TD SYNNEX

Mail security con Proofpoint

Una soluzione completa per la protezione delle caselle e degli utenti

24 Gennaio 2025

Webinar

Andrea Pezzoni – Security Presales Specialist – TD SYNNEX
Giuseppe Vacca – TechSystem srl

Le caselle email come vettore privilegiato

Le caselle mail sono il metodo più semplice ed efficace per iniziare un attacco

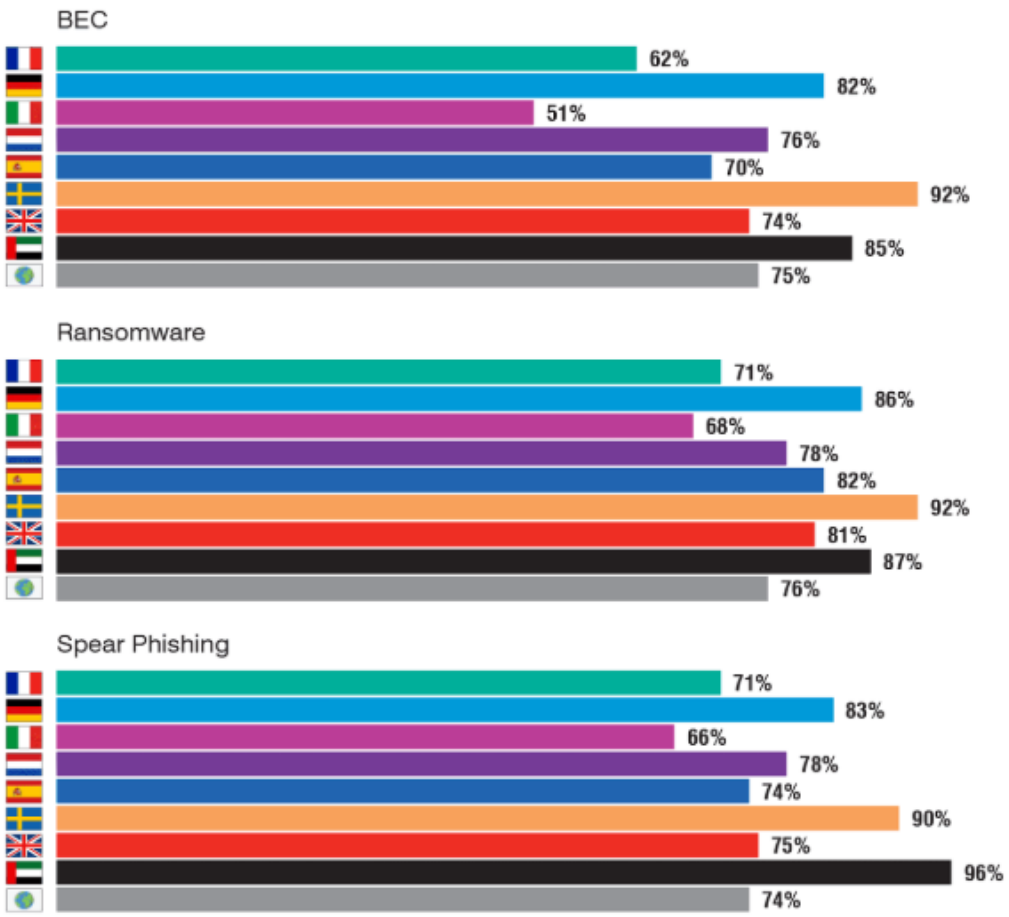
- 57% delle organizzazioni affronta campagne di Phishing quotidianamente o settimanalmente (GreatHorn)
- 1,2% delle email spedite quotidianamente sono malevole, circa 3,4 Miliardi di mail al giorno (APWG)
- 80% degli incidenti di sicurezza segnalati partono da un’attività di Phishing (CSO Online)
- 51,7% delle mail malevole impersonificano un brand conosciuto (Cloudflare)
- 35% degli attacchi malware comincia con una mail di Phishing (IBM)
- AI-Powered Phishing è la nuova frontiera delle campagne malevole (Zscaler)
- Un nuovo sito collegato a campagne Phishing viene creato ogni 20 secondi (DataProt)

