

Rapporto sugli attacchi e sulle criticità attuali nella cybersecurity

Paolo Passeri
ppasseri@netskope.com
@paulsparrows
<https://www.linkedin.com/in/paulsparrows/>

WHOAMI



Paolo Passeri, (ex) Alfista e Cyber Intelligence Principal di Netskope, è un professionista di sicurezza informatica con oltre 20 anni di esperienza

I campi di interesse includono la sicurezza delle applicazioni cloud, ed il rilevamento del malware avanzato.

Paolo è anche un blogger: nel suo tempo libero, oltre alla corsa e alla bicicletta, gestisce il suo blog personale, hackmageddon.com, considerato una fonte primaria di dati e tendenze nel panorama delle minacce informatiche



IL PANORAMA ATTUALE

- Il 60% dei dati risiede nel cloud¹
- Una organizzazione media utilizza 2,415 servizi cloud²
- Oltre il 60% dei dipendenti lavora da remoto³
- Il concetto di *Digital Trust* degli utenti è cambiato⁴

¹ <https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/>

² <https://www.netskope.com/resources/reports-guides/cloud-and-threat-report-february-2020-edition>

³ <https://www.netskope.com/resources/reports-guides/cloud-and-threat-report-2022-year-in-review>

IL CLOUD ACCELERA LA TRASFORMAZIONE DIGITALE

Cloud has a multitude of implications for corporate strategy, risk, and the broader business.

Category	Example impact	
 Improved speed and agility	~90%	improvement in time to market
 Easier innovation	~95%	time reduction for adding digital features
 Efficient scalability	~10–15%	savings from capacity utilization
 Reduced risk	~90%	outage reduction

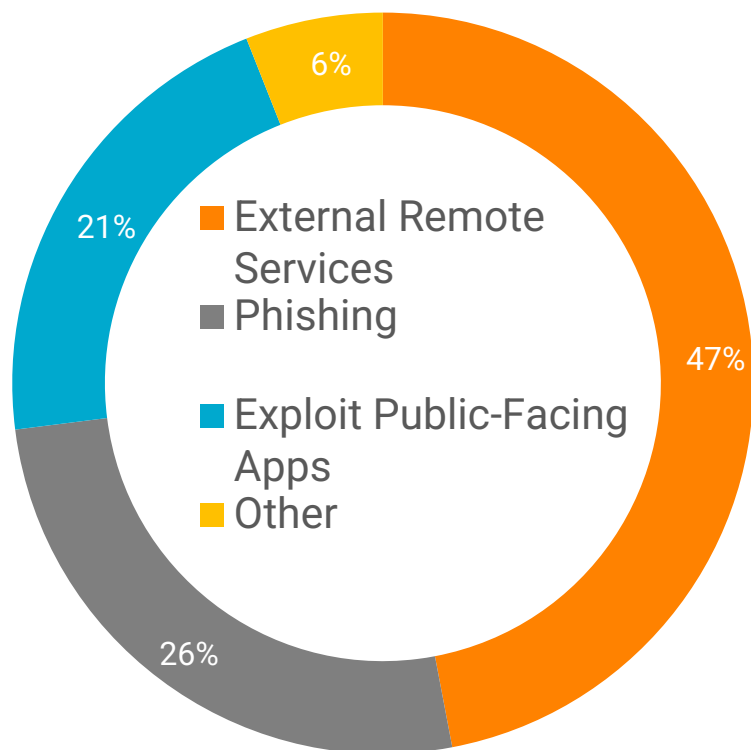
Ma introduce anche nuovi rischi...

Source: Based on externally available information on the internet and team analysis

McKinsey
& Company

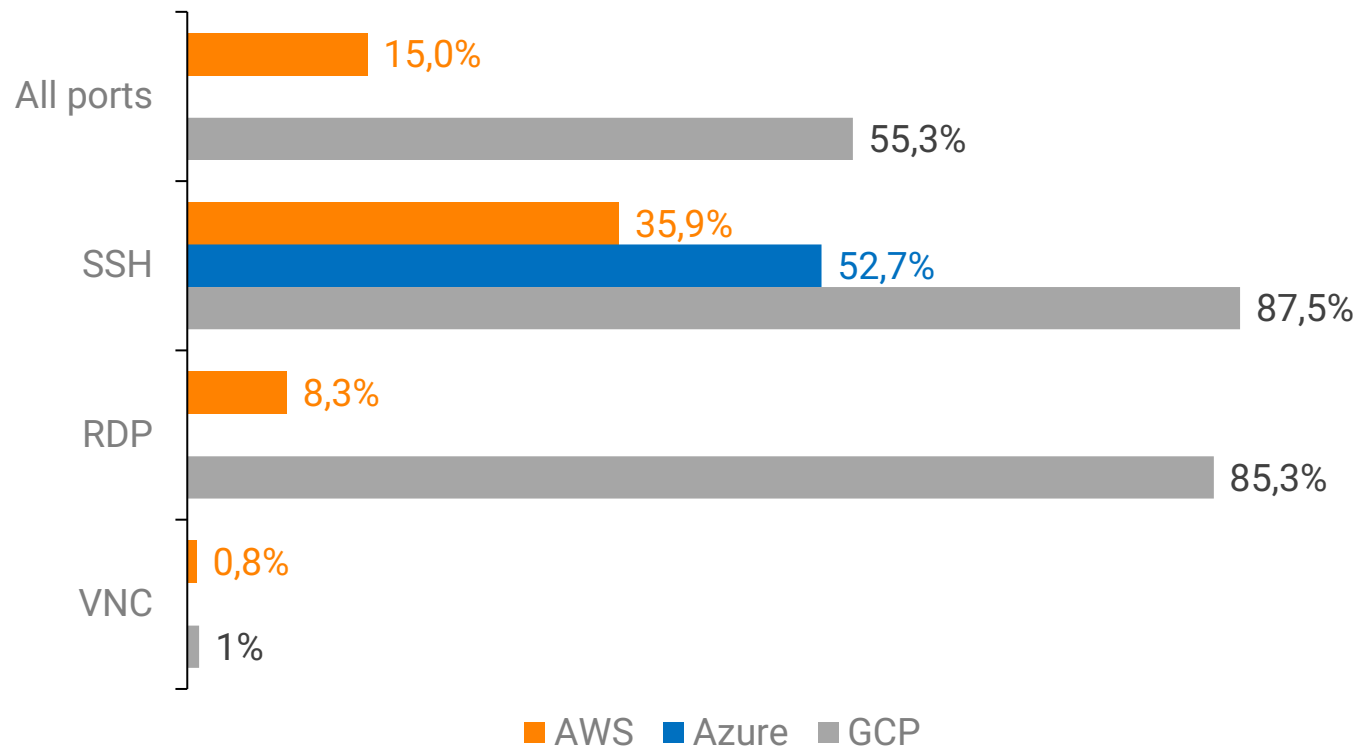
SERVIZI ESPOSTI: IL CLOUD COME OBBIETTIVO

