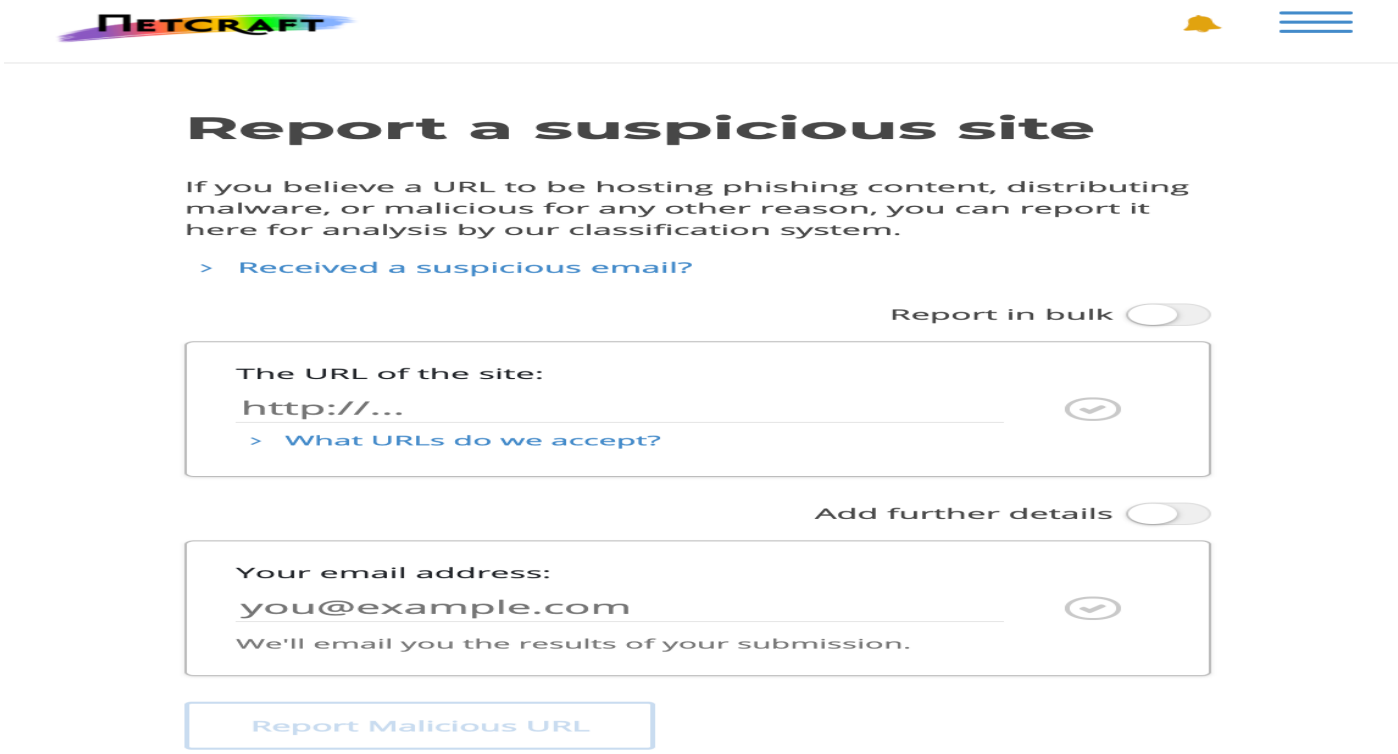
Phishtank

https://www.phishtank.com/

