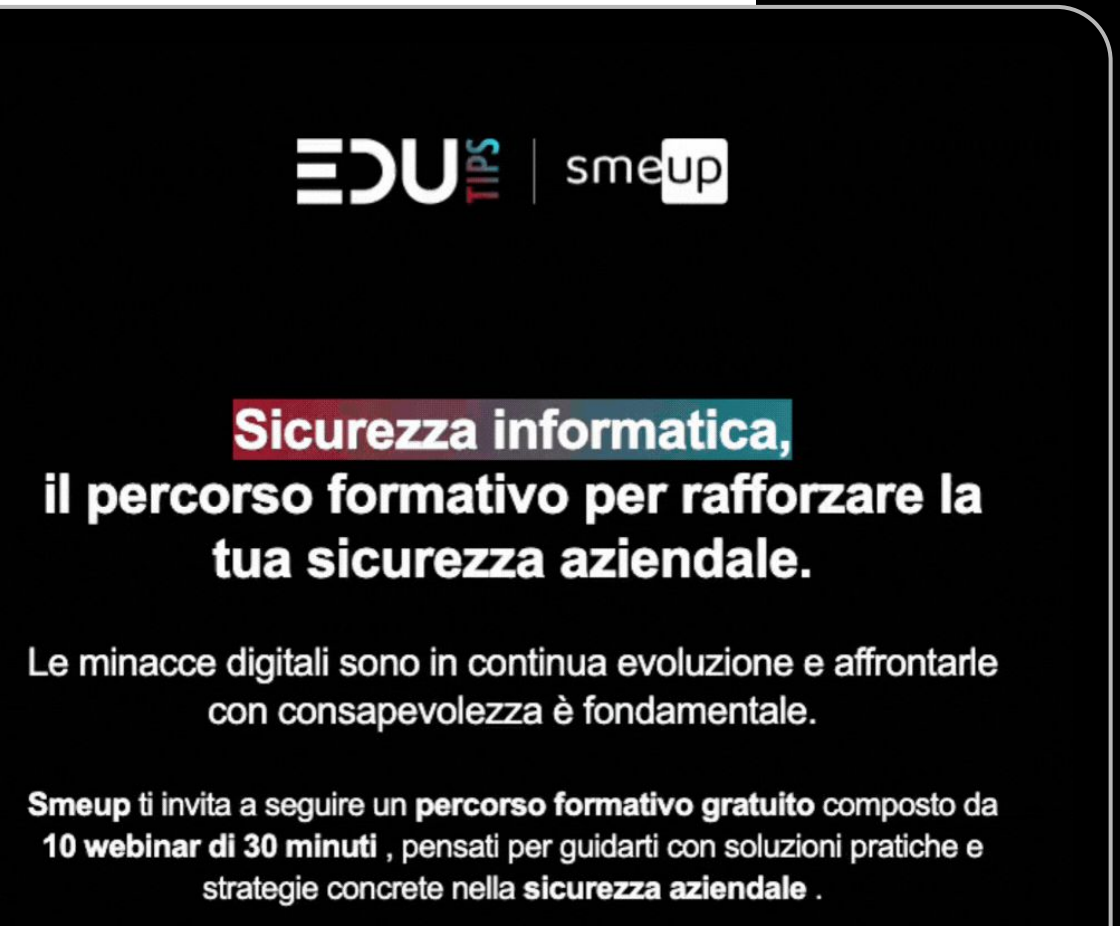
WEBINAR

Cyber Security Awareness

Proteggi te stesso e la tua azienda dagli attacchi informatici

13 FEBBRAIO
2025

EDU TIPS
CYBERSECURITY



EDU TIPS Cybersecurity

10 webinar TIPS - 30 minuti al mese
su tematiche specifiche di Cybersecurity

DATA	DESCRIZIONE
28/1	Mese 1: **Sicurezza dell'infrastruttura**
13/2	**Mese 2: Cyber Security Awareness**
13/3	Mese 3: **Data Protection**
10/4	Mese 4: **Identità e accesso**
13/5	Mese 5: **Cloud security**
12/6	Mese 6: **Incident response**
8/7	Mese 7: **Sicurezza delle applicazioni**
11/9	Mese 8: **Analisi delle minacce e vulnerability assessment**
10/10	Mese 9: **Sicurezza delle reti industriali (OT)**
11/11	Mese 10: **Sicurezza in ambito A.I.**

