

Glossario

Accesso

Processo di accesso dell'utente, p. es. per utilizzare un dispositivo o un servizio online. Solitamente questa procedura serve a comunicare al sistema che ha inizio una sessione e che l'utente desidera collegarsi a un account, come il proprio account per il sistema di e-banking.

Vedi anche: [Uscita \(https://www.ebas.ch/it/glossary/uscita-logout/\)](https://www.ebas.ch/it/glossary/uscita-logout/), [Autenticazione \(https://www.ebas.ch/it/glossary/autenticazione/\)](https://www.ebas.ch/it/glossary/autenticazione/)

Advanced Encryption Standard (AES)

Metodo di crittografia dei dati. Il sistema AES può essere utilizzato p. es. per crittografare i dati trasmessi in una rete WLAN (WPA2, WPA3), cifrando tutto ciò che viene scambiato tra il router WLAN e un dispositivo collegato senza fili.

Vedi anche: [Wi-Fi Protected Access \(WPA\) \(https://www.ebas.ch/it/glossary/wi-fi-protected-access-wpa-wpa2-wpa3/\)](https://www.ebas.ch/it/glossary/wi-fi-protected-access-wpa-wpa2-wpa3/), [Wireless Local Area Network \(WLAN\) \(https://www.ebas.ch/it/glossary/wireless-local-area-network-wlan-wi-fi/\)](https://www.ebas.ch/it/glossary/wireless-local-area-network-wlan-wi-fi/)

Adware

Termine composto dalle parole inglesi «advertisement» (pubblicità) e «software» che identifica quei programmi che oltre a svolgere le proprie funzioni mostrano all'utente annunci pubblicitari o installano altro software per visualizzarli.

Vedi anche: [Malware \(https://www.ebas.ch/it/glossary/malware-software-dannoso/\)](https://www.ebas.ch/it/glossary/malware-software-dannoso/)

Aggiornamento

Piccola attualizzazione di un programma che spesso risolve i bug (errori) di un software. La maggior parte delle aggiornamenti viene distribuita dai produttori di software tramite download gratuito dai loro siti Internet oppure in modo automatico.

Vedi anche: [Patch \(https://www.ebas.ch/it/glossary/patch/\)](https://www.ebas.ch/it/glossary/patch/), [Upgrade \(https://www.ebas.ch/it/glossary/upgrade/\)](https://www.ebas.ch/it/glossary/upgrade/)

American Standard Code for Information Interchange (ASCII)

Codifica di caratteri contenente 95 caratteri stampabili e 33 caratteri non stampabili. I caratteri stampabili comprendono le lettere dell'alfabeto latino (A-Z, a-z), le dieci cifre arabe (0-9), alcuni segni di interpunzione e altri caratteri speciali.

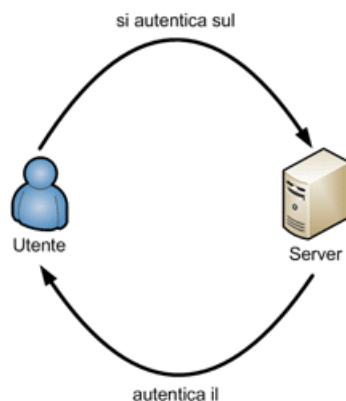
Vedi anche: [Unicode \(https://www.ebas.ch/it/glossary/unicode/\)](https://www.ebas.ch/it/glossary/unicode/)

Applicazioni di desktop remoto e terminal server (RDP)

Applicazioni che consentono agli utenti di utilizzare sistemi informatici in remoto. Lo scopo primario è quello di trasportare la visualizzazione dello schermo, gli input della tastiera e i movimenti del mouse attraverso distanze notevoli tra il sistema e l'utente.

Autenticazione

Procedura di verifica dell'identità dichiarata da una persona o da un dispositivo per mezzo di una o più specifiche caratteristiche (p. es. password, tessera dotata di chip o impronta digitale).



Vedi anche: [Autorizzazione \(https://www.ebas.ch/it/glossary/autorizzazione/\)](https://www.ebas.ch/it/glossary/autorizzazione/), [Autenticazione a doppio fattore \(2FA\) \(https://www.ebas.ch/it/glossary/autenticazione-a-doppio-fattore-2fa/\)](https://www.ebas.ch/it/glossary/autenticazione-a-doppio-fattore-2fa/)

Autenticazione a doppio fattore (2FA)

Con la cosiddetta autenticazione a doppio fattore, quando viene effettuato il login viene chiesto di utilizzare, oltre al primo elemento di sicurezza (solitamente una password), anche un secondo elemento di sicurezza indipendente dal primo. Può trattarsi, p. es., di un codice che viene inviato a un telefonino o che viene generato su uno smartphone.

Vedi anche: [Accesso \(https://www.ebas.ch/it/glossary/accesso-login/\)](https://www.ebas.ch/it/glossary/accesso-login/), [Autenticazione \(https://www.ebas.ch/it/glossary/autenticazione/\)](https://www.ebas.ch/it/glossary/autenticazione/)

Autenticazione a più fattori (MFA)

L'autenticazione a più fattori è una procedura di sicurezza in cui l'identità di un utente viene verificata combinando diversi fattori slegati tra loro, quali ad esempio una password, la scansione di codici QR o le caratteristiche biometriche. L'uso dell'MFA riduce il rischio di accessi non autorizzati, in quanto un utente malintenzionato dovrebbe superare diversi ostacoli separati per accedere. La forma più comune di MFA è l'autenticazione a due fattori (2FA).