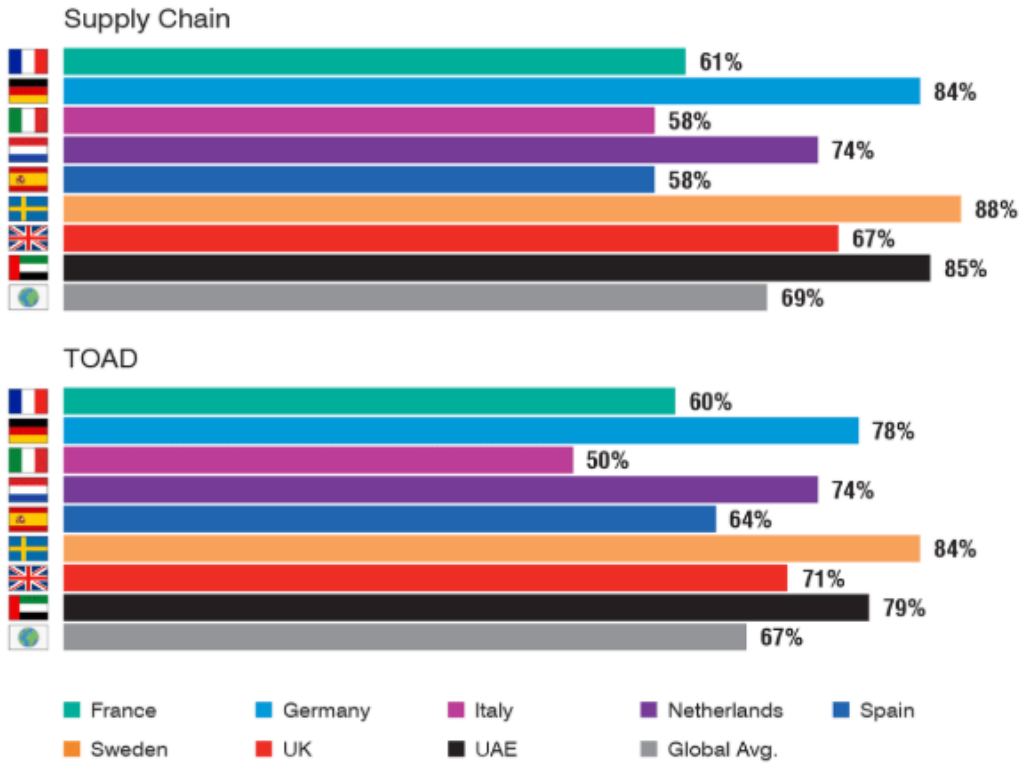
Email Attacks: non solo Phishing

- Phishing
- Whale Phishing
- Spear Phishing
- Vishing
- Quishing
- Adware
- Social Engineering
- Brand Impersonation
- Man in the middle
- Pharming
- Malware attack
- Spoofing
- Spam
- Evil twin attack
- Angler attack