👉 **SCOPRI DI PIÙ**

EDU TIPS CYBERSECURITY

JESSICA **BARSÀ**

ICS Engineer - Security Specialist *@smeup ICS*

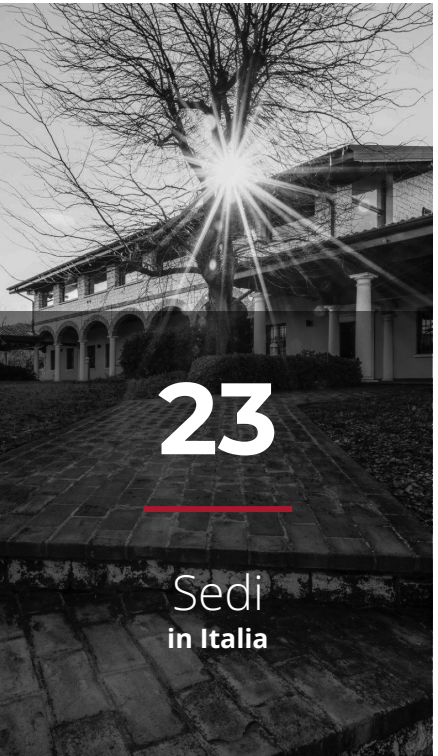
jessica.barsa@smeup.com

COMPANY OVERVIEW

smeup in breve.

COMPANY **OVERVIEW**

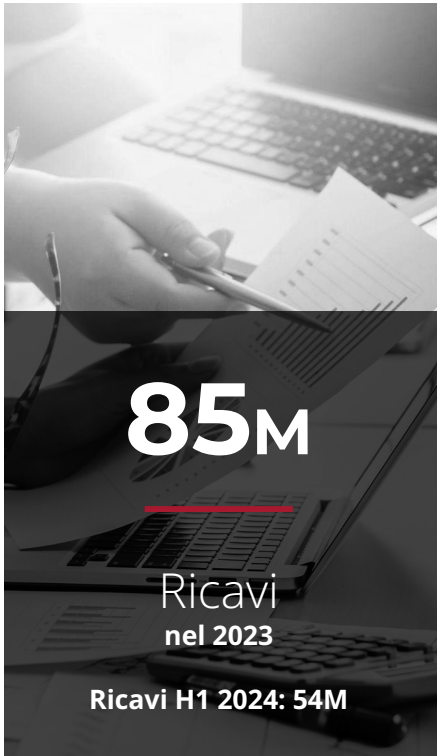
smeup in Numeri



23

Sedi

in Italia



85M

Ricavi

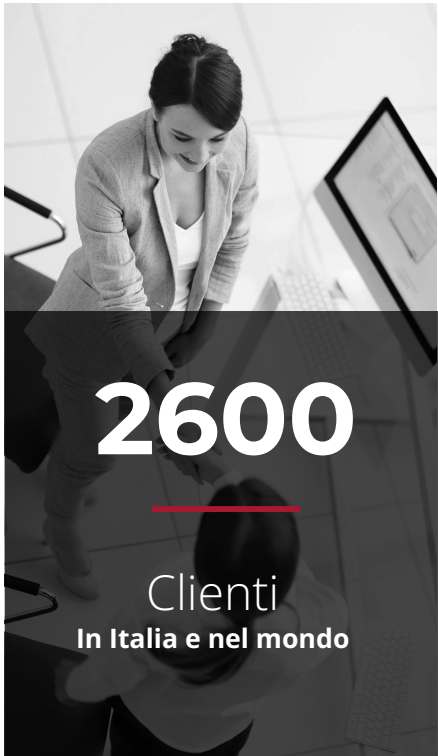
nel 2023

Ricavi H1 2024: 54M

610

Collaboratori

nelle nostre aziende



2600

Clienti

In Italia e nel mondo

BUSINESS SECTOR

BUSINESS SOFTWARE APPLICATION

Soluzioni **Software** per **PMI** e **grandi industrie.**

Ogni azienda è unica. smeup lo sa!
Usare la digitalizzazione per sviluppare il business e generare valore, ***insieme***.