Vedi anche: [Autenticazione \(https://www.ebas.ch/it/glossary/autenticazione/\)](https://www.ebas.ch/it/glossary/autenticazione/), [Autenticazione a doppio fattore \(2FA\) \(https://www.ebas.ch/it/glossary/autenticazione-a-doppio-fattore-2fa/\)](https://www.ebas.ch/it/glossary/autenticazione-a-doppio-fattore-2fa/)

Autorizzazione

Conferimento di credenziali. Con le credenziali viene dato il permesso di accedere a determinate risorse (p. es. file, software, pagamenti ecc.) una volta effettuate un'identificazione e un'autenticazione corrette.

Vedi anche: [Autenticazione \(https://www.ebas.ch/it/glossary/autenticazione/\)](https://www.ebas.ch/it/glossary/autenticazione/)

Backdoor

Termine inglese che significa «porta sul retro». Nel contesto del software significa solitamente un accesso non documentato che permette al produttore (o a terzi) di accedere dall'esterno al software stesso oppure ai dati dell'utente.

Vedi anche: [Malware \(https://www.ebas.ch/it/glossary/malware-software-dannoso/\)](https://www.ebas.ch/it/glossary/malware-software-dannoso/)

Backup

Salvataggio dei dati con il quale si copiano informazioni elettroniche (dati) su un supporto di memorizzazione esterno (p. es. un disco rigido esterno). Solitamente i backup vengono eseguiti secondo un calendario regolare.

Banche online

Le banche online offrono i loro prodotti esclusivamente via Internet. Non hanno filiali fisiche e ciò permette loro di offrire i prodotti a commissioni relativamente contenute. Le modalità di contatto limitate possono creare, in caso di problemi, grosse differenze rispetto al supporto offerto dagli istituti finanziari tradizionali.

Bit

La più piccola unità di informazione nell'elaborazione elettronica dei dati; corrisponde a una decisione sì/no, oppure a uno 0/1 in una stringa di dati digitale.

Blockchain

Serie di blocchi di informazioni interconnessi tra loro e protetti attraverso procedure di crittografia. L'applicazione blockchain più famosa è Bitcoin, dove la blockchain rappresenta il libro contabile a prova di manomissione delle transazioni.

Vedi anche: [Criptovaluta \(https://www.ebas.ch/it/glossary/criptovaluta/\)](https://www.ebas.ch/it/glossary/criptovaluta/)

Bluetooth

Standard per la comunicazione radio su brevi distanze. La velocità di trasmissione può raggiungere i 2 MBit per secondo con una portata fino a 100 metri.

Botnet

Reti composte solitamente da diverse migliaia di dispositivi che vengono collegati tra loro in seguito a un'infezione da malware. Nella maggior parte dei casi chi gestisce una botnet illegale installa il software «bot» senza che il proprietario del dispositivo lo sappia e ne sfrutta le risorse per i propri scopi, p. es. per sferrare attacchi DDoS distribuiti, inviare e-mail di spam o coniare criptovalute. Solitamente i bot possono essere monitorati e ricevere comandi dall'operatore della botnet attraverso un canale di comunicazione.

Vedi anche: [Distributed Denial-of-Service \(DDoS\)](https://www.ebas.ch/it/glossary/distributed-denial-of-service-ddos/) (<https://www.ebas.ch/it/glossary/distributed-denial-of-service-ddos/>), [Criptovaluta](https://www.ebas.ch/it/glossary/criptovaluta/) (<https://www.ebas.ch/it/glossary/criptovaluta/>), [Malware](https://www.ebas.ch/it/glossary/malware-software-dannoso/) (<https://www.ebas.ch/it/glossary/malware-software-dannoso/>)

Browser

Speciale programma per la visualizzazione di pagine Internet salvate nel World Wide Web (WWW) o di documenti e dati in generale. I principali browser per Internet sono Google Chrome, Mozilla Firefox, Microsoft Edge e Apple Safari.

Vedi anche: [World Wide Web \(WWW\)](https://www.ebas.ch/it/glossary/world-wide-web-www/) (<https://www.ebas.ch/it/glossary/world-wide-web-www/>)

Cache

Rapida memoria intermedia utilizzata per rendere velocemente disponibili i dati (in caso di accesso ripetuto). Nel contesto di Internet, i browser salvano i contenuti delle pagine visitate per far sì che non sia necessario scaricarli nuovamente in occasione di una visita successiva e quindi consentirne una più rapida visualizzazione.

Captcha

Un captcha è un test automatizzato che garantisce che un utente sia un essere umano e non un programma informatico (bot). Tipicamente si tratta di indovinelli fotografici, riconoscimento di lettere distorte o semplici compiti (matematici).

Carding

Descrive la commercializzazione, la distribuzione e l'uso di carte di credito illegali. Le attività comprendono anche lo sfruttamento di dati personali e il riciclaggio di denaro.

Cavallo di Troia

Malware che si spaccia a prima vista per programma utile o videogioco, ma che in realtà persegue altri scopi in background. I cavalli di Troia, p. es., possono sottrarre password e altri dati riservati, modificarli, cancellarli o inoltrarli all'autore dell'attacco.

Vedi anche: [Malware \(https://www.ebas.ch/it/glossary/malware-software-dannoso/\)](https://www.ebas.ch/it/glossary/malware-software-dannoso/)

Centro nazionale per la cibersicurezza (NCSC)

Il Centro nazionale per la cibersicurezza (NCSC) è il centro di competenza della Confederazione per tutto ciò che concerne la sicurezza informatica ed è quindi il primo punto di contatto per gli operatori economici, le amministrazioni, gli istituti di formazione e la popolazione sulle questioni relative alla cibersicurezza.

