Glossary

Advanced Encryption Standard (AES)

This is a method for encrypting data. AES can for instance be used to encrypt transmissions inside a WLAN (WPA2, WPA3) network. This encrypts anything exchanged between the WLAN router and a device connected wirelessly.

See also: Wi-Fi Protected Access (https://www.ebas.ch/en/glossary/wi-fi-protected-access/) , Wireless Local Area Network (WLAN) (https://www.ebas.ch/en/glossary/wireless-local-area-network/)

Adware

This is made up from the words “advertisement” and “software” and denotes programs which show users ads while the actual program is running, or install additional software to display ads.

See also: Malware (https://www.ebas.ch/en/glossary/malware/)

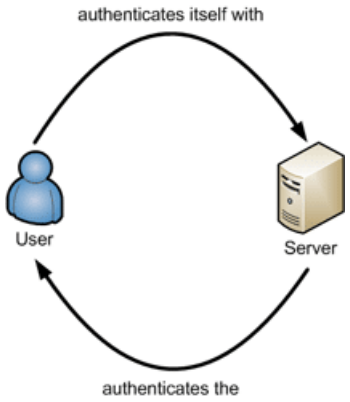
American Standard Code for Information Interchange (ASCII)

Character coding containing 95 printable and 33 non-printable characters. The printable characters include the Latin alphabet (A-Z, a-z), the ten Arabic numerals (0-9) as well as some punctuation marks (sentence symbols, word symbols) and other special characters.

See also: Unicode (https://www.ebas.ch/en/glossary/unicode/)

Authentification

This is a process where the purported identity of a person or device is checked based on one or several specific characteristics (e. g. password, chip card or finger print).



See also: Two-factor authentification (2FA) (https://www.ebas.ch/en/glossary/two-factor-authentification/) , Authorisation (https://www.ebas.ch/en/glossary/authorisation/)

Authorisation

The allocation of permissions. Based on permissions, authorisation is granted to access resources (e. g. files, software, payments, etc.) after successful identification and authentication.

See also: Authentification (https://www.ebas.ch/en/glossary/authentification/)

Back door

A “back door” in relation to software usually denotes non-documented access which allows manufacturers (or third parties) to access users’ software or data from the outside.

See also: Malware (https://www.ebas.ch/en/glossary/malware/)

Back-up

Data back-up, where electronic information (data) is copied to an external storage medium (e. g. an external hard drive). Back-ups are generally run at regular intervals.

Bit

This is the smallest information unit in electronic data processing, equivalent to a yes/no decision or 0/1 in a digital data record.

Blockchain

A series of interconnected blocks of information secured by cryptographic means. The best-known Blockchain application is Bitcoin, with Blockchain providing the manipulation-proof account book with all transactions.

See also: Cryptocurrency (https://www.ebas.ch/en/glossary/cryptocurrency/)

Bluetooth

This is a standard for wireless communication across small distances. Transmission power is up to 1MBit per second, with a range of up to 100 meters.

Botnet

These are networks usually consisting of several thousand devices linked with each other after being infected with malware. Illegal botnet operators usually install bots without a device owner's knowledge on the unit to abuse its resources for their purposes, for instance distributed DDoS attacks, sending out spam mails or mining crypto currencies. Most bots can be monitored via a communication channel by a bot net operator and can receive commands.

See also: Distributed denial of service (DDoS) (https://www.ebas.ch/en/glossary/distributed-denial-of-service/) , Cryptocurrency (https://www.ebas.ch/en/glossary/cryptocurrency/) , Malware (https://www.ebas.ch/en/glossary/malware/)

Browser

A special computer program to display websites on the World Wide Web (WWW) or data and documents in general. The most important browsers used on the Internet are Google Chrome, Mozilla Firefox, Microsoft Edge and Apple Safari.