TD SYNNEX

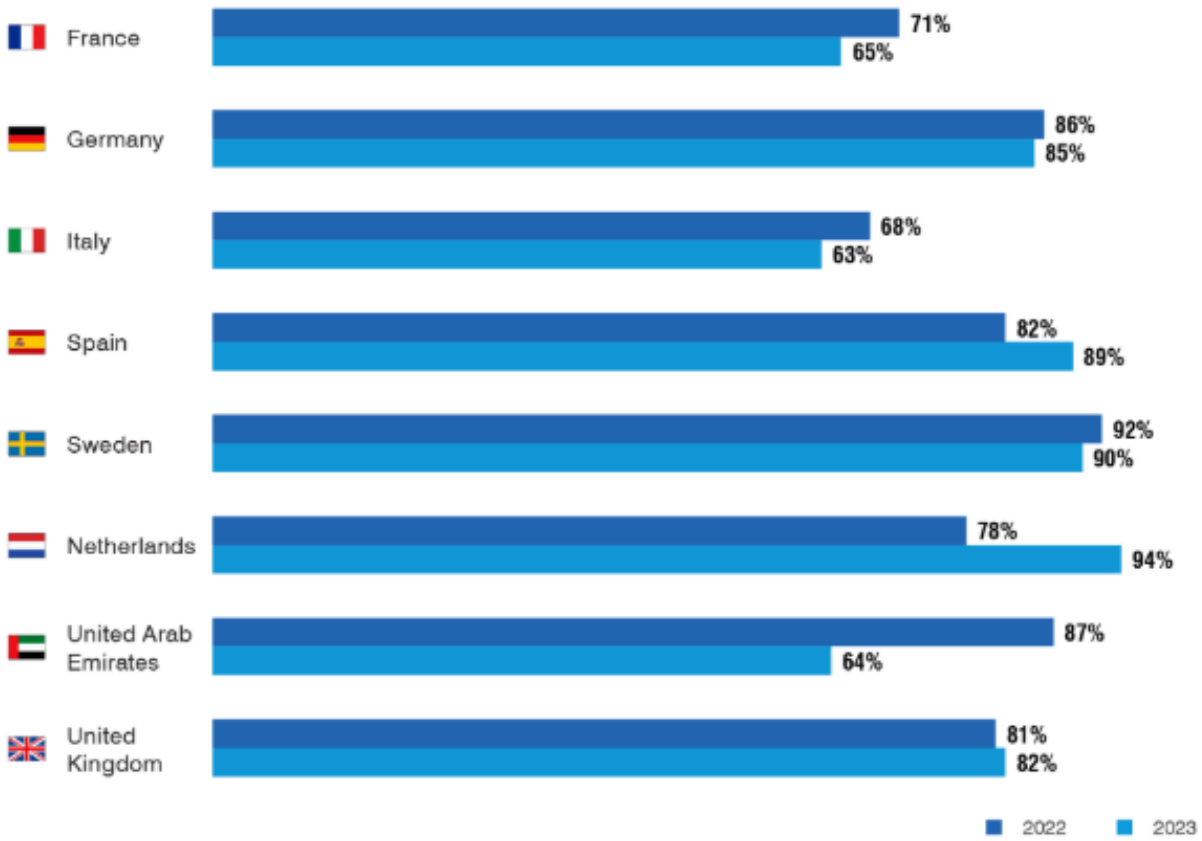
Statistiche



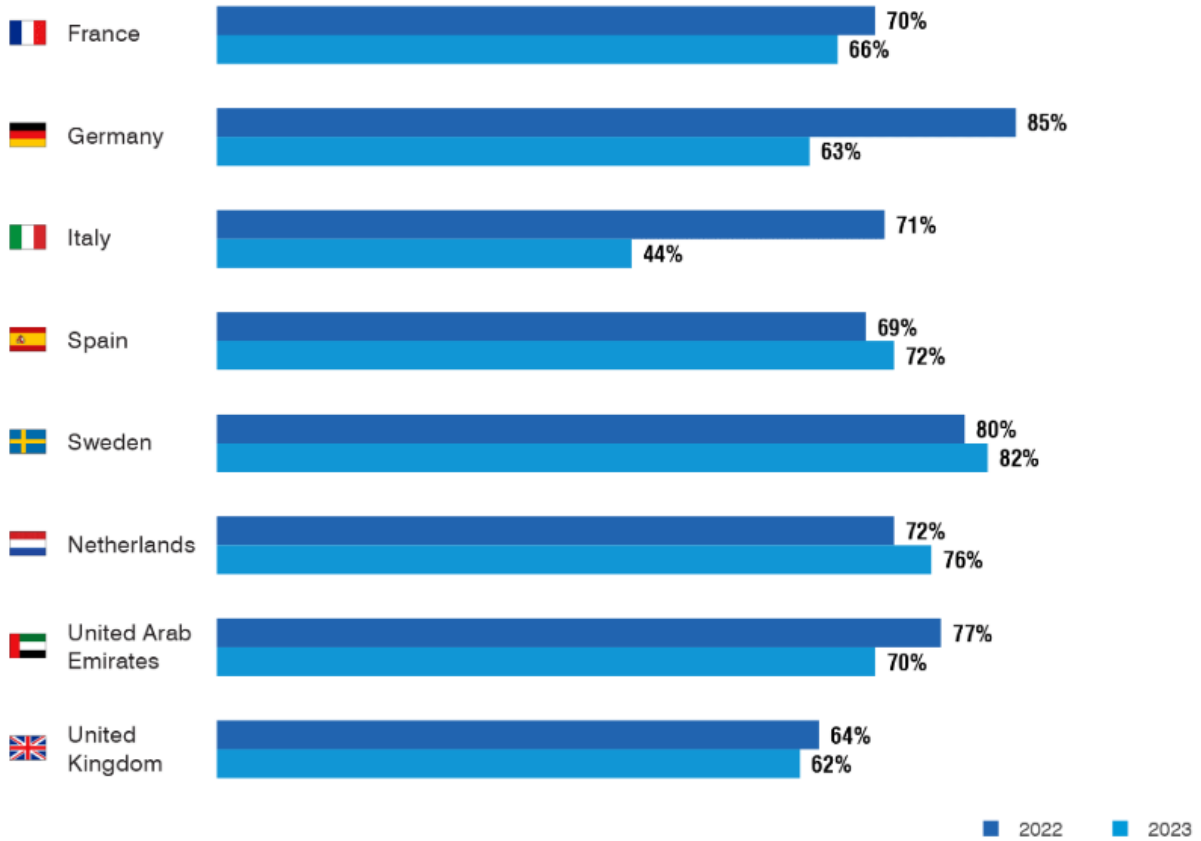


Alcuni numeri

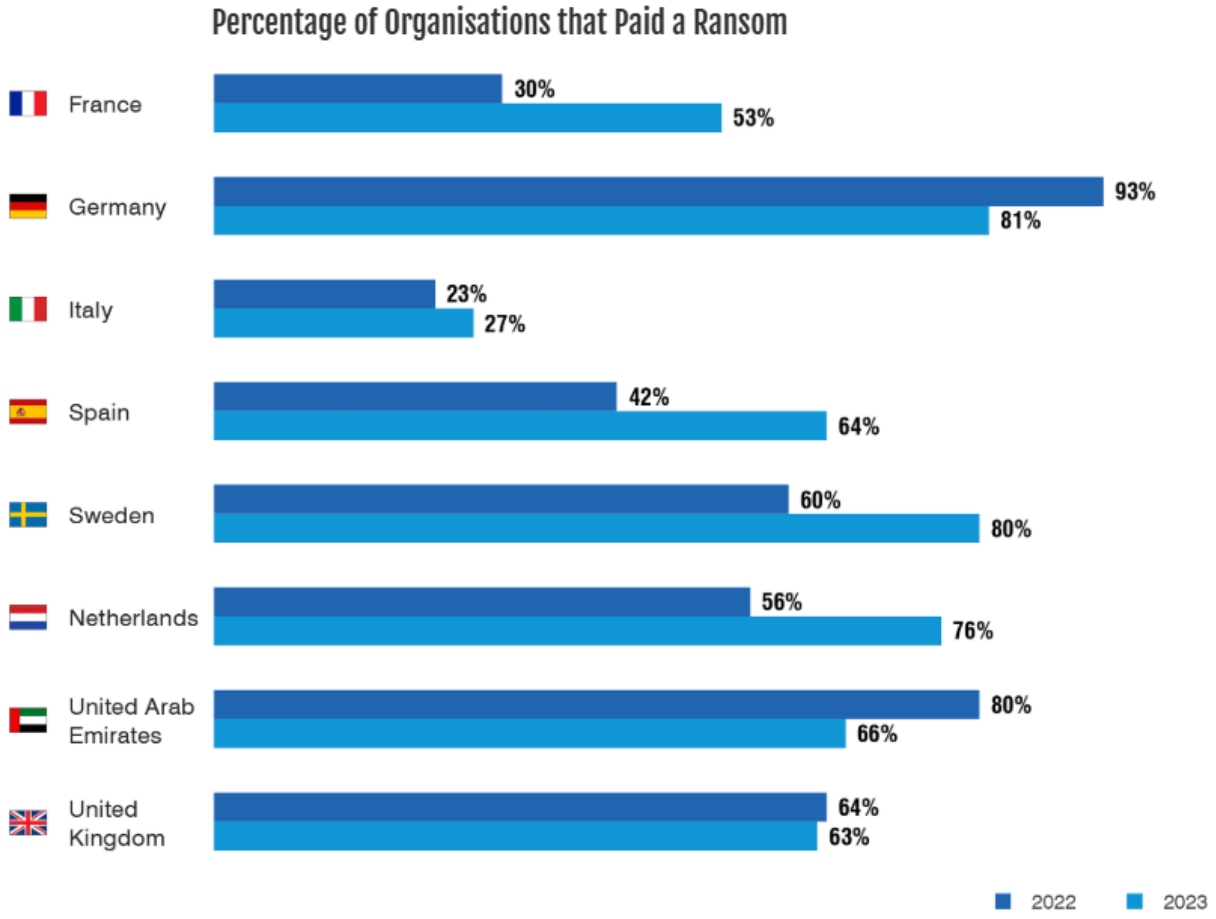
Email-Based Ransomware Attack Trend

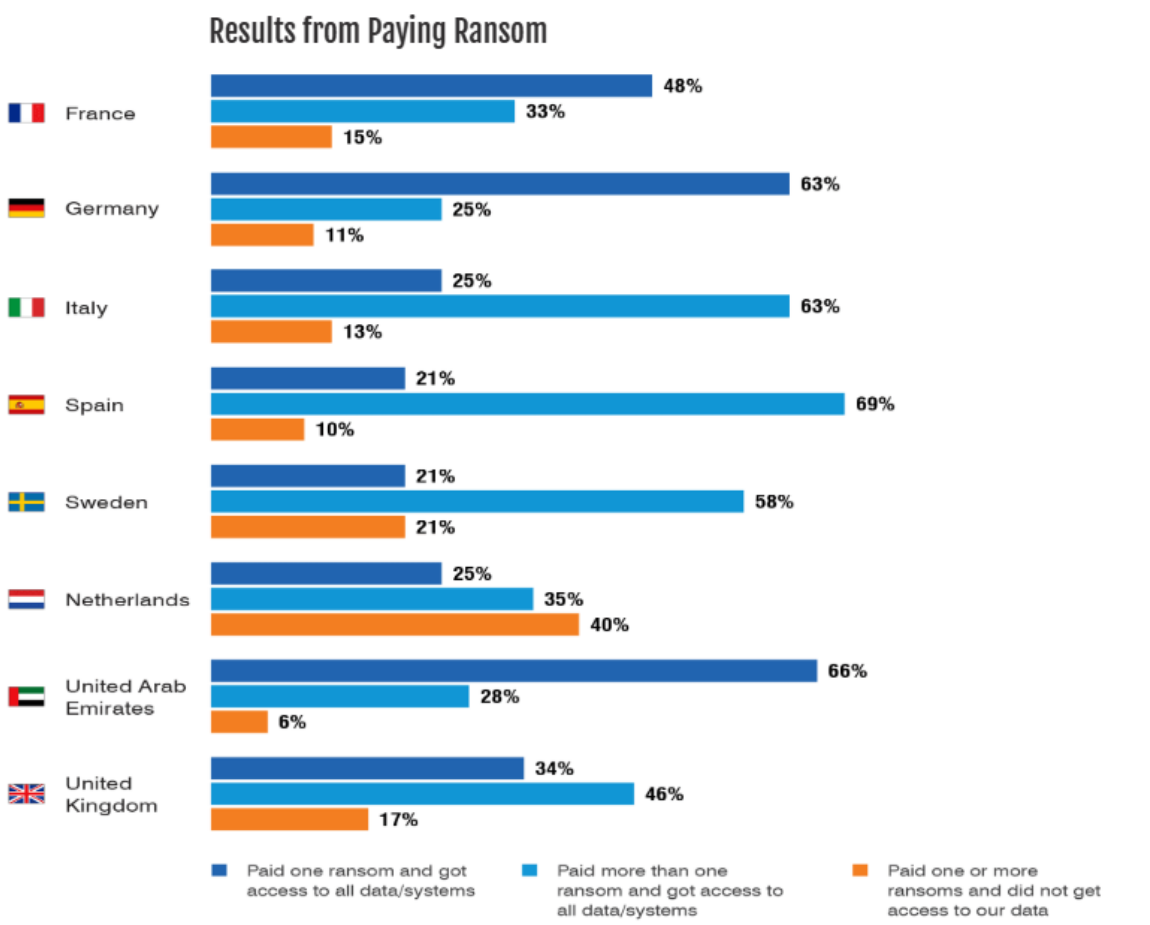


Ransomware Infection Trend



I numeri dei riscatti





