smeup

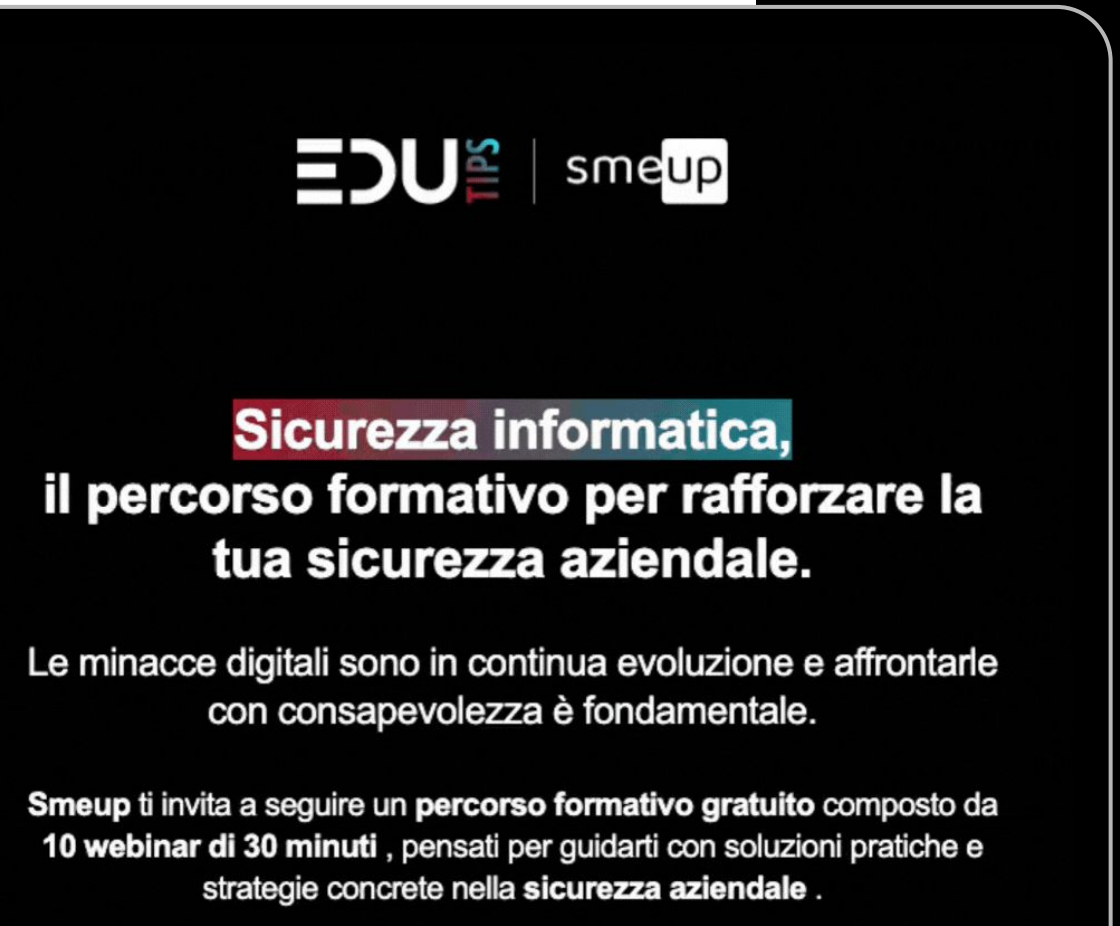
WEBINAR

Identità e accesso

Proteggi gli accessi aziendali con le strategie giuste!