VETTORI PRINCIPALI DI ACCESSO INIZIALE PER IL RANSOMWARE



Group-IB: Ransomware Uncovered 2021-2022

WORKLOAD ESPOSTI IN CLOUD



Netskope: Remote Access Statistics for Public Cloud Workloads

PRINCIPALI MINACCE AL CLOUD

Posizione 2022		Posizione 2019
1	Insufficient Identity, Credentials, Access, and Key Management	4 
2	Insecure Interfaces and APIs	7 
3	Misconfiguration and Inadequate Change Control	2 
4	Lack of Cloud Security Architecture and Strategy	3 
5	Insecure Software Development	
6	Unsecured Third-Party Resources	
7	System Vulnerabilities	
8	Accidental Cloud Data Disclosure	
9	Misconfiguration and Exploitation of Serverless and Container Workloads	
10	Organized Crime/Hackers/APT	11 
11	Cloud Storage Data Exfiltration	

Top Threats to Cloud Computing



A man in a dark suit and tie stands in the foreground with his hands raised in a gesture of surrender or protest. He is looking upwards with a concerned expression. The background is a scene of total urban devastation. A massive firestorm, composed of a dense cloud of orange and yellow sparks and flames, engulfs the city. In the distance, the skeletal remains of several tall buildings are visible against the hazy, smoke-filled sky. To the right, a large, dark, jagged structure, possibly a damaged industrial building or bridge, stands amidst the wreckage. A lone figure can be seen running away from the viewer in the lower right background. The overall atmosphere is one of chaos and despair.

**Nothing to see here.
Please disperse.**

E COME VETTORE DI ATTACCO...