La soluzione Proofpoint Essential

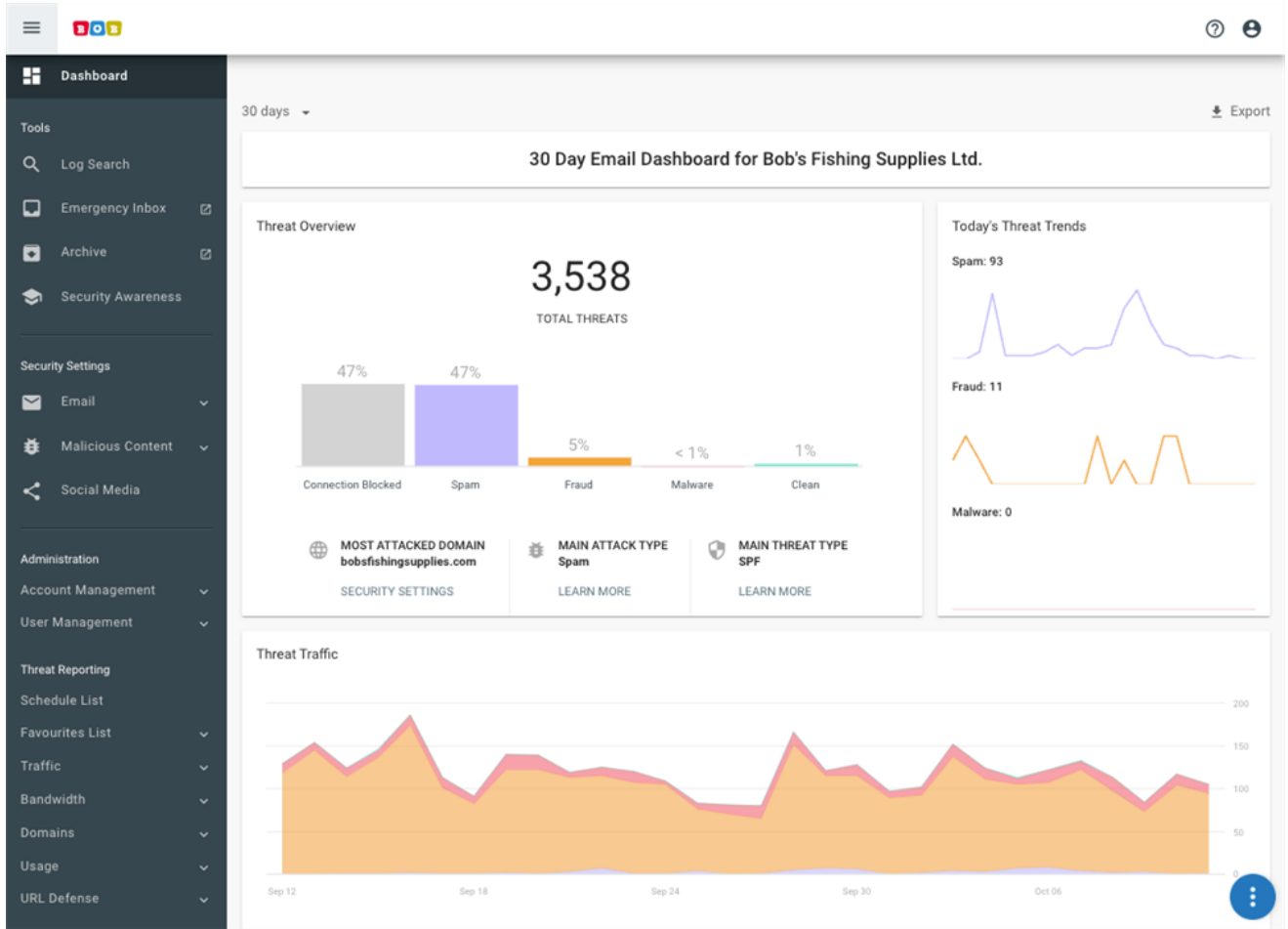
- Soluzione Leader di mercato per Gartner nella protezione mail
- Piattaforma cloud per Mail Security e Security Awareness
- Nativamente Multitenant
- Fatturazione mensile, nessun impegno a lungo termine
- Soluzione ready to go
- Paga solo quello che consumi