10 APRILE
2025

EDU TIPS
SPECIALE TEMA EDU TIPS



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

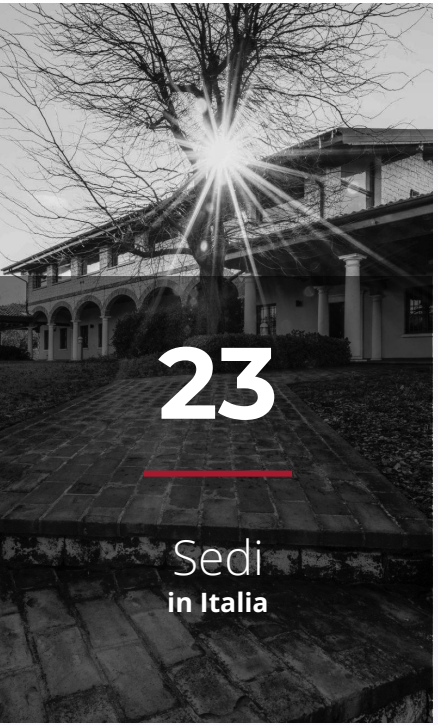
WEBINAR
SPECIALE CYBERSECURITY

SIMONE ZABBERONI

Security Specialist @smeup ICS

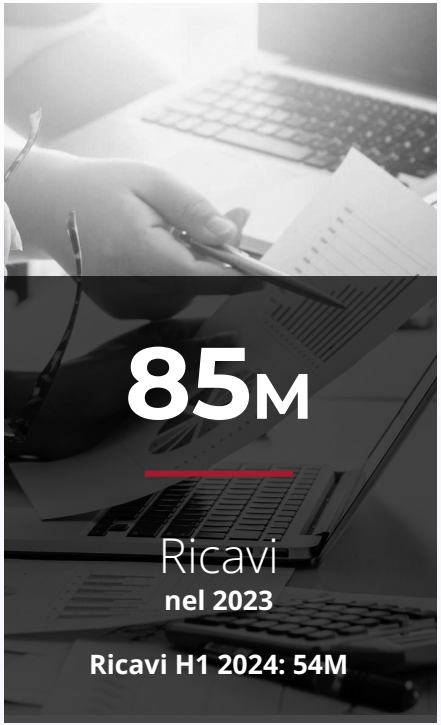
COMPANY **OVERVIEW**

smeup in Numeri.



23

Sedi
in Italia



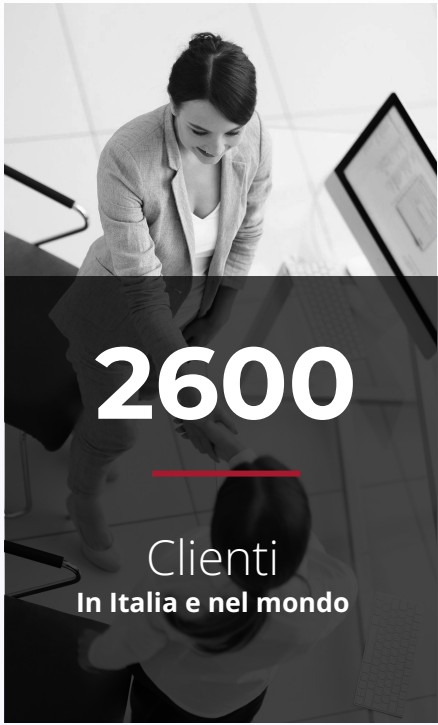
85M

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
- **b** BUSINESS ANALYTICS
- **d** DOCUMENTALE
- **w** WEB & MOBILE APPLICATION
- **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

DIMMI **CHI SEI**

La questione dell'identità.

Proteggere l'identità è il primo passo per garantire la sicurezza informatica!

L'identità digitale è il punto di partenza per garantire l'accesso sicuro ai sistemi.
Ma come si è evoluta nel tempo?

- **Il passato:** in molti contesti l'identità era inesistente o poco strutturata. Si usavano PC senza password, utenti condivisi e dati commisti tra più persone. (*In alcuni ambienti industriali, questa pratica è ancora diffusa per comodità*).
- **L'era di internet:** dagli anni 2000, con l'esplosione dei servizi online, ogni utente si è trovato a gestire decine di account distinti per accedere ai vari servizi.
- **L'evoluzione:** sono nati strumenti come **Single Sign-On (SSO) e Social Login**, che semplificano l'accesso ma centralizzano il rischio: se l'identità primaria viene compromessa, lo saranno anche tutte le identità collegate.
- **Oltre le persone:** oggi non solo gli utenti hanno un'identità digitale, ma anche i dispositivi e i sistemi:
    - **Service account** per l'esecuzione di processi automatizzati
    - **Certificati digitali** per l'autenticazione
    - **Chiavi API** per la comunicazione tra applicazioni

I **PERICOLI**

Il problema dell’identità digitale.