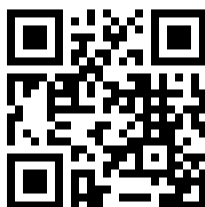
Codice di transazione (TAN)

Tipo di password utilizzabile una sola volta che si abbina all'uso di una password o di un PIN. I codici TAN si possono generare e far pervenire all'utente in modi diversi – p. es. il mobile TAN (mTAN) viene trasmesso dall'istituto finanziario via SMS, il Photo-TAN viene visualizzato decifrando un mosaico colorato.

Codice Quick Response (codice QR)

Originariamente i [codici QR \(https://www.ebas.ch/qrcode\)](https://www.ebas.ch/qrcode) furono sviluppati per contrassegnare componenti e moduli nel settore della produzione automobilistica. Con il tempo sono stati adottati anche da settori come [Fattura QR \(https://www.ebas.ch/it/fattura-qr/\)](https://www.ebas.ch/it/fattura-qr/) e l'editoria e il marketing per consentire un collegamento diretto da oggetti fisici (prodotti, stampati, poster ecc.) al mondo online per rendere disponibili informazioni più approfondite. Poiché il contenuto dei codici QR non è immediatamente decodificabile da un essere umano, i codici vanno scansionati usando p. es. lo smartphone.

Prima di leggere un codice QR, quindi, l'utente in genere non può riconoscere il tipo di informazioni che sono state codificate. Per questo motivo è consigliabile, se possibile, utilizzare uno scanner di codici QR (un'app) che visualizzi innanzitutto i contenuti decodificati e chiedi conferma prima di aprire un certo link o eseguire una certa azione.



Esempio del codice QR di «eBanking – ma sicuro!»

Collegamento ipertestuale

Riferimento p. es. a siti Internet che con un clic permette di passare a un altro documento elettronico o a un'altra sezione dello stesso documento. Nel WWW gli indirizzi di destinazione di questi passaggi possono essere anche altri siti Internet.

Cookie

File di testo che vengono generati e salvati sui dispositivi quando si apre una pagina Internet. Ciò consente di riconoscere i visitatori alle successive consultazioni della stessa pagina Internet. Questo sistema permette di effettuare l'accesso automaticamente, p. es., o di ripristinare gli articoli contenuti nel carrello della spesa.

Tuttavia i cookie vengono utilizzati anche dalle reti pubblicitarie per registrare i comportamenti di utilizzo degli utenti e visualizzare pubblicità mirate.

Criptovaluta

Le criptovalute sono mezzi digitali di scambio e pagamento o valori patrimoniali che utilizzano procedure di crittografia per garantire la sicurezza del sistema di pagamento. Se del software dannoso riesce a paralizzare un dato sistema, solitamente i criminali informatici esigono un pagamento in una criptovaluta (p. es. Bitcoin) per rendere impossibile la tracciabilità.

Crittografia

Scienza della cifratura applicata alla trasmissione e all'archiviazione di informazioni in modo segreto.

Crypto mining

Con il crypto mining vengono prodotte unità (coin) di una criptovaluta (p. es. Bitcoin) e vengono verificate le nuove transazioni. Poiché in genere le criptovalute non sono emesse da un'istanza sovraordinata, hanno bisogno di cosiddetti crypto miner che registrino, verifichino e iscrivano tutte le transazioni.

Vedi anche: [Criptovaluta \(https://www.ebas.ch/it/glossary/cryptovaluta/\)](https://www.ebas.ch/it/glossary/cryptovaluta/)

Crypto wallet

Le criptovalute sono memorizzate in formato digitale nei cosiddetti wallet (portafogli) e protette da codici di accesso.

Vedi anche: [Criptovaluta \(https://www.ebas.ch/it/glossary/cryptovaluta/\)](https://www.ebas.ch/it/glossary/cryptovaluta/)

Darknet

In una darknet gli utenti di Internet possono muoversi pressoché nel massimo anonimato. È un'area di Internet sfruttata da chi attribuisce grande importanza alla sfera privata o vive in un sistema politico repressivo – ma anche, molto spesso, dai criminali.

Deepfake

Contenuti multimediali realistici, come foto, video o file audio, che sono stati manipolati o creati da zero con l'aiuto dell'intelligenza artificiale. Lo scopo è quello di rappresentare persone, luoghi o eventi come se fossero reali, benché contraffatti o del tutto inventati.

Distributed Denial-of-Service (DDoS)

Un attacco DDoS consiste in un attacco al sito Internet o al server di un'azienda sferrato da più fonti contemporaneamente. Un alto numero di dispositivi (solitamente parte di una botnet) bombarda il bersaglio con una serie innumerevole di richieste. Come risultato, il sito Internet o il server non riescono a resistere al sovraccarico e non sono più accessibili, oppure solo limitatamente. Dietro gli attacchi DDoS alle aziende si cela spesso un tentativo di ricatto. Se non viene pagato quanto richiesto, i criminali minacciano di ripetere gli attacchi.

Vedi anche: [Botnet \(https://www.ebas.ch/it/glossary/botnet/\)](https://www.ebas.ch/it/glossary/botnet/)

Domain Name System (DNS)

Servizio Internet che converte un nome di dominio (p. es. www.ebas.ch) nel corrispondente indirizzo IP (217.26.54.120).

Dominio

Nome sotto il quale è raggiungibile una risorsa (p. es. un sito Internet). Ogni dominio è formato da più parti, divise tra loro da punti. Il dominio di questo sito Internet è p. es. [www.ebas.ch \(http://www.ebas.ch\)](http://www.ebas.ch).

Download drive-by

Infezione di un dispositivo per mezzo di malware per il tramite di una normale visita a una pagina Internet. Molte volte le pagine Internet infette contengono offerte serie e sono state manomesse per diffondere il malware. Basta aprire una pagina infetta per trasmettere l'infezione sul proprio dispositivo.