- e GESTIONALI ERP
- r RETAIL
- b BUSINESS ANALYTICS
- d DOCUMENTALE
- w WEB & MOBILE APPLICATION
- h RISORSE UMANE
- p PROGETTAZIONE
- f IOT E INTEGRAZIONE INDUSTRIALE
- l LOGISTICA E TRASPORTI

BUSINESS SECTOR

INFRASTRUCTURE, CLOUD & SECURITY

Soluzioni per **Architetture IT** e **servizi gestiti.**

Innovazione e **sicurezza** per rispondere ai bisogni delle aziende.

- i INFRASTRUTTURA
- c CLOUD
- cs CYBER SECURITY
- ps IBM POWER SYSTEMS

EDU TIPS
CYBERSECURITY

Security Awareness

13 FEBBRAIO
20**25**

SECURITY **AWARENESS**

Cosa si intende per User Awareness?

È la consapevolezza degli utenti rispetto ai temi di sicurezza informatica.

Quali sono i rischi, sia personali che aziendali, di una condotta errata?

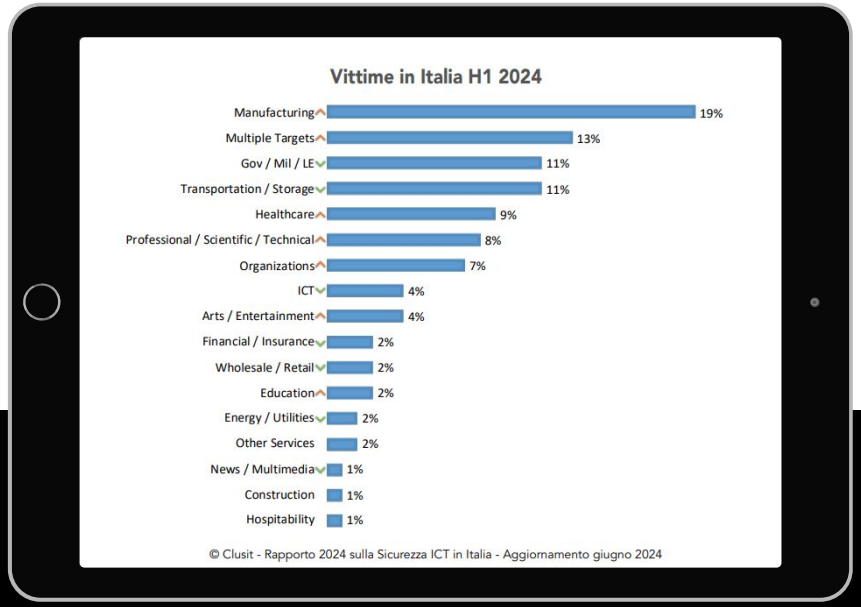
Cosa vogliono gli attaccanti?

Quali sono i metodi usati dagli attaccanti?

Ogni utente gioca un ruolo fondamentale nella sicurezza aziendale.

QUALCHE **DATO**

La situazione attuale.



Clusit – Associazione Italiana per la Sicurezza Informatica – **pubblica ogni anno un report che analizza la situazione della Cybersecurity in Italia.**

01 **CRESCITA DEGLI ATTACCHI**
Gli attacchi cyber nel 2024 sono aumentati del **23%** rispetto al semestre precedente, con 9 attacchi significativi al giorno a livello globale.

02 **IN ITALIA**
Il **7,6%** degli attacchi globali si sono verificati in Italia, con un incremento costante degli incidenti gravi dal 2019 al 2024.

03 **AUMENTO DELLA GRAVITÁ**
Oltre l'**81%** degli attacchi nel 2023 sono stati classificati come critici o gravi, segnalando un peggioramento continuo.

Distribuzione degli attacchi cyber in Italia per settore
Il manifatturiero risulta il settore più colpito, segnalando una vulnerabilità crescente nelle PMI.

RICONOSCI I **RISCHI**

Quali sono le tipologie di attacco?

PHISHING

Attacchi tramite email o messaggi fraudolenti che mirano a ingannare le vittime per ottenere dati sensibili, come credenziali di accesso o numeri di carta di credito.