Se un attaccante ruba la tua identità, può accedere a:

Email
VPN
Home banking
Social media

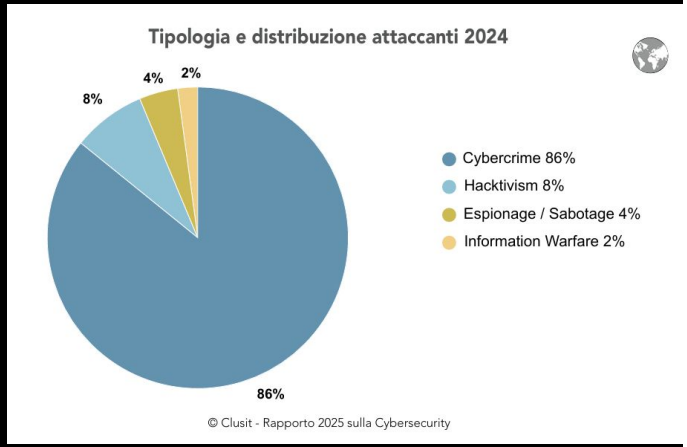
Un accesso aziendale ha un enorme valore, anche se la vittima non ha ruoli di alto livello.

> ***Cosa può fare un attaccante con il tuo account email?***

- **Rubare dati sensibili**
- **Forgiare documenti**
- **Cambiare credenziali di altri account**
- **Clonare l’MFA**
- **Sfruttare il social engineering per attaccare colleghi**

Anche gli account personali sono una porta d’ingresso verso l’azienda. E se non bastasse, possono essere venduti per truffe e frodi di vario tipo!

Proteggere la propria identità digitale significa proteggere tutto il proprio ecosistema!



LA SITUAZIONE DELLA **CYBERSECURITY**

Il Rapporto Clusit 2025.

PHISHING E CREDENTIAL THEFT IN AUMENTO

71,7%

Il Credential Phishing rappresenta la minaccia più diffusa delle attività malevole analizzate.

Fonte: Rapporto Clusit 2025 (Fastweb)

+35%

crescita degli incidenti in Italia basati su phishing e ingegneria sociale tra il 2023 e il 2024.

Fonte: Rapporto Clusit 2025

TREND GENERALI DEGLI ATTACCHI

+27,4%

Nel 2024, il numero di incidenti rilevati è aumentato del 27,4%, passando da 2.779 a 3.541.".

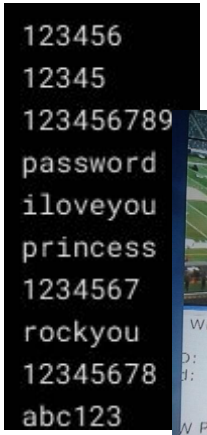
Oltre alla crescita costante degli attacchi, è **peggiorata anche la gravità degli incidenti**: l'indice di Severity Media è aumentato ogni anno negli ultimi cinque anni, amplificando i danni subiti.

Fonte: Rapporto Clusit 2025

PASSWORD

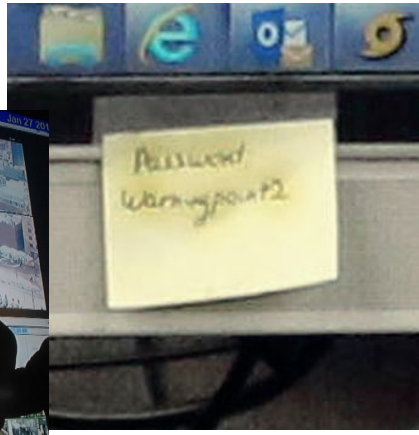
“Ma perchè siamo messi così?”

Le **password,** anche se usate bene, **da sole non bastano**! Ma almeno le usiamo correttamente?



Elenco password "rockyou" da Kali Linux

[Fonte]



[Fonte]

BEST PRACTICE PER LE **PASSWORD**

I “soliti” consigli.

I CONSIGLI FONDAMENTALI

Lunghezza
Più una password è lunga, più è resistente ad attacchi.

Complessità
Usa caratteri speciali, numeri e lettere maiuscole/minuscole. *Es. "Password1!" è facilmente violabile.*

No al riutilizzo
Ogni password deve essere unica per ogni servizio. Riutilizzare le password aumenta enormemente il rischio di attacco.

COSA EVITARE

Non salvare le password nei browser
Sono le prime informazioni rubate dai malware *"stealer".*

Niente fogli Excel o post-it
Il file *“password.xls”* sulla NAS è una pessima idea!