48%

DEL MALWARE
PROVIENE DA
APPLICAZIONI
CLOUD

401

DIFFERENTI
APPLICAZIONI
CLOUD UTILIZZATE
PER DISTRIBUIRE
MALWARE

94.4%

PERCENTUALE DI
MALWARE PROVENIENTE
DA SITI COMPROMESSI,
SITI FAKE O SERVIZI DI
HOSTING

30%

DEL MALWARE
PROVIENE DA
ONEDRIVE

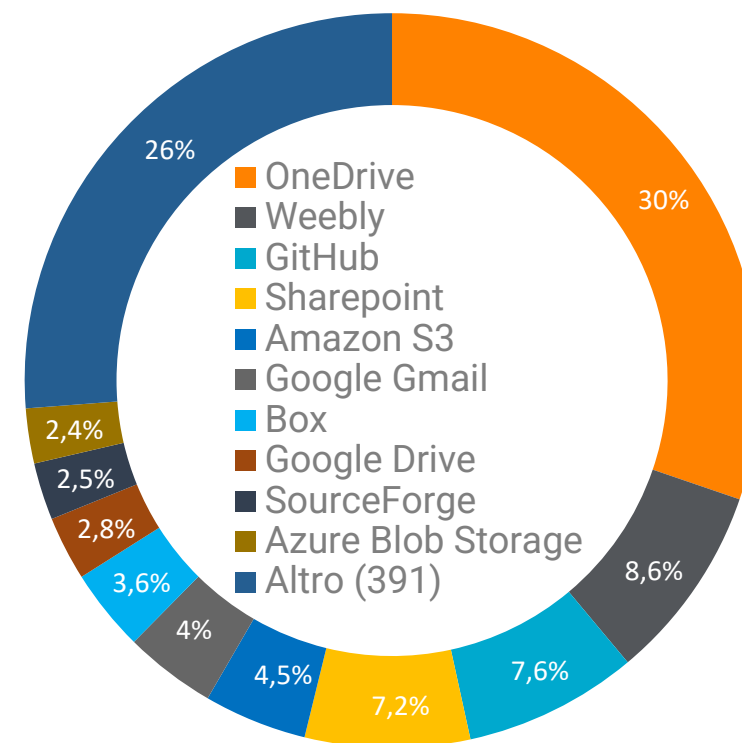
40%

UTENTI CHE USANO
ONEDRIVE OGNI
GIORNO

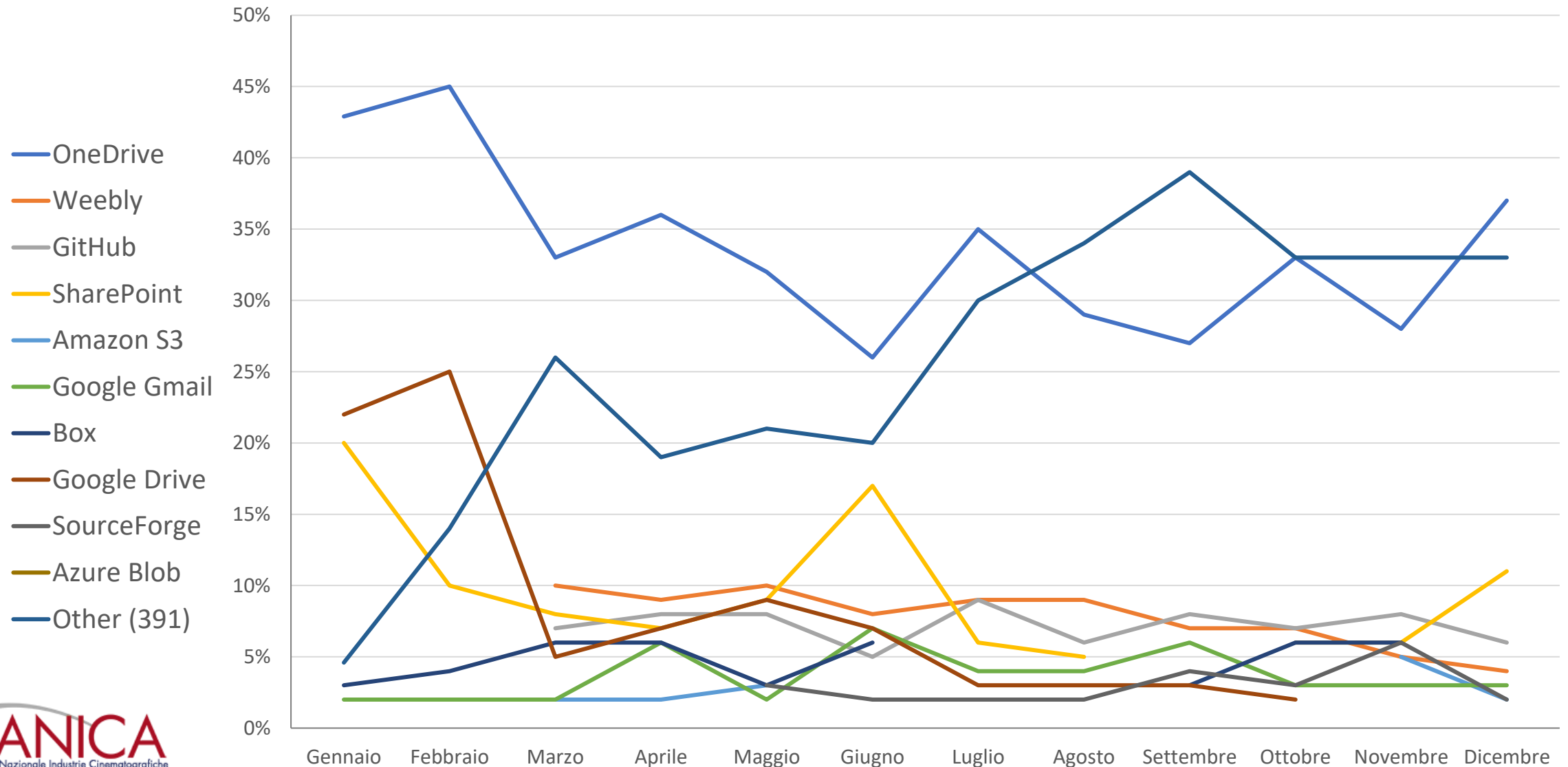
25%

UTENTI CHE CARICANO
FILE SU ONEDRIVE OGNI
GIORNO

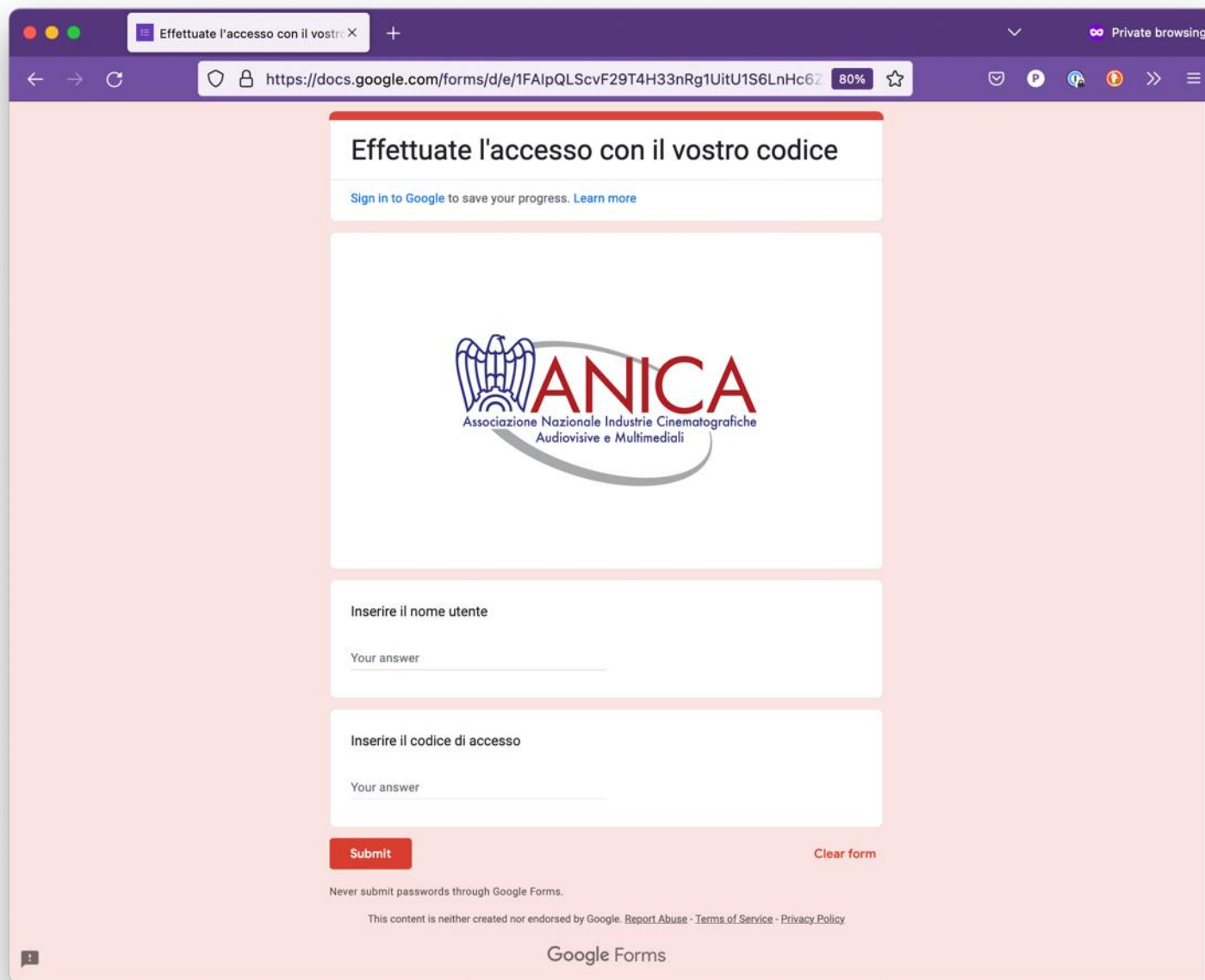
TOP EXPLOITED APPS



PRINCIPALI APP PER DISTRIBUIRE MALWARE



PAGINA DI PHISHING SU UN SERVIZIO CLOUD



The screenshot shows a web browser window displaying a phishing page designed to look like a Google Form. The browser's address bar shows a URL from docs.google.com. The page has a light pink background and a white central box containing the ANICA logo and form fields. The ANICA logo is at the top, followed by the text 'Effettuate l'accesso con il vostro codice'. Below this is a link to 'Sign in to Google'. The form has two input fields: 'Inserire il nome utente' and 'Inserire il codice di accesso', each with a 'Your answer' placeholder. At the bottom of the form are 'Submit' and 'Clear form' buttons. A warning message at the bottom of the page states: 'Never submit passwords through Google Forms. This content is neither created nor endorsed by Google. Report Abuse · Terms of Service · Privacy Policy'. The Google Forms logo is at the very bottom.

Effettuate l'accesso con il vostro codice

[Sign in to Google](#) to save your progress. [Learn more](#)


Associazione Nazionale Industrie Cinematografiche
Audiovisive e Multimediali

Inserire il nome utente

Your answer

Inserire il codice di accesso

Your answer

Submit Clear form

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. [Report Abuse](#) · [Terms of Service](#) · [Privacy Policy](#)

Google Forms

- Tempo necessario per creare la pagina: **5 minuti** (ascoltando la musica e parlando al telefono)
- Costo: **0 EURO**
- **BONUS POINT:** Gmail può essere utilizzata per inviare la mail di phishing