Vedi anche: [Malware \(https://www.ebas.ch/it/glossary/malware-software-dannoso/\)](https://www.ebas.ch/it/glossary/malware-software-dannoso/)

Dropper e downloader

Un dropper (malware) è un piccolo programma il cui unico compito è quello di eseguire su un sistema un malware (che di solito ha funzioni più ampie).

Un downloader è un dropper che scarica il malware da Internet.

Vedi anche: [Malware \(https://www.ebas.ch/it/glossary/malware-software-dannoso/\)](https://www.ebas.ch/it/glossary/malware-software-dannoso/)

Exploit

Un **exploit** (dal verbo inglese «sfruttare») è un programma dannoso che sfrutta in modo mirato una certa vulnerabilità per compromettere un sistema.

Falla di sicurezza

Una falla di sicurezza consiste in un punto debole identificato in un hardware o software che, in determinate condizioni, innesca un comportamento del sistema imprevisto e indesiderato.

Vedi anche: [Vulnerabilità \(https://www.ebas.ch/it/glossary/vulnerabilita/\)](https://www.ebas.ch/it/glossary/vulnerabilita/)

Falla zero-day

Falla di sicurezza in un software che non è ancora nota al produttore e per la quale, quindi, non esiste ancora una patch. «Zero-day» significa che ci sono «zero giorni» tra la scoperta di questa vulnerabilità e il primo attacco.

Vedi anche: [Exploit \(https://www.ebas.ch/it/glossary/exploit/\)](https://www.ebas.ch/it/glossary/exploit/), [Malware \(https://www.ebas.ch/it/glossary/malware-software-dannoso/\)](https://www.ebas.ch/it/glossary/malware-software-dannoso/), [Patch \(https://www.ebas.ch/it/glossary/patch/\)](https://www.ebas.ch/it/glossary/patch/), [Ransomware \(https://www.ebas.ch/it/glossary/ransomware-cavallo-di-troia-crittografante/\)](https://www.ebas.ch/it/glossary/ransomware-cavallo-di-troia-crittografante/), [Falla di sicurezza \(https://www.ebas.ch/it/glossary/falla-di-sicurezza/\)](https://www.ebas.ch/it/glossary/falla-di-sicurezza/), [Vulnerabilità \(https://www.ebas.ch/it/glossary/vulnerabilita/\)](https://www.ebas.ch/it/glossary/vulnerabilita/)

Filtro anti-spam

Sistema per filtrare dalla posta in arrivo le e-mail di spam indesiderate.

Vedi anche: [Spam \(https://www.ebas.ch/it/glossary/spam/\)](https://www.ebas.ch/it/glossary/spam/)

Firewall

Sistema di sicurezza che protegge una rete di computer o un singolo dispositivo dagli accessi indesiderati.

Firma digitale

Sigillo digitale che produce un legame univoco e non manipolabile tra una persona fisica e un documento elettronico (p. es. un'e-mail). Sulla base del documento da firmare viene calcolata una checksum (o somma di controllo, codice hash) secondo un determinato algoritmo. La checksum viene crittografata con la chiave di firma segreta del mittente e inviata al destinatario insieme al documento originale. Utilizzando lo stesso algoritmo questo produce un nuovo codice hash basato sul documento. Inoltre utilizzando la chiave pubblica del mittente decifra il codice hash che ha ricevuto e che è stato creato inizialmente dal mittente. Se i due codici hash corrispondono, può essere sicuro che il documento gli è giunto senza essere stato contraffatto e che il mittente è effettivamente la persona che dice di essere.

Impersonificazione

Presentarsi sotto falsa identità. Nell'ambito dell'e-banking ciò significa che una terza persona esegue l'accesso presso un istituto finanziario utilizzando dati altrui e quindi non a nome proprio. La terza persona dispone così di accesso illimitato ai conti. L'istituto finanziario non ha alcun modo di sapere se sta comunicando con il cliente in persona, un intermediario legittimamente incaricato o un intruso criminale. L'impersonificazione viene utilizzata nei classici attacchi di [phishing \(https://www.ebas.ch/it/phishing/\)](https://www.ebas.ch/it/phishing/) e nell'[accesso di terze parti ai conti bancari \(https://www.ebas.ch/it/accesso-di-terze-parti-ai-conti-bancari/\)](https://www.ebas.ch/it/accesso-di-terze-parti-ai-conti-bancari/).

Impronta digitale

Procedura che consente di verificare una chiave crittografica senza dover confrontare l'intera chiave. Ciò permette p. es. di verificare l'autenticità di un certificato con cui è stata instaurata una connessione TLS/SSL. Un'impronta digitale si presenta generalmente come una sequenza esadecimale di lettere dalla A alla F e numeri dallo 0 al 9.

Indirizzo Internet Protocol

Indirizzo in una rete di computer basato sul protocollo Internet (IP). Viene assegnato ai dispositivi collegati alla rete per renderli individuabili e raggiungibili.

Vedi anche: [Transmission Control Protocol/Internet Protocol \(TCP/IP\) \(https://www.ebas.ch/it/glossary/transmission-control-protocol-internet-protocol-tcp-ip/\)](https://www.ebas.ch/it/glossary/transmission-control-protocol-internet-protocol-tcp-ip/), [Domain Name System \(DNS\) \(https://www.ebas.ch/it/glossary/domain-name-system-dns/\)](https://www.ebas.ch/it/glossary/domain-name-system-dns/)

Indirizzo Media Access Control

Numero di identificazione individuale di un dispositivo di rete (p. es. un collegamento WLAN). Generalmente il codice identificativo viene assegnato in fabbrica. Lo si può paragonare al numero di telaio di un'automobile.