ALTERNATIVE PIÙ SICURE

Passphrase
Frasi lunghe e memorabili, es.: Ma!Che!Bel!Castello! L1N2A3I4C5P6S7 *(tratto da "La nebbia agli irti colli...")*

Password Manager
Per archiviare e gestire password complesse in modo sicuro. Proteggi il tuo password manager con una passphrase robusta e MFA.

ATTACCHI **BRUTE FORCE**

Quanto tempo ci vuole?

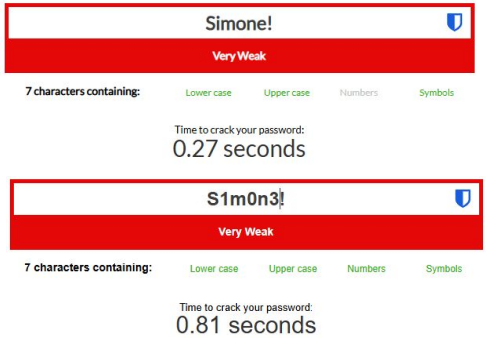
TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

HIVE SYSTEMS

› Learn how we made this table at **hivesystems.io/password**

Fonte: hivesystems.io/password



Fonte: passwordmonster.com

PIÙ' SICUREZZA **PER LA TUA IDENTITÀ'**

La Multifactor Authentication.

Anche con password ben gestite, gli attacchi sono sempre possibili. La soluzione? Aggiungere più fattori di verifica!

I tre fattori di autenticazione:

01 **QUALCOSA CHE CONOSCI**
Password, PIN

02 **QUALCOSA CHE HAI**
Telefono, token fisico

03 **QUALCOSA CHE SEI**
Impronta digitale, FaceID, riconoscimento vocale

Più fattori = più sicurezza!
2FA → Usa due fattori
MFA → Usa più fattori

QUALI **FATTORI?**

Non tutte le MFA sono uguali!

SICUREZZA	METODO	RISCHI
Bassa	📧 Codici via email	Facile da intercettare (phishing, compromissione email).
Bassa	📲 Codici via SMS	Vulnerabile a SIM swap, attacchi MITM, malware.
Media	📱 App di autenticazione (TOTP)	Es. Google Authenticator, Microsoft Authenticator. Generano codici offline, più sicuri degli SMS.
Media	🔔 OTP via notifica push	Es. Microsoft Authenticator, Watchguard AuthPoint. Meno rischio di phishing rispetto agli SMS.
Alta	🔑 Chiavi di sicurezza hardware (FIDO2/U2F)	Es. YubiKey, Google Titan. Non clonabili, richiedono un dispositivo fisico.
Alta	🌐 Passkey/WebAuthn	Basate su crittografia asimmetrica, legate a dispositivi affidabili (iPhone, Android, PC, chiavette).
Alta	🆔 Autenticazione biometrica	Es. Face ID, Windows Hello. Basata su caratteristiche uniche dell'utente.

✅ Maggiore sicurezza = Minore rischio di compromissione!

ACCESSO **CONDIZIONALE**

Controllo basato sul contesto.

I moderni Identity Provider supportano logiche di accesso condizionale che permettono di affinare il controllo sulle identità in base al contesto.

SITUAZIONE	REGOLA DI ACCESSO
📍 Accesso dall'Italia	Richiesta di **password + Authenticator**
🌙 Di notte o nel weekend	Richiesta di **password + passkey hardware**
🚫 Da paesi in blacklist (es. Russia, Cina)	**Accesso bloccato** senza verificare l'identità
✈️ Da altri stati esteri	Richiesta di **password + passkey hardware**

✅ Risultato:
Maggiore sicurezza e minore rischio di accessi fraudolenti!