TD SYNNEX

Livelli di servizio

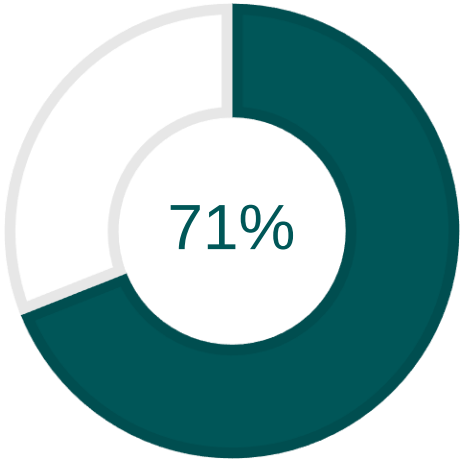
	BEGINNER	BUSINESS	ADVANCED	PRO
SECURITY				
Anti Virus	✓	✓	✓	✓
Spam Filtering	✓	✓	✓	✓
Reporting	✓	✓	✓	✓
Content Filtering	✓	✓	✓	✓
Outbound Filtering	✓	✓	✓	✓
Impostor Email Protection	✓	✓	✓	✓
Data Loss Prevention		✓	✓	✓
URL Defense (Sandboxing)		✓	✓	✓
Attachment Defense (Reputation)		✓	✓	✓
Attachment Defense (Sandboxing)			✓	✓
Email Encryption			✓	✓
Social Media Account Protection			✓	✓

Analisi e Log a vostro servizio



- Analisi dinamica delle minacce
- Identificazione degli utenti più colpiti
- Gestione della quarantena
- Geolocalizzazione del mittente
- Analisi dei contenuti e indice di affidabilità
- Emergency Inbox
- Filtri personalizzabili