VOICE/SMS & QR CODE PHISHING

Truffe telefoniche e messaggi ingannevoli che inducono gli utenti a visitare siti pericolosi o a fornire informazioni sensibili tramite codici QR compromessi.

RETI Wi-Fi E SITI NON SICURI

La connessione a reti Wi-Fi non protette e la navigazione su siti web privi di HTTPS possono esporre dati riservati a intercettazioni e attacchi informatici.

CHIAVETTE USB

Dispositivi infetti che, se collegati a computer aziendali, possono diffondere malware o sottrarre informazioni sensibili, compromettendo la sicurezza dei dati.

PIÚ STRATI **PIÚ PROTEZIONE**

La sicurezza informatica è davvero garantita da firewall, EDR e antispam?

Questi strumenti sono fondamentali, ma più livelli di protezione vengono attivati tra utenti e minacce esterne, maggiore sarà la sicurezza. Tuttavia...

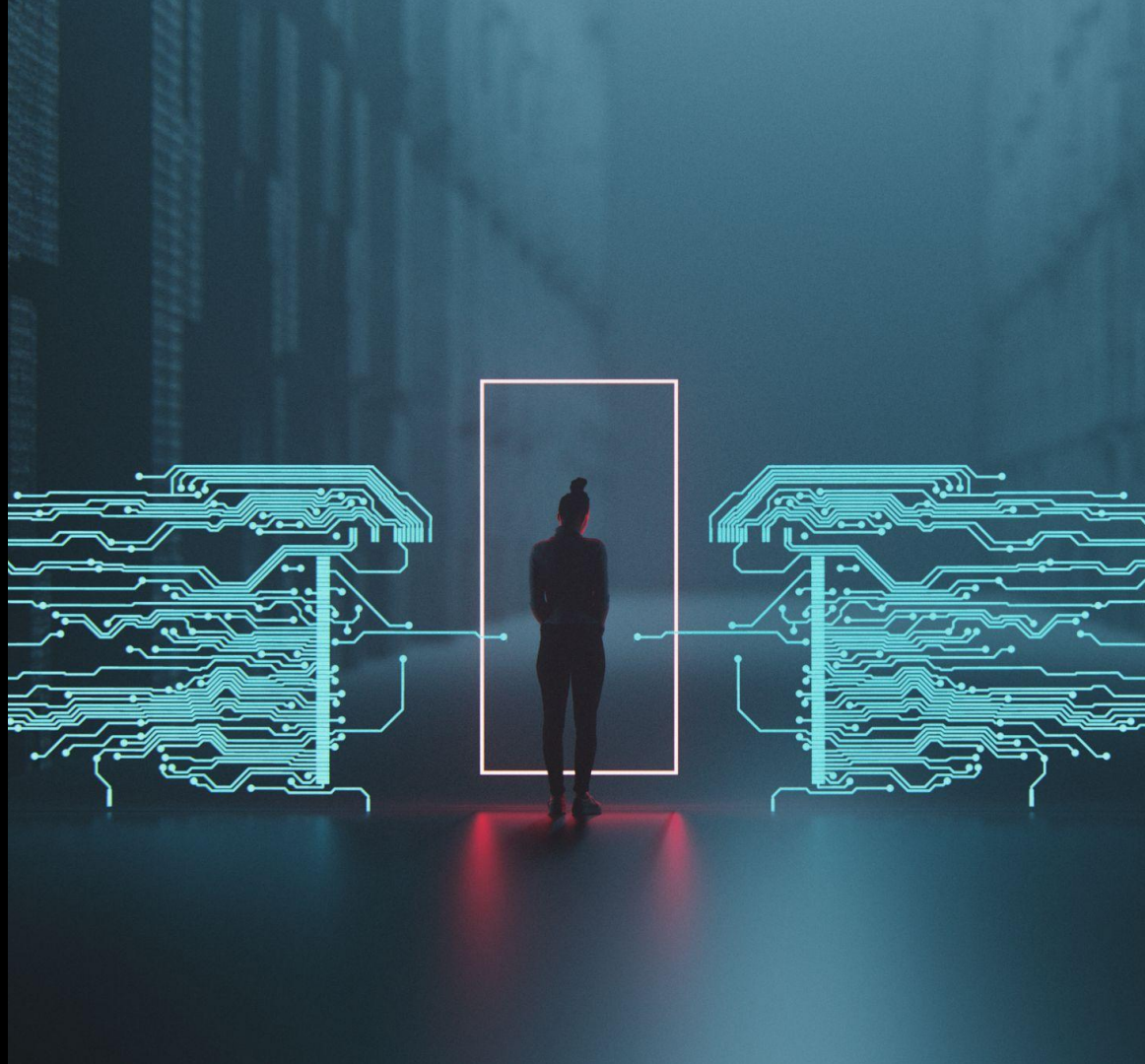
- **Non** tutte le aziende dispongono di tutti gli strati di protezione possibili.
- Molti sistemi possono essere violati tramite attacchi Zero-Day, ossia vulnerabilità non ancora note e vendute sul dark web.
- **Non** tutte le aziende hanno un IT interno in grado di mantenere sempre aggiornati sistemi e applicazioni.
- Alcuni attacchi bypassano del tutto le difese informatiche e colpiscono direttamente gli utenti.