ZERO **TRUST**

Never trust, always verify

- In situazione normale, un login rende implicitamente accessibili troppe risorse e senza verifiche ulteriori per tutto il tempo della sessione *(es: login MS, VPN).*
- Un approccio Zero Trust impone controlli più granulari e continui, che rispondano dinamicamente al contesto

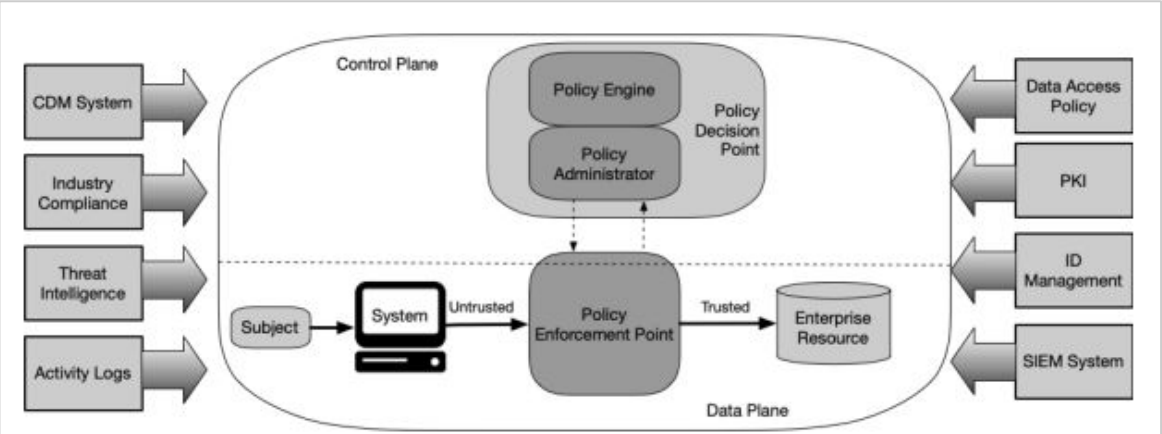


Figure 2: Core Zero Trust Logical Components

Fonte

DOVE **APPLICARLA**

Ambito di applicazione MFA e NIS2.

Cosa dice la direttiva NIS2?

Non specifica un tipo di MFA obbligatorio, ma richiede misure di sicurezza adeguate per proteggere le identità digitali.

Impone l'uso di MFA "ove appropriato" nei settori critici, ovvero in qualsiasi ambito in cui l'assenza di MFA possa portare a una violazione informatica.

APPLICAZIONE IDEALE

- **MFA ovunque:** in teoria, ogni accesso dovrebbe essere protetto.
- **Limitazioni:** alcuni sistemi potrebbero non supportarla o comportare costi elevati di implementazione e gestione.
- **Criterio di proporzionalità:** un risk assessment aiuta a identificare i punti critici che richiedono MFA.

DOV'È INDISPENSABILE LA MFA?

- **Email aziendale e personale**
- **VPN e accessi da remoto**
- **Portali bancari**
- **Servizi cloud** (Google Drive, OneDrive, SharePoint)
- Qualsiasi sistema che, se compromesso, possa essere sfruttato per un attacco più ampio

Come avvengono gli attacchi?

ATTACCHI ALLE PASSWORD

- Acquisto di credenziali sul dark web
- Brute force (tentativi automatici di indovinare la password)
- Credential stuffing (uso di credenziali rubate su più servizi)

ATTACCHI AGLI UTENTI

- Social engineering diretto (manipolazione psicologica)
- Phishing avanzato (es. attacchi basati su AI)
- Deepfake (uso di video/audio falsificati per ingannare gli utenti)
- Malware e stealer (software malevoli che rubano credenziali)

ATTACCHI AI SISTEMI MFA

- SIM swapping (furto del numero di telefono per intercettare codici SMS)
- MFA Fatigue (bombardamento di notifiche push per far cedere l'utente)
- EvilNGINX (attacchi di phishing avanzati per rubare sessioni di autenticazione)

CONSAPEVOLEZZA, **NON SOLO TECNOLOGIA**

L’MFA NON è infallibile!

Gli attaccanti trovano sempre nuovi modi per aggirare i controlli o ingannare gli utenti.
L’MFA è un grande aiuto ma NON RISOLVE TUTTO!

Cosa fare?

USER AWARENESS

La formazione degli utenti è fondamentale!

GOOD PRACTICES

MFA va implementata correttamente, senza abbassare la guardia.

OBIETTIVO

Ridurre il rischio e rendersi meno “appetibili” per gli attaccanti.