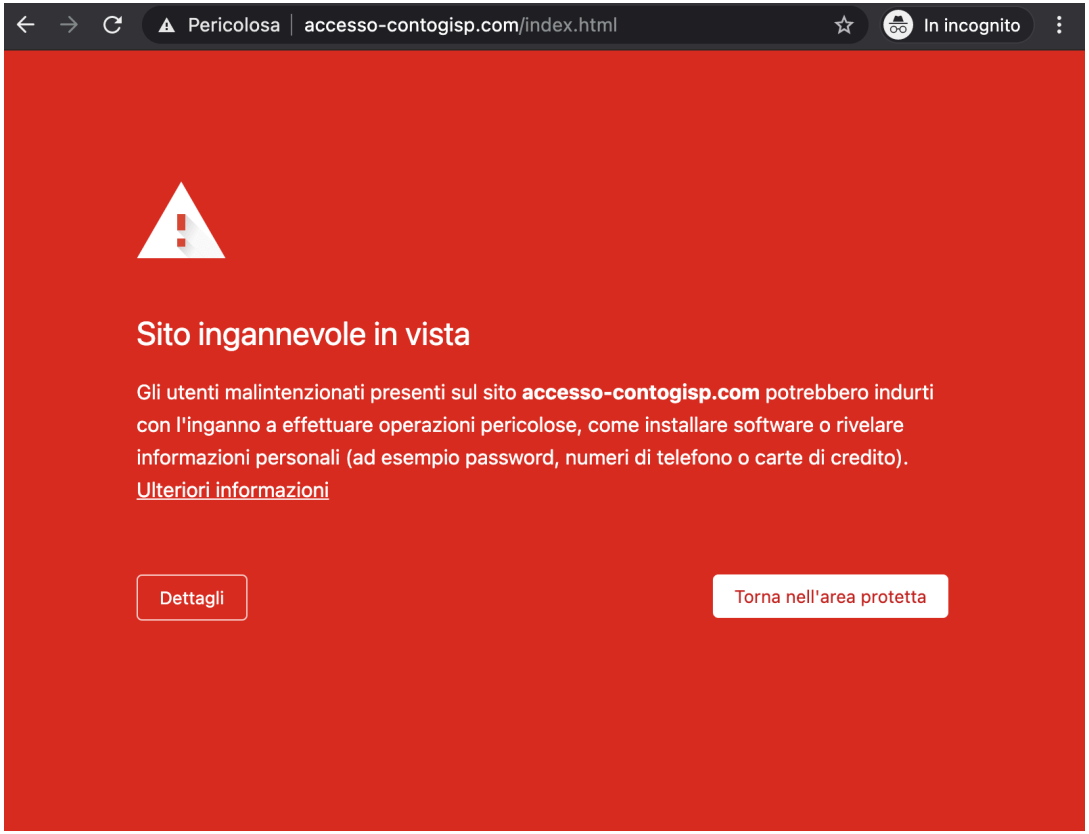


Netcraft

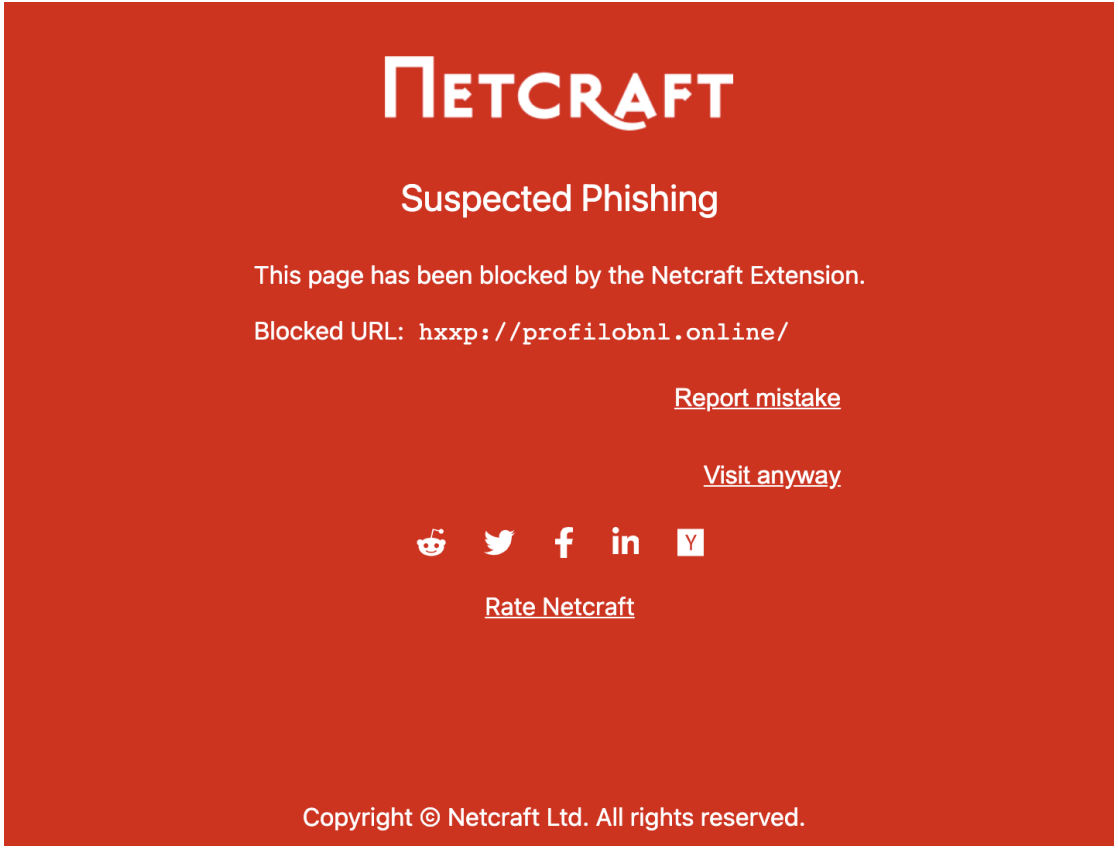
https://report.netcraft