Internet delle cose, Internet of Things (IoT)

Termine collettivo con cui si indicano le tecnologie che consentono di collegare in rete e far comunicare tra loro oggetti fisici o virtuali. Solitamente i dispositivi sono dotati di sensori per registrare informazioni ottenute dall'ambiente e un software integrato per collegarsi ad altri dispositivi e sistemi e scambiare dati. Esempi tipici sono la domotica (riscaldamento), il monitoraggio della salute (orologi sportivi) o il controllo delle condizioni ambientali (stazioni meteorologiche).

Investment Fraud

Nota anche come truffa sugli investimenti, consiste in una truffa in cui si inducono le persone a investire in progetti o prodotti fornendo loro informazioni errate o ingannevoli. Spesso si tratta di opportunità di investimento fittizie, fortemente sopravvalutate o i cui rischi vengono deliberatamente nascosti. L'obiettivo di questo inganno è quello di ottenere denaro dagli investitori promettendo rendimenti o benefici spesso irrealistici.

Jailbreak

Rimozione non autorizzata di limitazioni d'utilizzo, soprattutto per gli smartphone. Nel «jailbreak» un apposito software consente di modificare il sistema operativo per accedere a funzioni interne e al file system. La procedura può pregiudicare notevolmente la sicurezza e la stabilità del sistema operativo.

Java

Linguaggio di programmazione orientato agli oggetti e multi-piattaforma. Per eseguire i programmi Java è necessario che sul computer sia installata un'apposita struttura di supporto, denominata «Java runtime environment».

JavaScript

Linguaggio di script utilizzato per organizzare dinamicamente le pagine Internet. JavaScript permette di modificare o aggiornare contenuti e quindi visualizzare p. es. alcune proposte di ricerca già durante la digitazione.

Keylogger

Malware che registra quali tasti vengono premuti dall'utente nella speranza di individuare dati d'accesso, p. es. password.

Vedi anche: [Malware \(https://www.ebas.ch/it/glossary/malware-software-dannoso/\)](https://www.ebas.ch/it/glossary/malware-software-dannoso/)

Local Area Network

Si tratta di una rete locale, nella quale le postazioni di lavoro, i server e i dispositivi aggiuntivi sono connessi tra loro a distanza di poche centinaia di metri (massimale), solitamente all'interno di un edificio o di un complesso di edifici.

Vedi anche: [Wireless Local Area Network \(WLAN\) \(https://www.ebas.ch/it/glossary/wireless-local-area-network-wlan-wi-fi/\)](https://www.ebas.ch/it/glossary/wireless-local-area-network-wlan-wi-fi/)

Macro

Alcuni programmi (tra cui Microsoft Office e Adobe Acrobat) offrono agli utenti la possibilità di automatizzare determinate attività registrando dei programmi, noti come «macro», «azioni» o «script». Tuttavia, questa possibilità viene sfruttata anche per aggiungere codice dannoso (malware) a documenti dall'aspetto comune.

Vedi anche: [Malware \(https://www.ebas.ch/it/glossary/malware-software-dannoso/\)](https://www.ebas.ch/it/glossary/malware-software-dannoso/)

Malware

Composto delle parole inglesi «malicious» (maligno) e «software». Si tratta di un termine generico per indicare qualsiasi genere di software che esegue funzioni dannose su un dispositivo (come virus, worm, cavalli di Troia e ransomware).

Vedi anche: [Adware \(https://www.ebas.ch/it/glossary/adware/\)](https://www.ebas.ch/it/glossary/adware/), [Backdoor \(https://www.ebas.ch/it/glossary/backdoor/\)](https://www.ebas.ch/it/glossary/backdoor/), [Botnet \(https://www.ebas.ch/it/glossary/botnet/\)](https://www.ebas.ch/it/glossary/botnet/), [Download drive-by \(https://www.ebas.ch/it/glossary/download-drive-by/\)](https://www.ebas.ch/it/glossary/download-drive-by/), [Keylogger \(https://www.ebas.ch/it/glossary/keylogger/\)](https://www.ebas.ch/it/glossary/keylogger/), [Ransomware \(https://www.ebas.ch/it/glossary/ransomware-cavallo-di-troia-crittografante/\)](https://www.ebas.ch/it/glossary/ransomware-cavallo-di-troia-crittografante/), [Rootkit \(https://www.ebas.ch/it/glossary/rootkit/\)](https://www.ebas.ch/it/glossary/rootkit/), [Scareware \(https://www.ebas.ch/it/glossary/scareware/\)](https://www.ebas.ch/it/glossary/scareware/), [Session-Riding \(https://www.ebas.ch/it/glossary/session-riding/\)](https://www.ebas.ch/it/glossary/session-riding/), [Spyware \(https://www.ebas.ch/it/glossary/spyware/\)](https://www.ebas.ch/it/glossary/spyware/), [Cavallo di Troia \(https://www.ebas.ch/it/glossary/cavallo-di-troia-trojan/\)](https://www.ebas.ch/it/glossary/cavallo-di-troia-trojan/), [Virus \(https://www.ebas.ch/it/glossary/virus/\)](https://www.ebas.ch/it/glossary/virus/), [Worm \(https://www.ebas.ch/it/glossary/worm/\)](https://www.ebas.ch/it/glossary/worm/)

Man-in-the-middle (MitM)

Un attacco del tipo man-in-the-middle (letteralmente, «uomo nel mezzo») si basa su del malware (o a terzi) che si introduce nella sessione di e-banking collocandosi inosservato tra il dispositivo dell'utente e il server dell'istituto finanziario e assume il controllo dello scambio di dati.