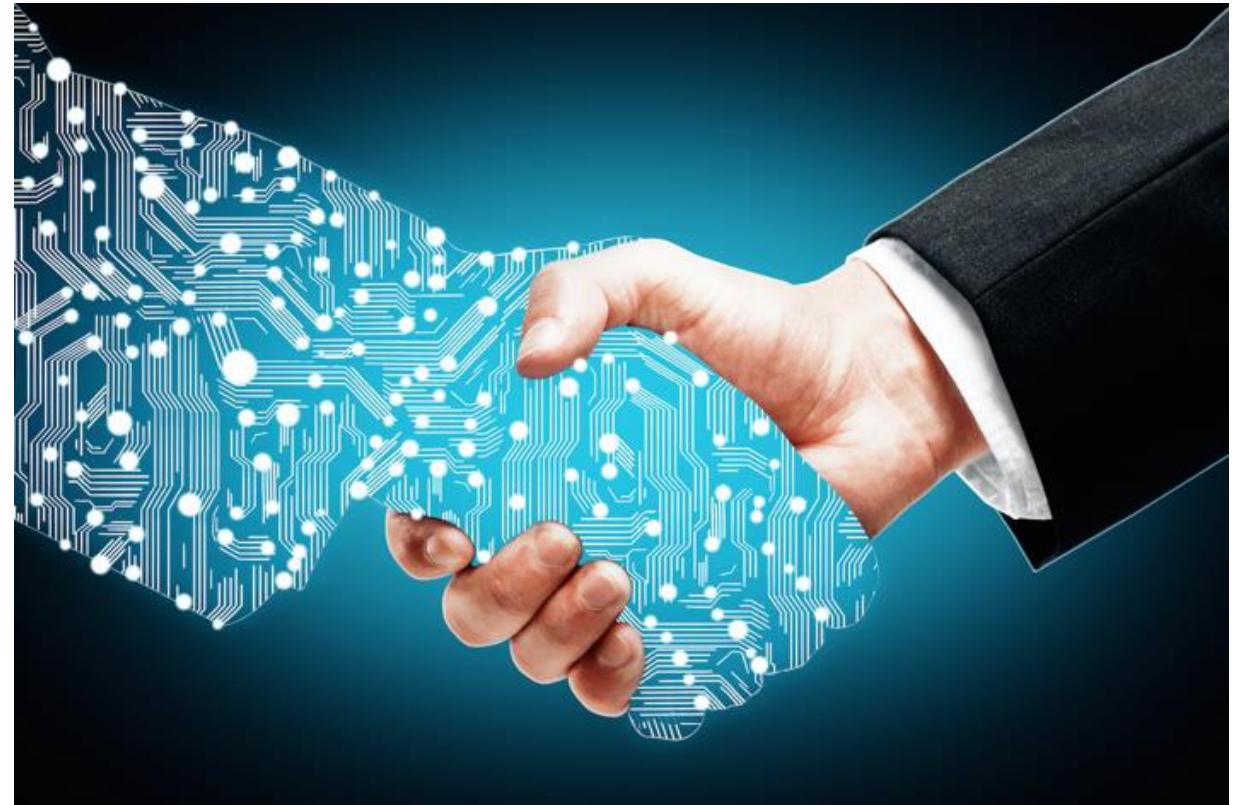
UNA TECNOLOGIA
TRADIZIONALE ALLE PRESE
CON IL TRAFFICO CLOUD

IL DIGITAL TRUST



Digital Trust is a necessity in a global economy reliant on ever-increasing connectivity, data use, and new innovative technologies.

In order to be trustworthy, technology must be secure (ensuring connected systems' confidentiality, integrity, and availability) as well as responsibly used.



COME CI VEDIAMO NOI...



COME CI VEDONO GLI ATTACCANTI



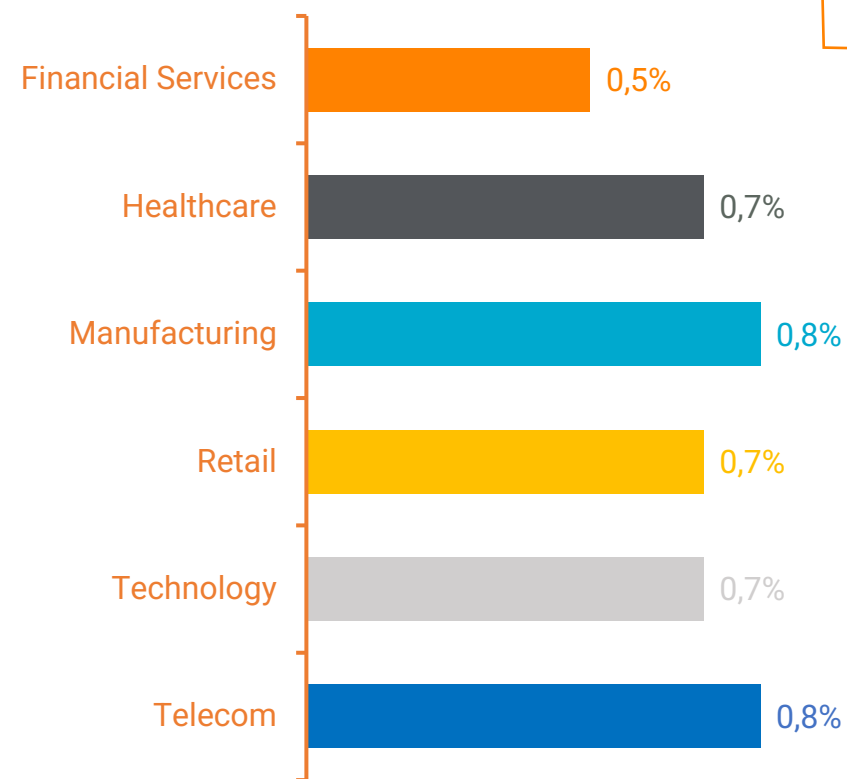
GLI ATTACCANTI SFRUTTANO CONTINUAMENTE IL DIGITAL TRUST

L'intento è quello di far presa sulle nostre emozioni e farci premere il famigerato bottone rosso (un link malevolo, aprire un allegato, etc..)