.com/report



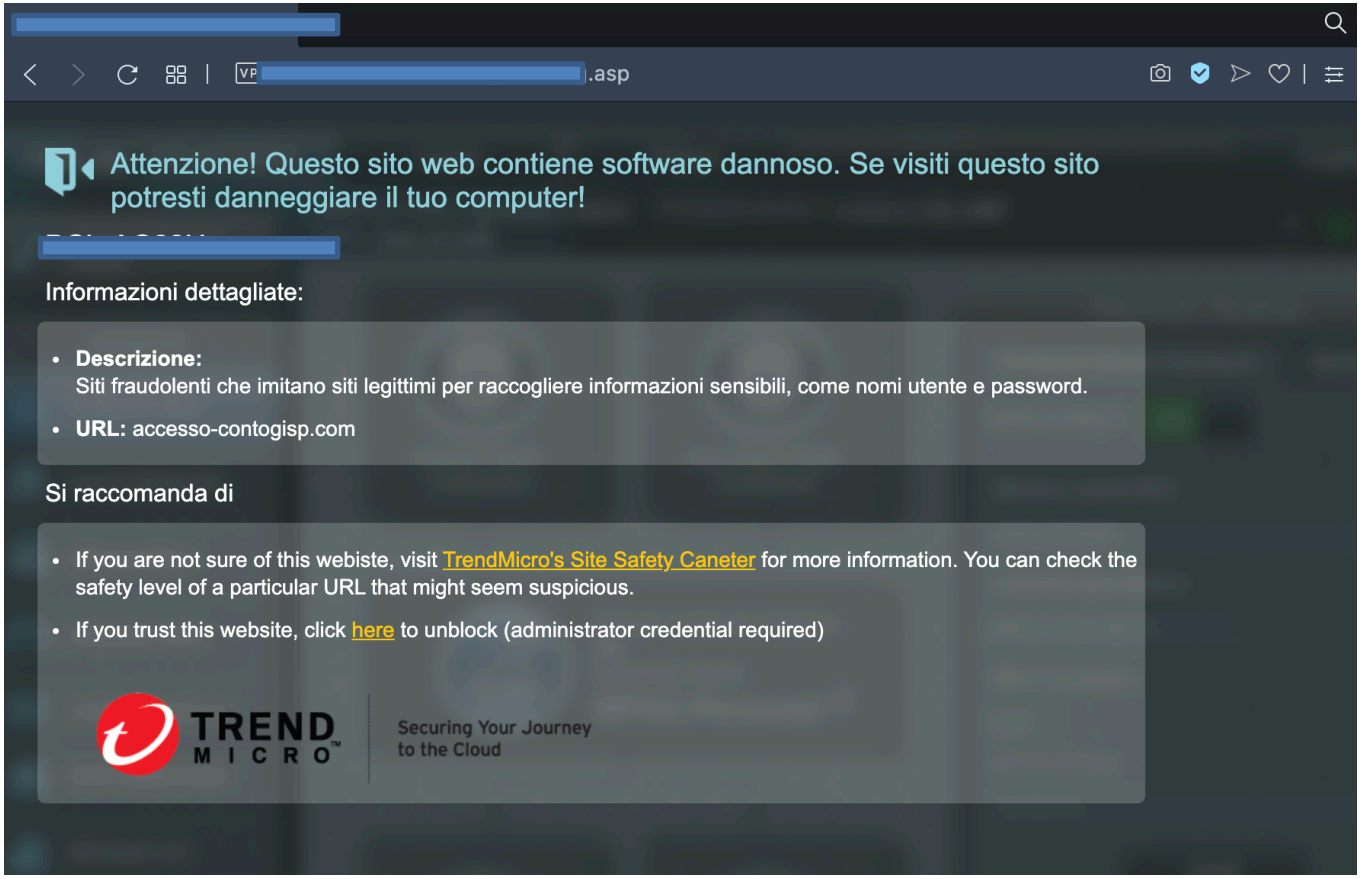
Blocco pagina di phishing (by Chrome)