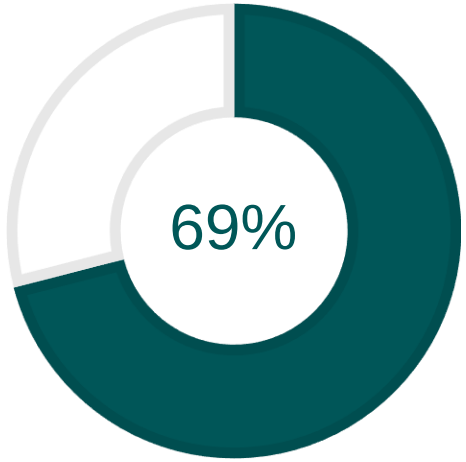
Il fattore umano



Utenti che hanno compiuto azioni rischiose dal punto di vista di sicurezza

E’ consapevole di aver compiuto azioni rischiose

Ha fatto azioni che lo espongono ad un attacco di Social Engineering

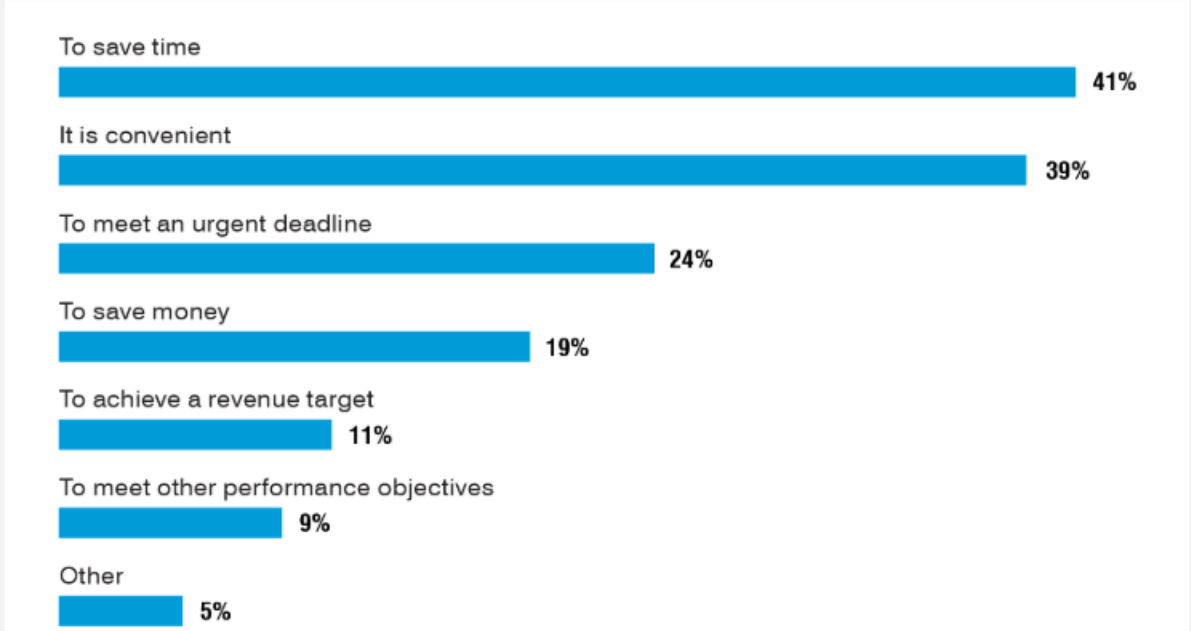


Organizzazione colpite da Ransomware negli ultimi 5 anni

Comportamenti rischiosi

Rank	Risky Behaviour (Ranked by Sec Pros)	Risky Behaviour (Conducted by Users)
1	**Reuse or share password**	Use work device for personal activities
2	Click on links or download attachments from someone I don't know	**Reuse or share password**
3	Upload sensitive data to unproven 3rd party cloud	Connect without using VPN at a public place
4	Give credentials to untrustworthy source	Respond to a message (email or SMS text) from someone I don't know
5	**Access inappropriate website**	**Access inappropriate websites**

Why Users Take Risky Actions



Awareness

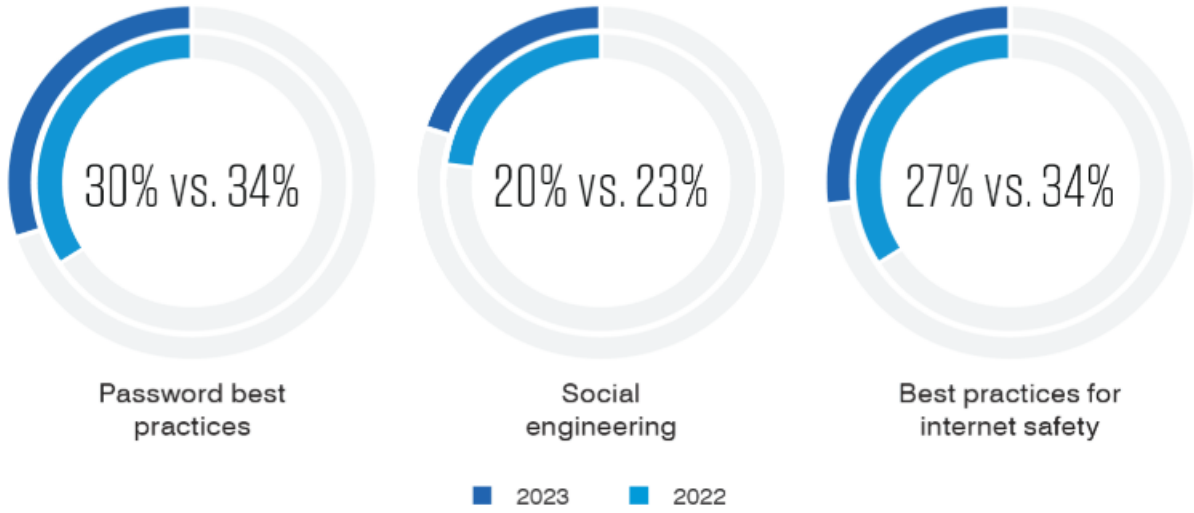
Obbligo normativo NIS2

Lavorare sul Layer 8 della sicurezza

Miglioramento del Firewall Umano

Campagne di formazione di base e di Phishing Simulation

However, the number of organisations training on essential topics seems to be declining:



These are all critical security basics. And if fewer users know how to set secure passwords, avoid common lures and surf the web safely, cybercriminals will surely take advantage.

TOAD Attack

Opportunities for Improvement

95% of organisations in the region already use threat intelligence to inform their security awareness training programs. But there are significant gaps. While most organisations reported being targeted by telephone-oriented attack delivery (TOAD), less than a third train on this tactic. In Germany, 78% of organisations experienced TOAD attacks, but only 21% train on the technique—one of the largest gulfs between daily attacks and training topics.

Overall, more time is being devoted to security awareness training across the region. Spain saw the largest increase, with a 120% rise in organisations spending three or more hours per year.

78%

of German organisations experienced TOAD attacks, but only

21%

train on the technique

I TOAD Attack, letteralmente Telephone Oriented Attack Delivery, sono attacchi mirati che mirano ad estrapolare credenziali e altre informazioni sensibili tramite una telefonata di un hacker che impersonifica il personale di assistenza tecnica di un'azienda, inducendo l'utente a rilevare credenziali.

L'attacco più famoso è quello degli alberghi MGM di Las Vegas del 2023.