ESEMPI **DI ATTACCO**

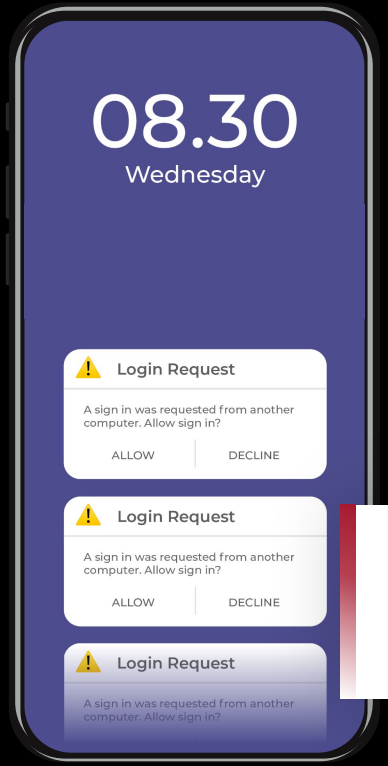
Strumenti “anti-MFA”

evilenginx 3.0

ESEMPI **DI ATTACCO**

Strumenti “anti-MFA”

MFA fatigue



COME FUNZIONA?

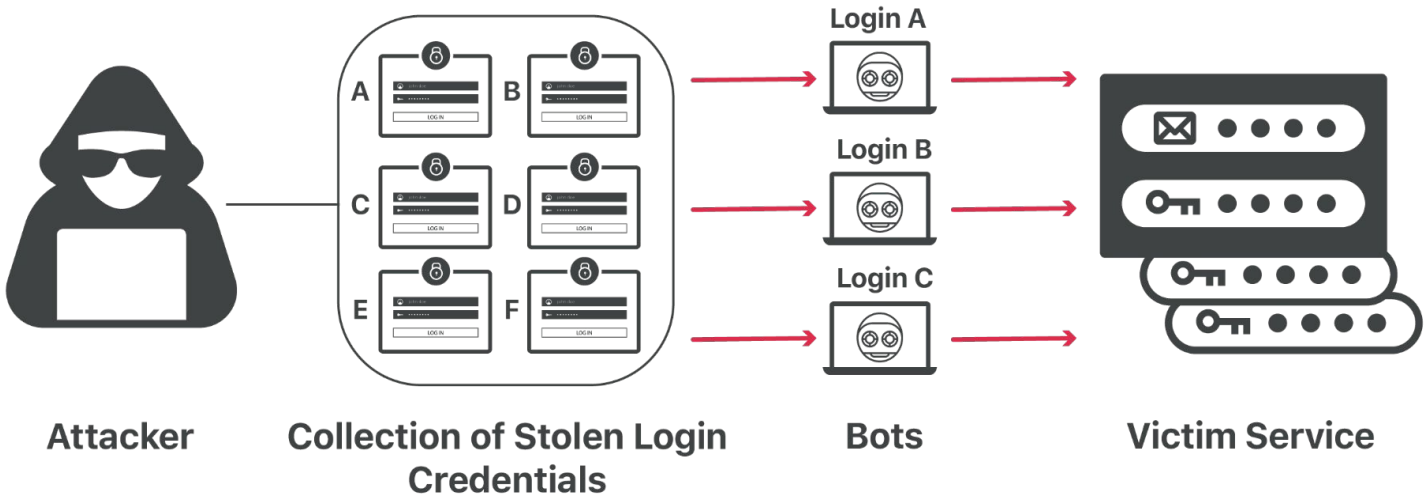
01 L’attaccante invia decine di richieste MFA push all’utente.

02 Alla lunga, per errore o stanchezza, l’utente accetta.

È un attacco semplice ma efficace, soprattutto se l’utente non è formato.

ESEMPI **DI ATTACCO**

Strumenti “anti-MFA”



BEST PRACTICE **GENERALI**

La sicurezza delle identità.

PASSWORD SICURE

- Non riutilizzarle
- Scegli password robuste

PASSWORD MANAGER

- Ricorda le credenziali per te
- Indispensabile per email e VPN

MFA SEMPRE

- Usa dove possibile
- Meglio con passkey o chiavi fisiche

FORMA GLI UTENTI

- Riconoscere phishing e truffe
- Difendersi dai social attack

MONITORA GLI ACCESSI

- Servono alert in tempo reale
- Individua violazioni subito

ACCESSO CONDIZIONATO

- Controlli basati su luogo, orario, device
- Blocca comportamenti anomali


EDU TIPS
Q&A

smeup

smeup.com

Thank you!

SIMONE **ZABBERONI**

Security Specialist - smeup ICS

simone.zabberoni@smeup.com

EDU TIPS CYBERSECURITY