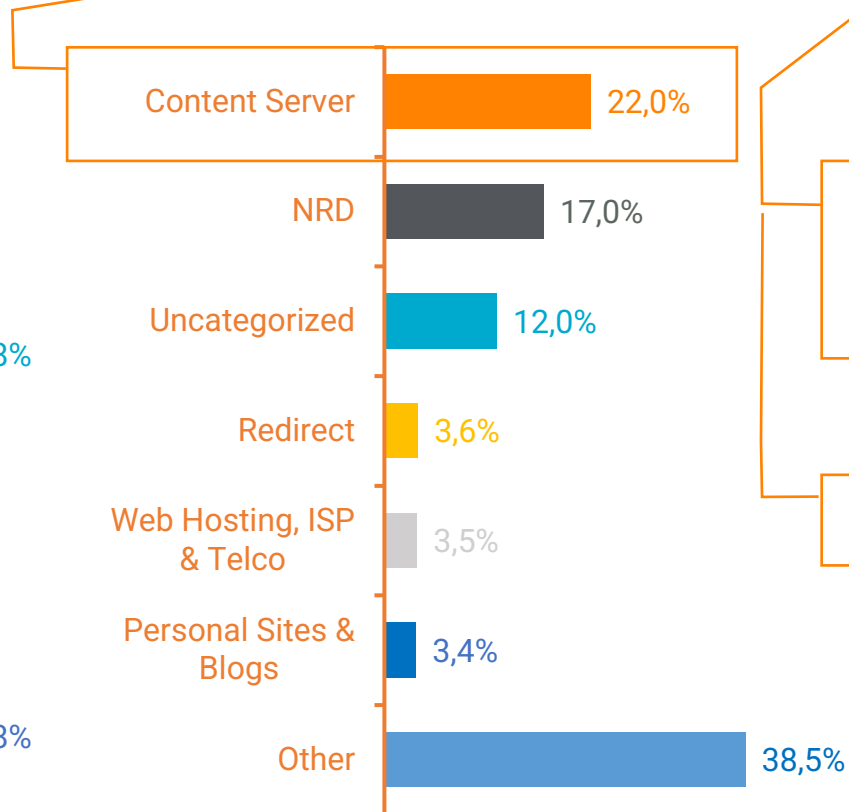


PHISHING: Q3 2022

PHISHING BY INDUSTRY
(CLICK EVERY 1000 USERS)