Parola ad una nostro partner

techsystem
Il tuo partner informatico

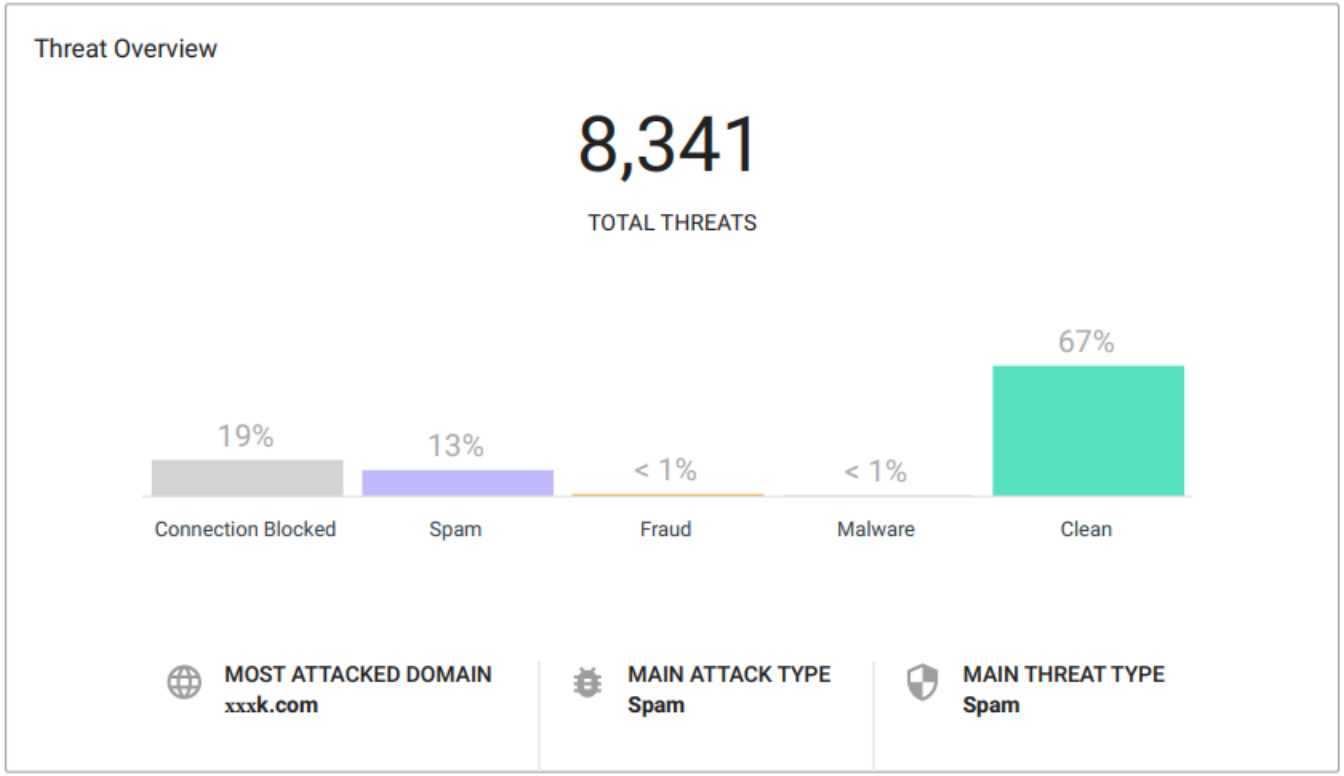
Techsystem: il tuo Partner informatico

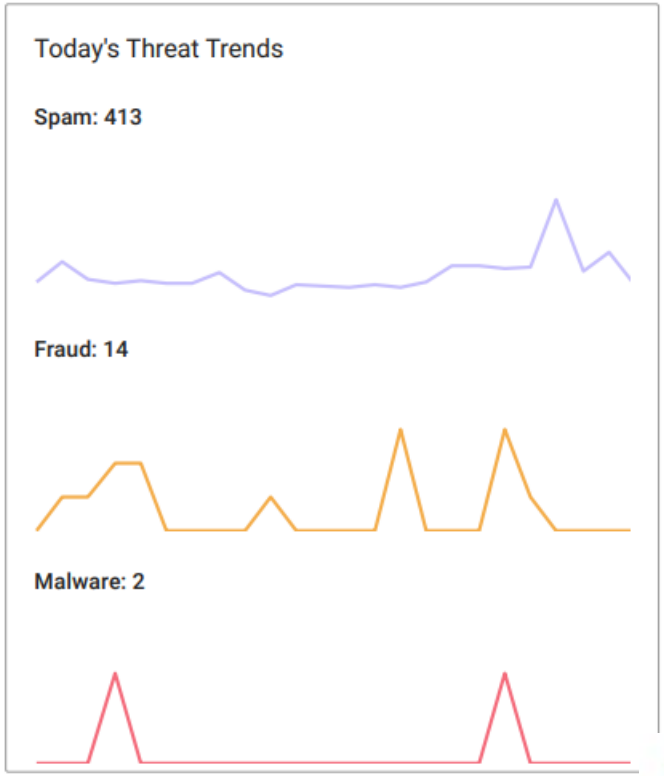
Abbiamo realizzato Smart-IT, l’offerta di servizi IT a supporto della crescita della tua impresa.
Una serie di servizi indispensabili per permetterti di lavorare in serenità, concentrarti sul tuo business e con un team di professionisti sempre al tuo fianco.