Vedi anche: [Phishing \(https://www.ebas.ch/it/glossary/phishing/\)](https://www.ebas.ch/it/glossary/phishing/), [Pharming \(https://www.ebas.ch/it/glossary/pharming/\)](https://www.ebas.ch/it/glossary/pharming/)

Money Mule

Con il termine [Money Mule \(https://www.ebas.ch/it/money-mules-agenti-finanziari/\)](https://www.ebas.ch/it/money-mules-agenti-finanziari/) o «agenti finanziari» si designano le persone che dietro compenso ricevono e trasferiscono denaro all'estero utilizzando i propri conti correnti. I fondi derivano quasi sempre da attività illecite. I Money Mule vengono reclutati solitamente per mezzo di offerte d'impiego redditizie che promettono guadagni rapidi e cospicui. Chi collabora a questi «affari» rischia un procedimento penale per supporto al riciclaggio di denaro.

Nome utente

Nome con cui un utente esegue l'autenticazione su un sistema. Quando si esegue l'accesso a un programma o un servizio (p. es. nell'e-banking) solitamente viene chiesto di inserire un nome utente e una password. Questi dati servono a identificare l'utente autorizzato.

Vedi anche: [Autenticazione \(https://www.ebas.ch/it/glossary/autenticazione/\)](https://www.ebas.ch/it/glossary/autenticazione/), [Accesso \(https://www.ebas.ch/it/glossary/accesso-login/\)](https://www.ebas.ch/it/glossary/accesso-login/)

Passkey

Una passkey permette di effettuare un login senza password. Il funzionamento si basa su una coppia di chiavi, una segreta e una pubblica. La chiave segreta rimane sempre su un dispositivo locale, p. es. uno smartphone o una chiavetta USB, senza uscirne mai. È il dispositivo a fungere da strumento di autenticazione. Quindi le passkey sono legate al dispositivo, non alla persona come le password.

Password

Strumento utilizzato per l'autenticazione. Viene concordata una sequenza di caratteri che qualcuno, solitamente una persona, può utilizzare per identificarsi e quindi confermare la propria identità.

Una [buona password \(https://www.ebas.ch/it/4-protectere-gli-accessi-online/\)](https://www.ebas.ch/it/4-protectere-gli-accessi-online/) dovrebbe essere lunga almeno 12 caratteri e composta da cifre, lettere maiuscole e minuscole e caratteri speciali.

Vedi anche: [Autenticazione \(https://www.ebas.ch/it/glossary/autenticazione/\)](https://www.ebas.ch/it/glossary/autenticazione/)

Patch

Piccola correzione di un programma che risolve i bug (errori) di un software. La maggior parte delle patch viene distribuita dai produttori di software tramite download gratuito dai loro siti Internet oppure in modo automatico.

Vedi anche: [Upgrade \(https://www.ebas.ch/it/glossary/upgrade/\)](https://www.ebas.ch/it/glossary/upgrade/)

Pharming

Come il classico phishing, rientra nella categoria degli attacchi man-in-the-middle. Nel pharming il reindirizzamento alla pagina Internet contraffatta avviene manipolando l'assegnazione di indirizzo IP e dominio.

Vedi anche: [Man-in-the-middle \(MitM\) \(https://www.ebas.ch/it/glossary/man-in-the-middle-mitm/\)](https://www.ebas.ch/it/glossary/man-in-the-middle-mitm/)

Phishing

Termine composto dalle parole inglesi «password» e «fishing» (andare a pesca). Per mezzo del [phishing](https://www.ebas.ch/it/phishing/) (<https://www.ebas.ch/it/phishing/>) i criminali cercano di carpire i dati riservati di ignari utenti Internet. Può trattarsi p. es. delle credenziali d'accesso per il sistema di e-banking o delle informazioni relative al proprio account su uno shop online. I malviventi sfruttano la buona fede e la disponibilità delle vittime presentandosi p. es. come collaboratori di un istituto finanziario affidabile.

Oltre al classico phishing tramite e-mail ci sono diverse altre varianti come il vishing (Voice-Phishing, detto anche Phone-Phishing), Smishing (phishing via SMS) e il phishing QR.

Vedi anche: [Man-in-the-middle \(MitM\)](https://www.ebas.ch/it/glossary/man-in-the-middle-mitm/) (<https://www.ebas.ch/it/glossary/man-in-the-middle-mitm/>)

Provider

Il fornitore dell'accesso a Internet, ossia l'organizzazione o l'azienda che permette agli utenti di collegare i loro dispositivi a Internet.

Ransomware

Malware che cifra i file presenti su un dispositivo ed eventuali unità di rete e supporti di memorizzazione connessi (p. es. dischi rigidi esterni, archivi cloud) esigendo poi il pagamento di un riscatto.



Vedi anche: [Malware](https://www.ebas.ch/it/glossary/malware-software-dannoso/) (<https://www.ebas.ch/it/glossary/malware-software-dannoso/>)

Rootkit

Software che si prefigge lo scopo di nascondere agli occhi dell'utente – e spesso anche di programmi di sicurezza (antivirus) – determinati file, cartelle, processi o registri di sistema. In sé e per sé un rootkit non è «dannoso», ma è un indizio della presenza di malware sul computer.

Vedi anche: [Malware](https://www.ebas.ch/it/glossary/malware-software-dannoso/) (<https://www.ebas.ch/it/glossary/malware-software-dannoso/>)

Scamming

Tradotto liberamente, «imbrogliare», una pratica diffusa in diversi contesti in Internet. L'obiettivo principale è quello di sottrarre denaro alle persone. Una forma molto diffusa è, ad esempio, il «Romance Scamming», ossia lo sviluppo di una relazione fingendo sentimenti d'amore, per poi chiedere del denaro.

