
DARKWEB ID

# Frequently Asked Questions

## Cos'è il Dark Web?

Il **Dark Web** è un vero e proprio universo nascosto all'interno del "Deep Web", un sottoinsieme di Internet **non raggiunto dai normali motori di ricerca**.

I motori come Google, Bing e Yahoo infatti indicizzano solamente lo 0,4% di Internet, l'equivalente della parte della Rete che appare in superficie. Il restante 99,96% del Web è composto da database, reti private, accademiche e governative, nonché dal Dark Web. Si calcola **che il Dark Web sia 550 volte più grande rispetto al Web visibile** e che le sue dimensioni siano in continua espansione.

Dal momento che è possibile muoversi al suo interno in modo del tutto anonimo, il **Dark Web è il contenitore di un'enormità di dati rubati e teatro di attività illecite**.

## Come può contribuire Dark Web ID a proteggere la mia azienda?

**Dark Web ID** è studiato per aiutare i clienti del settore pubblico e di quello privato a **intercettare e mitigare le cyberminacce** che sfruttano la **sottrazione di password e indirizzi email**.

Dark Web ID fa leva su una combinazione di intelligenza umana e artificiale che setaccia botnet, chat room criminali, blog, siti Web, bulletin board, reti Peer-to-Peer, forum, reti private e altri siti appartenenti al mercato nero **lavorando 24 ore per 7 giorni su 7, 365 giorni all'anno** allo scopo di identificare credenziali e altre informazioni personali sottratte.

## Come si riescono a trovare sul dark web le credenziali rubate o comunque esposte?

Gli esperti di Dark Web ID tengono **sotto controllo il Dark Web** e il sottobosco degli hacker criminali per rilevare l'esposizione ai malintenzionati delle credenziali dei clienti.

Raggiungono questo obiettivo dedicandosi **alla ricerca dei domini email di primo livello dei clienti**.

Una volta identificata una credenziale, la mettono da parte.

Anche se raccolgono dati dai tipici siti usati dagli hacker come Pastebin, gran parte delle loro informazioni derivano da **siti che permettono l'accesso solamente a chi è iscritto** o chi possiede una certa credibilità nella comunità hacker.

A tal fine monitorano oltre 500 canali IRC (Internet Relay Chat), 600.000 siti Web privati, 600 feed Twitter, ed eseguono quotidianamente 10.000 query specifiche.

## Il ritrovamento di credenziali esposte significa che si è stati presi di mira dagli hacker?

Per quanto non si possa affermare con sicurezza che i dati ritrovati siano già stati adoperati per colpire il cliente, il fatto di essere riusciti a **identificarne le credenziali dovrebbe essere fonte di seria preoccupazione**.

Le aziende dovrebbero rivolgersi al proprio servizio IT e/o team della sicurezza interno o esterno per determinare la possibile esistenza di un cyberincidente o di una violazione dei dati.

## Dove sono state trovate le informazioni?

La provenienza delle informazioni trovate nel Dark Web **può essere di varia natura**. In particolare la provenienza può essere classificata **sotto queste categorie**:

- **Dark Web Chatroom**: dati scoperti in un canale IRC nascosto;
- **Hacking Site**: dati presenti su un sito Web controllato da hacker o su un sito usato come data dump per immagazzinare grandi quantità di informazioni;
- **Hidden Theft Forum**: dati pubblicati all'interno di un forum o di una community di hacker;
- **P2P File Leak**: dati rilasciati da una rete o da un programma di file sharing Peer-to-Peer;
- **Social Media Post**: dati pubblicati su una piattaforma di social media;
- **C2 Server/Malware**: dati raccolti per mezzo di botnet o su un server C2C (Command and Control).

## Alcuni di questi dati sono obsoleti e riguardano dipendenti che non lavorano più con noi. Questo vuol dire che non corriamo rischi?

Anche se le persone possono essere uscite dall'azienda, **le relative credenziali potrebbero essere ancora attive e valide su sistemi di terze parti** utilizzati nel corso della loro permanenza nell'organizzazione.

In molti casi, i database e i sistemi di terze parti che sono stati compromessi esistono da oltre 10 anni e contengono milioni di account “zombie” che possono essere sfruttati per colpire un'azienda.

La scoperta di credenziali associate a ex-dipendenti dovrebbe costituire una **buona occasione per verificare l'avvenuta rimozione di qualsiasi account** interno o di terze parti che potrebbe essere adoperato per un attacco.

## Come hanno fatto i dati ad essere rubati o compromessi?

Qual è il meccanismo con cui i dati sono stati sottratti o compromessi? Come avviene il furto dei dati aziendali?

Questo è un elenco dei possibili metodi utilizzati per sottrarre i dati alle aziende:

- **Tested**: i dati compromessi sono stati oggetto di test per determinarne l'attuale validità;
- **Sample**: i dati compromessi sono stati pubblicati per provarne la validità;
- **Keylogged or Phished**: i dati compromessi sono stati inseriti in un sito fittizio o estratti mediante software realizzato per sottrarre informazioni personali;
- **3rd Party Breach**: i dati compromessi derivano da una violazione dei dati interni o di un sito di terze parti;
- **Accidental Exposure**: i dati compromessi sono stati pubblicati per errore su un sito Web, sui social media o su un sito Peer-to-Peer;
- **Malicious / Doxed**: i dati compromessi sono stati diffusi intenzionalmente per rendere pubbliche le informazioni personali.