Scopri i vantaggi di avere Techsystem come Partner informatico

TD SYNNEX

Parola ad una nostro partner

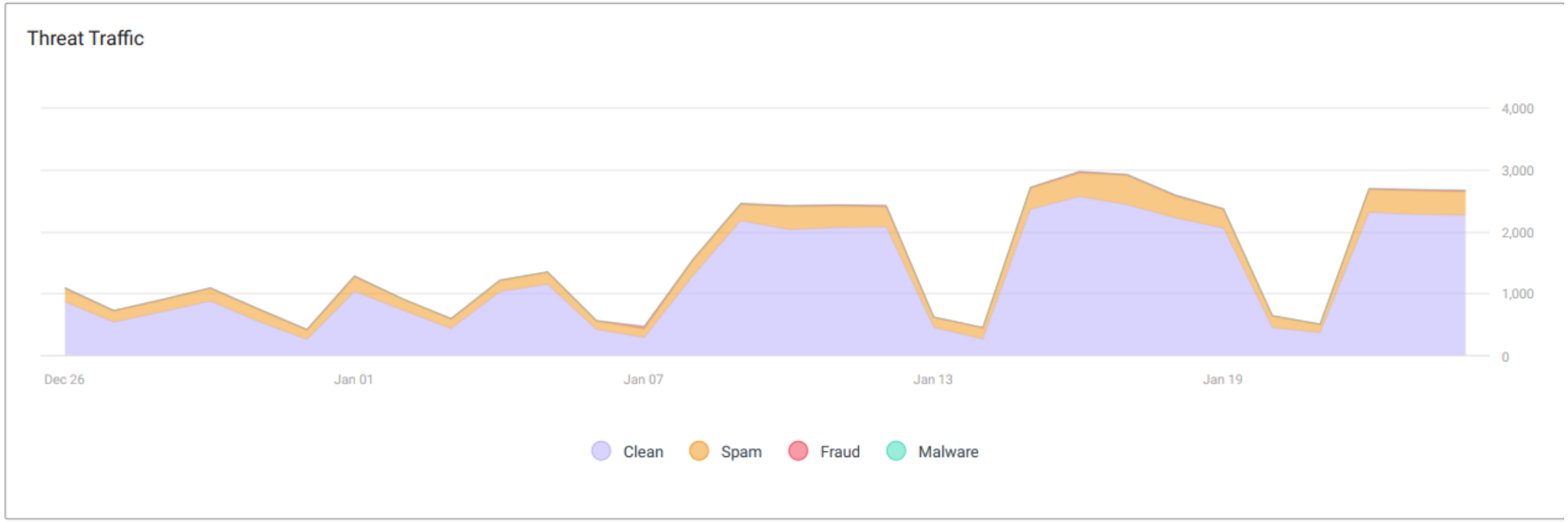




techsystem
Il tuo partner informatico

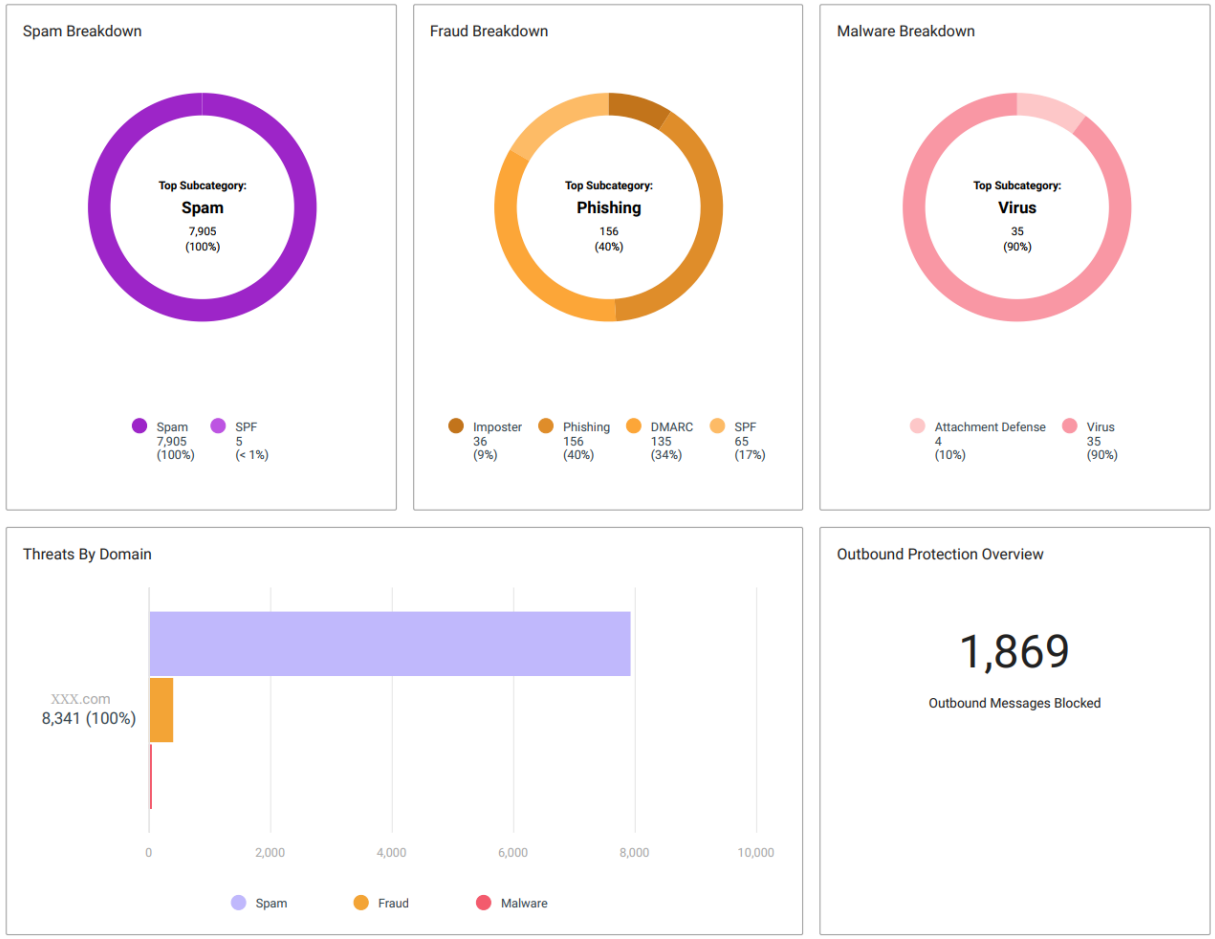
TD SYNNEX

Parola ad una nostro partner



techsystem
Il tuo partner informatico

Parola ad una nostro partner



In 30 giorni:

- Protette 250 caselle
- 60000 messaggi esaminati
- 1869 messaggi bloccati
- 7900 messaggi di Spam
- 156 Messaggi di Phishing
- 35 Messaggi contenenti Virus

TD SYNNEX

“No technology that’s connected to the internet is unhackable”

Abhijit Naskar

https://nis2directive.eu/
https://www.nis-2-directive.com/
https://www.digital4.biz/executive/nis2-cosa-prevede-applicazioni-direttiva-novita/
https://www.wallix.com/unravelling-directive-nis2-and-its-impact-on-european-businesses/
https://www.acn.gov.it/portale/nis/ambito-registrazione
https://www.proofpoint.com/uk/resources/threat-reports/human-factor
https://www.proofpoint.com/us/blog/email-and-cloud-threats
https://www.proofpoint.com/uk/resources/threat-reports/state-of-phish
https://www.proofpoint.com/sites/default/files/pfpt-us-essentials-packages-overview-180807.pdf
https://www.linkedin.com/company/techsystem-srl/posts/?feedView=all

Q&A

PROSSIMI APPUNTAMENTI

24 GENNAIO: Mail security con Proofpoint

31 GENNAIO: Cisco Security

7 FEBBRAIO: Evoluzione delle reti distribuite

TEAM SECURITY: security.it@tdsynnex.com
SPEAKER: andrea.pezzoni@tdsynnex.com