Vedi anche: [Phishing \(https://www.ebas.ch/it/glossary/phishing/\)](https://www.ebas.ch/it/glossary/phishing/), [Money Mule \(https://www.ebas.ch/it/glossary/money-mule-agente-finanziario/\)](https://www.ebas.ch/it/glossary/money-mule-agente-finanziario/), [Social Engineering \(https://www.ebas.ch/it/glossary/social-engineering/\)](https://www.ebas.ch/it/glossary/social-engineering/)

Scareware

Termine composto dalle parole inglesi «scare» (spaventare) e «software». Facendo comparire avvisi ingannevoli relativi p.e. a un'ipotetica infezione del dispositivo, si cerca di spaventare e disorientare gli utenti, spingendoli ad acquistare p. es. (inutile) «software antivirus» di dubbia origine.

Vedi anche: [Malware \(https://www.ebas.ch/it/glossary/malware-software-dannoso/\)](https://www.ebas.ch/it/glossary/malware-software-dannoso/)

Secure Sockets Layer (SSL)

Precedente denominazione di Transport Layer Security (TLS).

Vedi anche: [Transport Layer Security \(TLS\) \(https://www.ebas.ch/it/glossary/transport-layer-security-tls/\)](https://www.ebas.ch/it/glossary/transport-layer-security-tls/)

Service Set Identifier (SSID)

Rappresenta il nome di una rete WLAN.

Vedi anche: [Wireless Local Area Network \(WLAN\) \(https://www.ebas.ch/it/glossary/wireless-local-area-network-wlan-wi-fi/\)](https://www.ebas.ch/it/glossary/wireless-local-area-network-wlan-wi-fi/)

Session-Riding

Diversamente dal phishing e dal pharming, il session riding non è un attacco man-in-the-middle. Invece di deviare le credenziali d'accesso verso un malintenzionato, nel session riding le comunicazioni con l'istituto finanziario vengono manipolate già sul dispositivo della vittima per mezzo di malware.

Vedi anche: [Malware \(https://www.ebas.ch/it/glossary/malware-software-dannoso/\)](https://www.ebas.ch/it/glossary/malware-software-dannoso/)

Sistema operativo

Programma del dispositivo che gestisce le risorse del sistema come il processore, i supporti di memorizzazione e i dispositivi di input/output mettendoli a disposizione delle applicazioni (software). Sistemi operativi noti sono p. es. Windows, macOS, Linux, Android e iOS.

Social Engineering

Attacco che segue uno schema più psicologico che tecnologico. Si tratta di un metodo diffuso per l'acquisizione di informazioni riservate. Nel mirino ci sono sempre i singoli individui. Per raggiungere questo obiettivo vengono spesso sfruttate la buona fede e la disponibilità – così come l'insicurezza – delle persone. Dalle telefonate fittizie alle persone che si spacciano per qualcun altro, agli attacchi di phishing, non c'è limite alla varietà.

Spam

Termine generico per identificare i messaggi di posta elettronica indesiderata, spesso contenenti pubblicità. Le e-mail di phishing, che mirano a sottrarre i dati personali del destinatario, rientrano in questa categoria.

Vedi anche: [Filtro anti-spam \(https://www.ebas.ch/it/glossary/filtro-anti-spam/\)](https://www.ebas.ch/it/glossary/filtro-anti-spam/)

Spoofing

Dal verbo inglese che significa «parodiare» e per estensione «mascherarsi», si tratta di un metodo di attacco con il quale i criminali informatici assumono una falsa identità, ad esempio per presentarsi come una persona o un'organizzazione affidabile. Vengono falsificati per esempio indirizzi e-mail e numeri di telefono.

Spyware

Malware che, a insaputa dell'utente, registra e trasmette informazioni riguardanti il suo dispositivo e le sue attività online. I destinatari delle informazioni possono così ricostruire p. es. le abitudini dell'utente in termini di navigazione o shopping online. Generalmente i programmi di spionaggio di questo tipo si introducono in un dispositivo durante l'installazione di programmi shareware o freeware.

Vedi anche: [Malware \(https://www.ebas.ch/it/glossary/malware-software-dannoso/\)](https://www.ebas.ch/it/glossary/malware-software-dannoso/)

Transmission Control Protocol/Internet Protocol (TCP/IP)

Famiglia di protocolli composta dai protocolli di comunicazione fondamentali di Internet. Spesso tali protocolli vengono utilizzati anche nell'ambito di una rete privata.

Transport Layer Security (TLS)

Protocollo di crittografia ibrido per i trasferimenti di dati sicuri in Internet.

Vedi anche: [Secure Sockets Layer \(SSL\) \(https://www.ebas.ch/it/glossary/secure-sockets-layer-ssl/\)](https://www.ebas.ch/it/glossary/secure-sockets-layer-ssl/)

Ufficio federale della cibersicurezza (UFCS)

L'Ufficio federale della cibersicurezza (UFCS) è il centro di competenza della Confederazione per la cibersicurezza. Funge da primo servizio di contatto per l'economia, l'amministrazione pubblica, gli istituti di formazione e la popolazione nelle questioni legate alla cibersicurezza. È inoltre responsabile dell'attuazione coordinata della ciberstrategia nazionale (CSN).

Unicode

Standard internazionale che assegna in modo duraturo un codice digitale a ogni carattere o elemento testuale portatore di significato di ogni lingua scritta nota e di ogni set di caratteri. Lo scopo di tale sistema è eliminare l'uso di codifiche differenti e incompatibili tra loro in paesi o culture diverse. Lo standard Unicode viene ampliato continuamente con l'aggiunta di caratteri appartenenti a nuovi sistemi di scrittura.

Vedi anche: [American Standard Code for Information Interchange \(ASCII\)](https://www.ebas.ch/it/glossary/american-standard-code-for-information-interchange-ascii/) (<https://www.ebas.ch/it/glossary/american-standard-code-for-information-interchange-ascii/>)

Uniform Resource Locator (URL)

L'indirizzo di un sito Internet – p. es. <https://www.ebas.ch> (<https://www.ebas.ch>). Diversamente dal dominio, l'URL comprende anche il protocollo (p. es. <https://>) ed eventualmente anche altri dati, come la porta (p. es. :80).