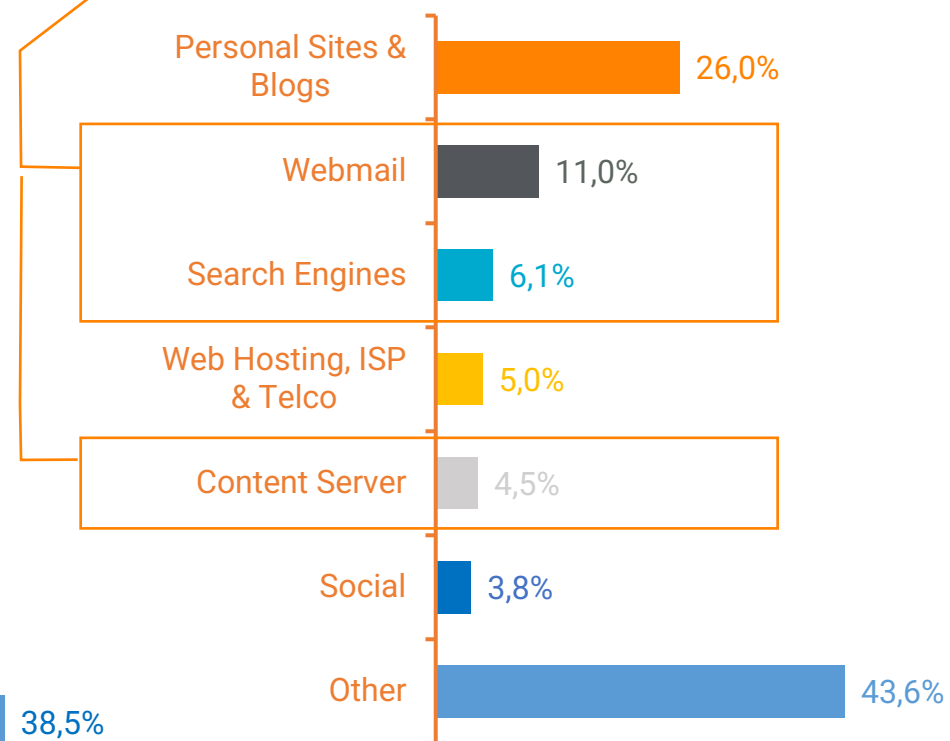


PHISHING HOSTING



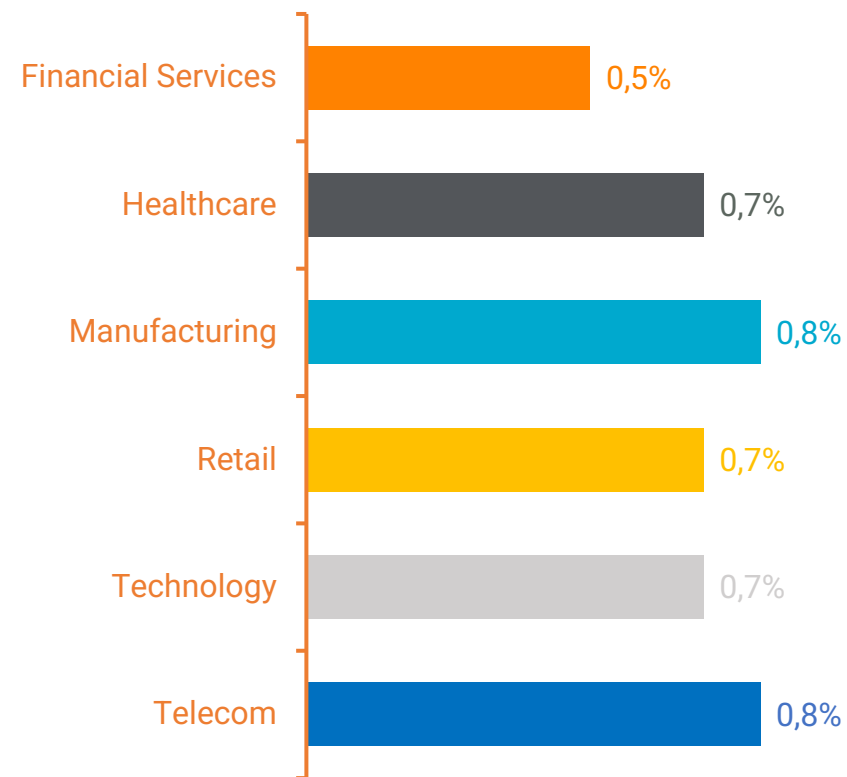
Sfruttamento del Digital Trust

PHISHING REFERERS

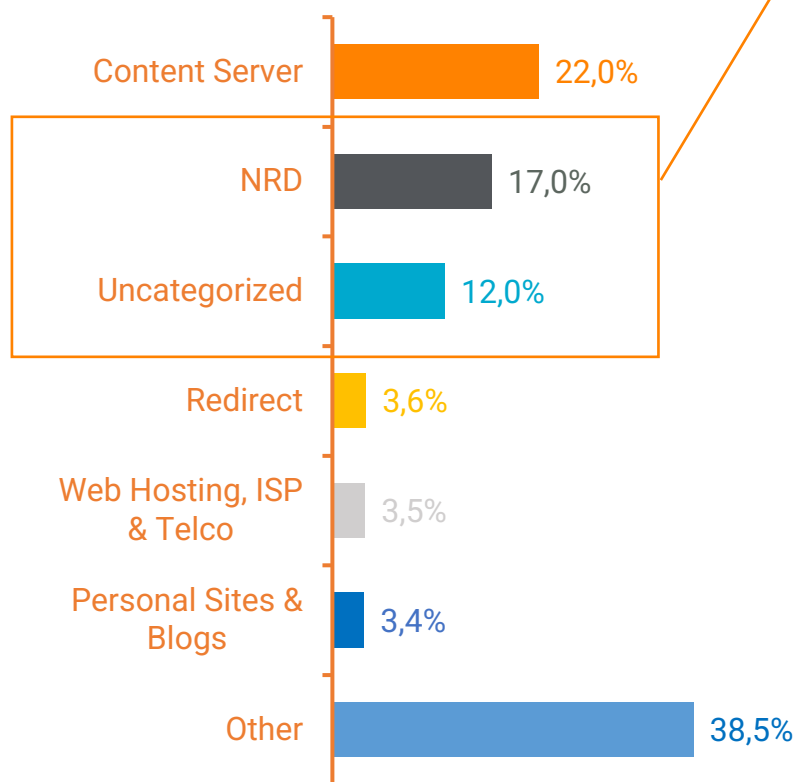


PHISHING: Q3 2022

PHISHING BY INDUSTRY
(CLICK EVERY 1000 USERS)