Anche con le migliori tecnologie di cybersecurity, esiste un fattore spesso sottovalutato: il **fattore umano**. Dipendenti e collaboratori rappresentano ancora l'anello più debole nella sicurezza digitale di qualsiasi organizzazione.

E QUINDI...

Human Firewall

L'utente non deve più essere un anello debole, deve diventare uno "Human Firewall". Quando le altre misure di sicurezza sono state superate, è l'utente ad essere il bastione di difesa che **protegge i dati**.



ALLENA LA TUA **SICUREZZA**

Come rendere davvero efficace la formazione?

Non basta un incontro occasionale in una grande sala: la formazione deve essere continua, interattiva e supportata da una misurazione costante.

ALLENA GLI UTENTI

Offri contenuti coinvolgenti come moduli interattivi, video e giochi per migliorare la consapevolezza sulla sicurezza.

METTILI ALLA PROVA

Simula attacchi di phishing automatizzati con template realistici per testare la reattività degli utenti.

ANALIZZA I RISULTATI

Monitora i progressi con report dettagliati su formazione e test di phishing.

La formazione deve essere **coinvolgente** e **accessibile**. Seminari troppo frontali e teorici rischiano di risultare noiosi e controproducenti, spingendo gli utenti a disinteressarsi.

BEST PRACTICE NELLA **FORMAZIONE**

Cosa NON fare!

01

Niente panico!

Informare sui rischi in modo chiaro, senza allarmismi e senza bloccare l’operatività aziendale.

02

NON colpevolizzare

Formare e responsabilizzare, senza creare paura o insicurezza tra i dipendenti.

03

Equilibrio nei training

Evitare il sovraccarico informativo seguito da lunghi periodi senza formazione.

04

Misure proporzionate

Non trattare ogni minaccia come un’emergenza critica: affrontare i rischi in modo equilibrato.

SECURITY AWARENESS E **NIS2**

Un requisito chiave per la conformità

La Direttiva **NIS2** sottolinea l'importanza della formazione e della consapevolezza sulla sicurezza informatica. Non basta implementare misure tecniche: le aziende devono garantire che i dipendenti siano preparati a riconoscere e gestire le minacce.

BEST PRACTICE NELLA **SECURITY AWARENESS**

Creare una cultura della sicurezza efficace.

Quali sono le azioni migliori per proteggere la nostra azienda?

Su cosa dobbiamo realmente focalizzarci?

La security awareness deve essere efficace, chiara e applicabile nella quotidianità, senza creare panico o ostacolare il lavoro. È fondamentale adottare un approccio concreto e consapevole, puntando su poche ma essenziali strategie per ridurre i rischi e migliorare la sicurezza aziendale.

ELEMENTI CHIAVE

- Diffidare dalle **email** sospette e non cliccare su link non verificati.
- Riconoscere i tentativi di **social engineering** e proteggere i dati aziendali.
- Usare **password** sicure e gestirle correttamente.
- Segnalare le **minacce** in modo rapido e responsabile.

Webinar **Edu Tips - Cybersecurity**

Thank you!

JESSICA BARSÀ

ICS Engineer - Security Specialist @smeup ICS

jessica.barsa@smeup.com