Blocco pagina di phishing (by Netcraft)



Blocco pagina di phishing (by Firewall)



Blocco pagina di phishing (by 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

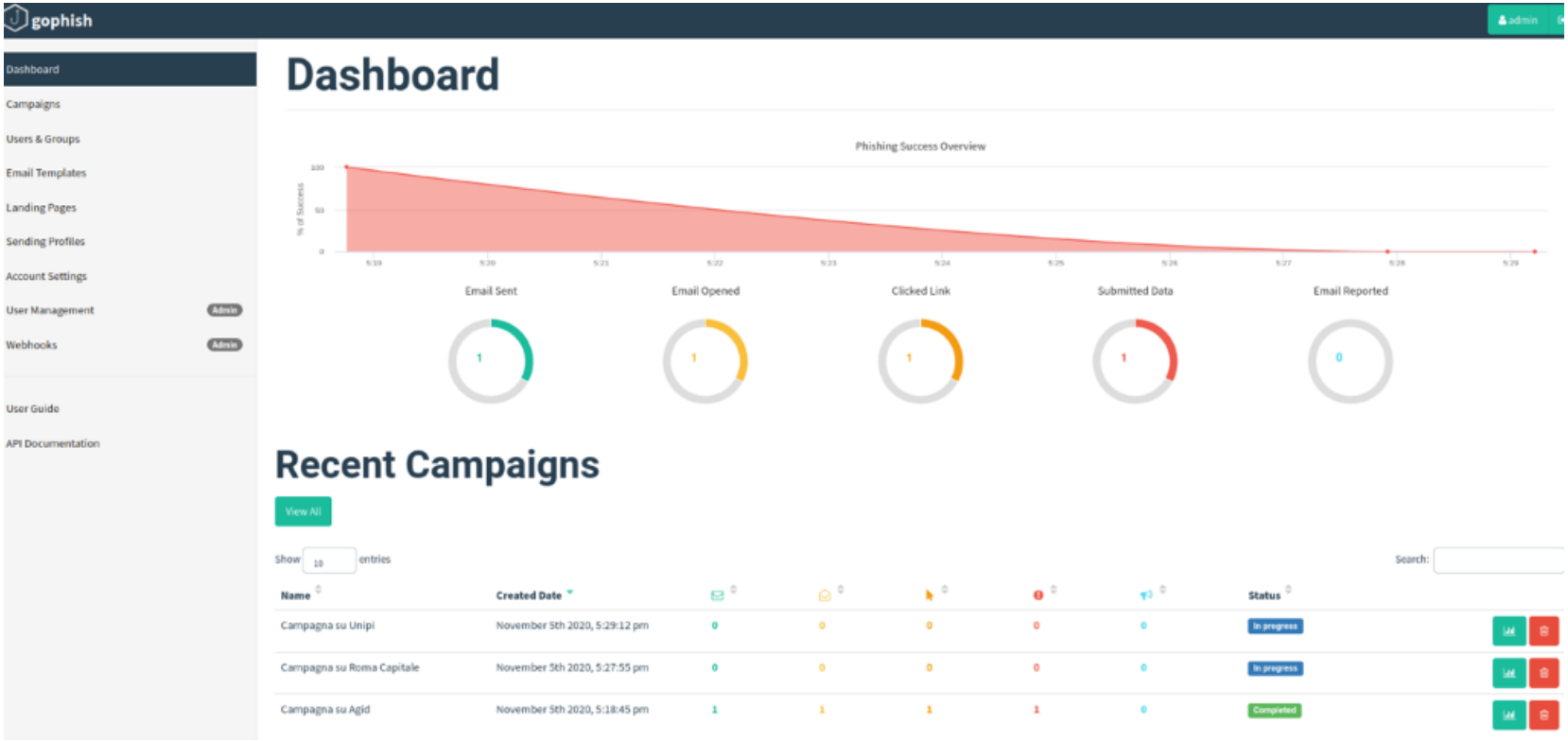
Gophish: tool di simulazione campagne di phishing

- **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**.

Simulazione di una campagna di phishing

- Processo in 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

Monitoraggio della campagna



I benifici delle campagne simulate all'interno delle organizzazioni

- **Miglioramento del livello di consapevolezza** della PA 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.

AGID | Agenzia per l'Italia Digitale

FormezPA

GRAZIE PER L'ATTENZIONE