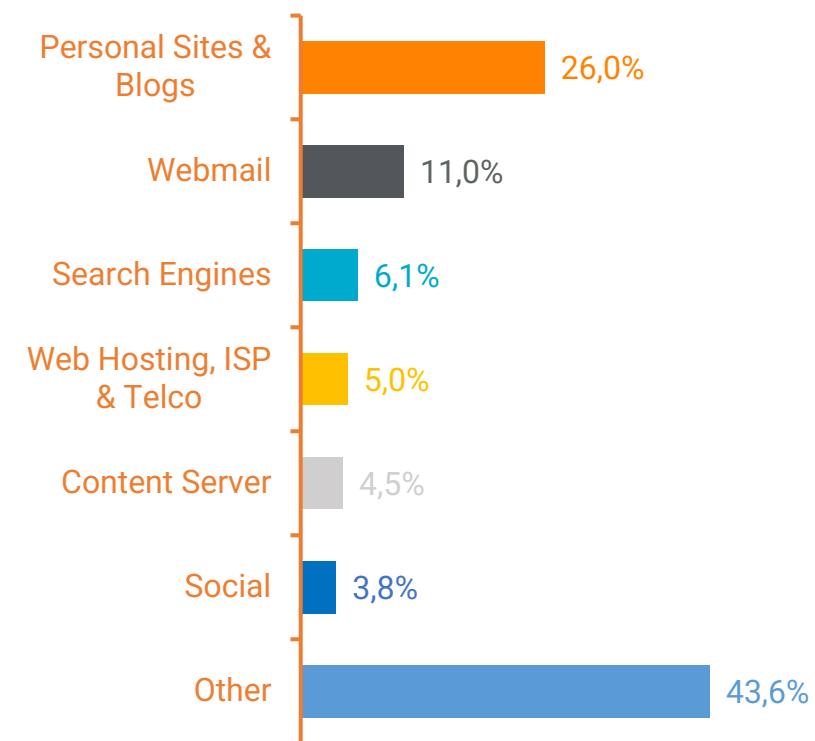


PHISHING HOSTING



Mancanza di educazione di sicurezza

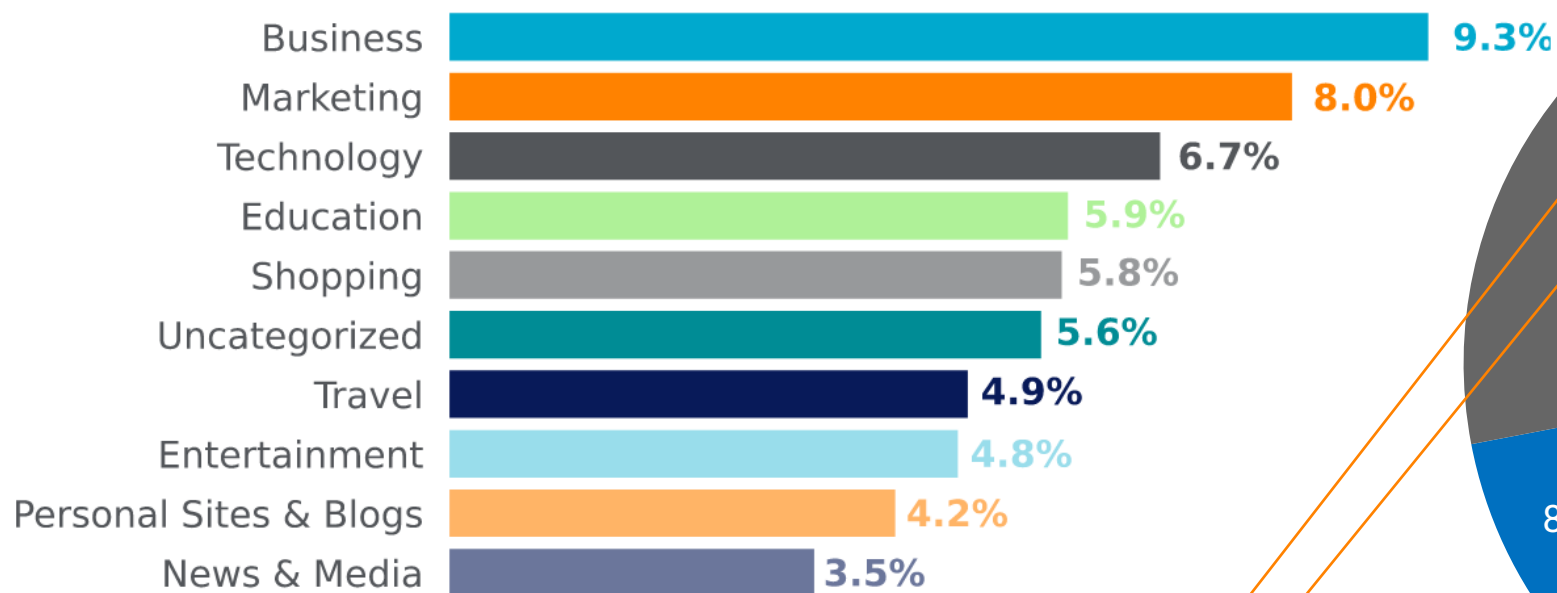
PHISHING REFERERS



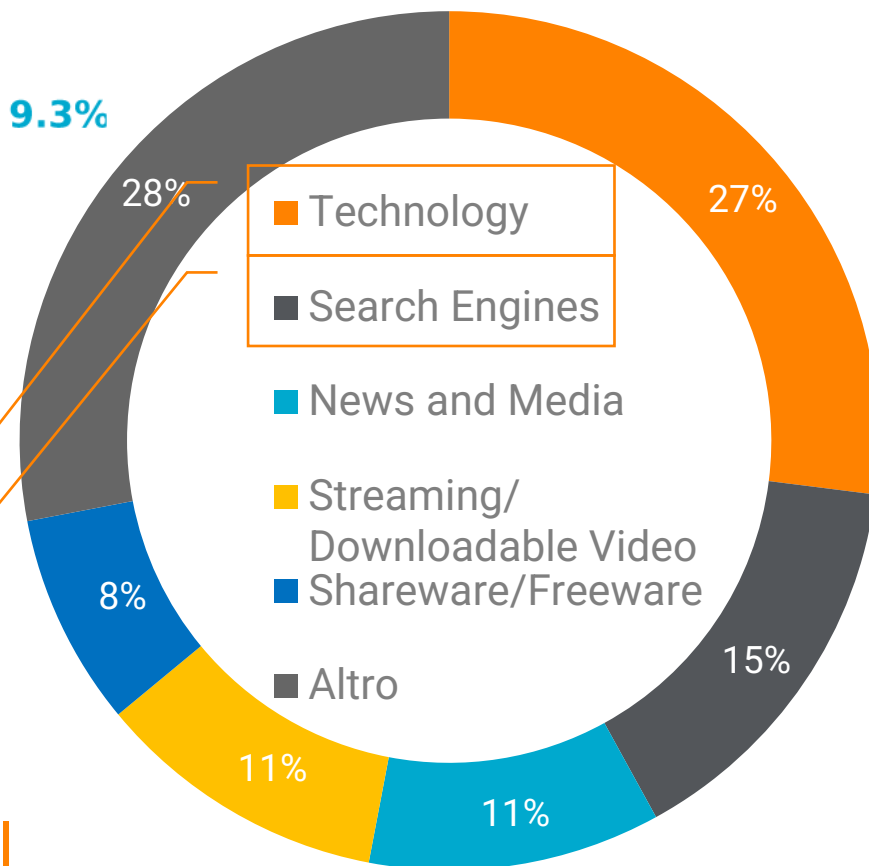
Netskope Cloud and Threat Report: Phishing
Data from July 1, 2022 through September 30, 2022.

PHISHING: Q3 2022

PRINCIPALI CATEGORIE DI DISTRIBUZIONE DEL MALWARE



LINK DI PROVENIENZA



Sfruttamento del
Digital Trust



ONE DOES NOT SIMPLY...

GIVES AWAY WINDOWS 11 UPGRADES FOR FREE

STRATEGIE DI MITIGAZIONE

- Il **cloud** è un fattore abilitante per la trasformazione digitale, ma anche un fattore di ampliamento della superficie di attacco.
- Gli attaccanti stanno sfruttando il **digital trust**, utilizzando servizi leciti per distribuire malware o per reindirizzare a contenuto malevolo.
- Le organizzazioni devono incoraggiare una **cultura di sicurezza**
- Questi aspetti sono critici dal momento che la **forza lavoro** è distribuita e gli utilizzano i dispositivi aziendali per uso personale
- I controlli di sicurezza debbono ora essere applicati al punto di accesso per proteggere gli utenti da ovunque essi si colleghino, indipendentemente dal dispositivo.