## Cosa significa Password Criteria?

Password Criteria **permette a te o ai tuoi clienti di identificare criteri associati alle password** di rete allo scopo di assegnare un livello di allarme superiore in caso di diffusione di credenziali che rispettano le caratteristiche indicate.

I criteri selezionabili sono lunghezza minima, numero di lettere, numeri, caratteri speciali e di punteggiatura, e lettere maiuscole.

## Cosa significa quando una password è formata da una lunga serie casuale di numeri e lettere?

Questo indica che della password **è stata pubblicato solamente il relativo "hash"** (e quindi la password è ancora cifrata). Sul Web sono reperibili centinaia di dizionari crittografici, e **non è insolito che queste password vengano "craccate"** o decifrate per diventare disponibili su svariati siti.

## Ho notato che ci sono indirizzi email fasulli (falsi positivi). Perché sono importanti?

Account di posta elettronica fasulli vengono regolarmente creati dai dipendenti come caselle "usa e getta" quando desiderano accedere a un certo sistema o a un'informazione. Tuttavia, gli account fasulli sono **spesso creati anche per facilitare azioni di social engineering e/o attacchi di phishing**.

L'identificazione di account di posta fasulli indica che nel passato l'azienda è stata oggetto di attenzioni indesiderate da parte di singoli o gruppi.

## Le password identificate non rispondono ai nostri criteri di rete. A cosa serve questa indicazione?

Se nel report appaiono password semplici e i criteri di complessità in uso nella rete sono più restrittivi, il cliente può essere portato a pensare di essere al sicuro.

Questo in realtà non è vero perché esistono diversi modi (anche automatici, come i framework di Metasploit) per complicare la password non sicura in un attacco brute force.

Gli utenti sono infatti spesso portati a utilizzare la stessa tipologia di password (o addirittura riciclarle) per le proprie credenziali personali e di lavoro, variando o aggiungendo solo alcuni caratteri per rispettare i criteri di complessità.

Se la policy interna richiede una lettera maiuscola e un carattere speciale o di punteggiatura, è facile che l'utente scelga una password che già usa, aggiungendoci una maiuscola e un punto esclamativo. Ad esempio, per una password esposta "cowboys", le variazioni più probabili saranno "Cowboys!", "Cowboys1", "Cowboys!1" e così via.

Inoltre, se la password esposta è la data di nascita, è facile per un attaccante partire da quella aggiungendo altri caratteri prima o dopo per trovarne una più complicata che usi la data come punto di partenza, riducendo il tempo necessario a indovinare la password completa.

Gli hacker hanno ben presenti questi comportamenti, quindi utilizzano script ad hoc per coprire più varianti possibili e ottenere l'accesso ai sistemi.

## Ho visto che nello stesso giorno compaiono più utenti con la medesima password. Cosa significa?

Nella maggior parte dei casi è l'indicazione **che qualcuno sta provando ad abbinare una medesima password a una serie di utenti differenti** per verificare la possibilità di accedere a un sistema.

## Qual è la differenza tra un utente Standard e uno Privilegiato?

L'utente Standard non può visualizzare le password.

## Posso tenere sotto controllo anche account di posta personali?

Oltre a tutti gli indirizzi che ricadono all'interno del dominio dell'azienda, è possibile **monitorare anche un massimo di 5 indirizzi email** personali per azienda.

## Esiste qualche best practice per gli utenti o l'IT aziendale relativa alla frequenza con cui modificare le password o gli indirizzi di posta personali o professionali?

A questo proposito, si consiglia la lettura del documento Special Publication 800-63B Digital Identity pubblicato dal National Institute of Standards and Technology (NIST) e consultabile all'indirizzo: *https://pages.nist.gov/800-63-3/sp800-63b.html*

Per una best practice operativa di sicurezza elevata, è possibile consultare i criteri password applicati dalla NASA: *https://www.grc.nasa.gov/its-training/best-practices/password-rules/*

Le best practice per le regole riguardanti le password sono comunque in continua evoluzione, quindi si consiglia di rivedere i criteri periodicamente.

## Si può dire che lo storage in cloud sia a serio rischio di violazioni dei dati? Ora che la maggior parte dei nostri strumenti software sta andando sul cloud, la proprietà intellettuale della mia azienda è a rischio più di prima?

I dati residenti all'interno di un ambiente Cloud **sono a rischio tanto quanto quelli che sono mantenuti localmente sui server di proprietà**.

Nella scelta dei provider di Cloud e data center, assicuratevi di verificare per bene le relative certificazioni e conformità agli standard e ai protocolli di sicurezza internazionali in vigore nel vostro settore di attività.

## I dati personali eventualmente trovati nel Dark Web possono essere rimossi?

Una volta che i dati vengono messi in vendita nel Dark Web, le informazioni sono rapidamente copiate e distribuite (rivendute o scambiate) a un grande numero di cybercriminali entro un intervallo di tempo molto breve.

È generalmente **impraticabile pensare di rimuovere dati** che siano stati disseminati all'interno del Dark Web.

## Per investigare nel dark web occorrono credenziali particolari?

Per entrare nel deep Web o Dark Web non servono permessi speciali. Tuttavia, l'accesso a questi ambienti richiede l'utilizzo di un **browser "TOR" e dovrebbe essere effettuato esclusivamente attraverso un tunnel VPN cifrato**.

In generale sconsigliamo di provare ad accedere al Dark Web.