Vedi anche: [Dominio](https://www.ebas.ch/it/glossary/dominio/) (<https://www.ebas.ch/it/glossary/dominio/>)

Upgrade

Potenziamento/ampliamento di un sistema o software. Inizialmente il termine «upgrade» veniva utilizzato soltanto per gli aggiornamenti hardware, ora è (quasi) sinonimo di «update». Alcuni produttori di software operano una distinzione tra update gratuiti (con cui solitamente si correggono errori ecc.) e upgrade a pagamento (che solitamente offrono funzioni aggiuntive).

Vedi anche: [Patch](https://www.ebas.ch/it/glossary/patch/) (<https://www.ebas.ch/it/glossary/patch/>)

Uscita

Processo di uscita dell'utente, con cui si segnala al sistema l'intenzione di concludere la sessione corrente.

Vedi anche: [Accesso](https://www.ebas.ch/it/glossary/accesso-login/) (<https://www.ebas.ch/it/glossary/accesso-login/>)

Virtual Private Network (VPN)

Indica una rete di comunicazione privata (chiusa in sé) virtuale. In genere una VPN viene utilizzata per instaurare, su una rete non sicura (p. es. Internet), una connessione sicura tra un dispositivo e una rete sicura (p. es. la rete aziendale). Durante il trasporto i contenuti vengono cifrati (crittografia end-to-end).

Virus

Benché il termine sia ancora noto a tutti gli utenti, nella realtà di oggi i virus (per computer) veri e propri sono pochi. Il virus (per computer) classico infetta i file esistenti su un dispositivo nella speranza che una sua copia venga trasmessa a un altro utente. Quando il software dannoso (malware) non agisce in alcun modo per diffondersi attivamente, si parla di virus. Se invece il software dannoso è anche in grado di diffondersi automaticamente, p. es. tramite posta elettronica, si parla di worm.

Vedi anche: [Malware \(https://www.ebas.ch/it/glossary/malware-software-dannoso/\)](https://www.ebas.ch/it/glossary/malware-software-dannoso/), [Worm \(https://www.ebas.ch/it/glossary/worm/\)](https://www.ebas.ch/it/glossary/worm/)

Vulnerabilità

Una **vulnerabilità** (in inglese «vulnerability») consiste in un punto debole identificato in un hardware o software che, in determinate condizioni, innesca un comportamento del sistema imprevisto e indesiderato.

Wi-Fi Protected Access (WPA)

Il Wi-Fi Protected Access è un metodo di crittografia per le reti senza fili (WLAN) che diversamente dal WEP offre una protezione aggiuntiva grazie a una chiave dinamica. Il WPA2 è la versione successiva al WPA, ma oggi si conoscono punti deboli sia per il WPA che per il WPA2. Essendo stati riscontrati diversi attacchi ai sistemi WPA e WPA2, è preferibile utilizzare la versione successiva, il WPA3.

Vedi anche: [Advanced Encryption Standard \(AES\) \(https://www.ebas.ch/it/glossary/advanced-encryption-standard-aes/\)](https://www.ebas.ch/it/glossary/advanced-encryption-standard-aes/), [Wireless Local Area Network \(WLAN\) \(https://www.ebas.ch/it/glossary/wireless-local-area-network-wlan-wi-fi/\)](https://www.ebas.ch/it/glossary/wireless-local-area-network-wlan-wi-fi/)

Wireless Local Area Network (WLAN)

Rete locale senza fili o rete radio. Spesso viene usato come sinonimo il termine «Wi-Fi».

Vedi anche: [Advanced Encryption Standard \(AES\) \(https://www.ebas.ch/it/glossary/advanced-encryption-standard-aes/\)](https://www.ebas.ch/it/glossary/advanced-encryption-standard-aes/), [Local Area Network \(https://www.ebas.ch/it/glossary/local-area-network-lan/\)](https://www.ebas.ch/it/glossary/local-area-network-lan/), [Service Set Identifier \(SSID\) \(https://www.ebas.ch/it/glossary/service-set-identifier-ssid/\)](https://www.ebas.ch/it/glossary/service-set-identifier-ssid/), [Wi-Fi Protected Access \(WPA\) \(https://www.ebas.ch/it/glossary/wi-fi-protected-access-wpa-wpa2-wpa3/\)](https://www.ebas.ch/it/glossary/wi-fi-protected-access-wpa-wpa2-wpa3/)

World Wide Web (WWW)

Il WWW fu sviluppato nel 1993 presso il Centro Europeo per la Ricerca Nucleare (CERN) di Losanna in Svizzera come sistema ipermediale per Internet. Allo sviluppo partecipò anche il National Center for Supercomputing Applications (NCSA) dell'Università dell'Illinois, USA. Ora lo sviluppo viene portato avanti dal WWW Consortium (W3C).

Vedi anche: [Browser \(https://www.ebas.ch/it/glossary/browser/\)](https://www.ebas.ch/it/glossary/browser/)

Worm

Anche i worm, come i virus, sono una forma di malware non più particolarmente diffusa al giorno d'oggi. Un worm consiste in un piccolo programma capace di diffondersi autonomamente, p. es. via e-mail, SMS o sfruttando falle di sicurezza.

Vedi anche: [Malware \(https://www.ebas.ch/it/glossary/malware-software-dannoso/\)](https://www.ebas.ch/it/glossary/malware-software-dannoso/), [Virus \(https://www.ebas.ch/it/glossary/virus/\)](https://www.ebas.ch/it/glossary/virus/)