See also: World Wide Web (WWW) (https://www.ebas.ch/en/glossary/world-wide-web/)

National Cyber Security Centre (NCSC)

The National Cyber Security Centre (NCSC) is the competence centre of the Federation for cyber security and hence the first port of call for businesses, administration, educational institutions and the population for any questions involving cyber security. It is responsible for the coordinated implementation of the Nationale Cyberstrategie (NCS, National Cyber Strategy).

Cache

Denotes fast buffer memory to be able to provide data quickly (in case of repeated access). In the context of the Internet, browsers will store content of websites visited, so that they don't have to be re-downloaded during the next visit, and the site can therefore be displayed more quickly.

Carding

Used to describe the trade, distribution and use of illegal credit cards. Such activities also include exploiting personal data and money laundering.

Cookie

These are text files generated when retrieving a website and then stored on the visitor's device. This facilitates the recognition of visitors during future visits. Visitors can for instance be automatically logged in, or items in their shopping cart restored, this way.

Cookies are however also used by advertising networks to record user behaviour and display adverts in a targeted manner.

Crypto Mining

During the process of crypto mining, the units (coins) of a cryptocurrency (e. g. Bitcoin) are generated and new transactions verified. Since cryptocurrencies are generally not issued by a superordinate institution, so-called crypto miners are needed to record, verify and register all transactions

See also: Cryptocurrency (https://www.ebas.ch/en/glossary/cryptocurrency/)

Crypto wallet

Cryptocurrencies are stored digitally in so-called wallets, protected by access codes.

See also: Cryptocurrency (https://www.ebas.ch/en/glossary/cryptocurrency/)

Cryptocurrency

Cryptocurrencies are digital means of exchange/payment or assets using cryptographic techniques to ensure a payment system is secure. When systems are being paralysed by malware, cyber-criminals usually demand a cryptocurrency payment (e. g. bitcoins) to make tracing impossible.

Cryptography

The science of encryption for the purpose of secretly transmitting and storing information.

Darknet

Internet users can move almost totally anonymously on the darknet. This area of the Internet is used by people who attach high importance to their privacy, or who live inside a repressive political system - but also quite frequently by criminals.

Digital signature

This is a digital seal which creates a unique connection between a natural person and an electronic document (e.g. e-mail), which cannot be manipulated. In accordance with a certain calculation rule, a check sum (hash value) is computed from the document to be signed. The check sum is encrypted using the signatory's secret key, and then sent to recipients together with the original document. Applying the same calculation rule, they will then create another hash value from the document. Recipients also encrypt the hash value using the public key of senders which has been created by senders to start with. If both hash values are identical, they can assume that the document has arrived on their system unaltered, and that the senders are actually who they purport to be.

Distributed denial of service (DDoS)

A DDoS attack is a distributed attack on a company's website or server. Many devices (mostly those which are part of a bot net) bombard their target with innumerable requests during such an attack. The result: Due to overload, the attacked website or server relents to the pressure and is no longer available, or only to a limited degree. Blackmail attempts are frequently the reason behind DDoS attacks. If no payment is made, criminals will threaten to repeat the attacks.

See also: Botnet (https://www.ebas.ch/en/glossary/botnet/)

Domain (Domain name)

This is the name under which a resource (e. g. a website) can be reached. Every domain (name) consists of several parts separated from each other by a full stop. The domain of this website for instance is www.ebas.ch (https://www.ebas.ch) .

Domain Name System (DNS)

This is an Internet service converting a domain name (e. g. www.ebas.ch) into the associated IP address (217.26.54.120).

Drive-By Download

This is the term used for a device which becomes infected with malware solely by visiting a website. Websites affected often contain reputable offers and have been compromised beforehand to distribute malware. Simply “surfing” to an affected website is enough to infect a device.

See also: Malware (https://www.ebas.ch/en/glossary/malware/)

Dropper and Downloader

The term dropper (malware) denotes a small program with the single aim of executing (usually more extensive) malware programs on a system.

A downloader is a dropper which downloads more malware from the Internet.

See also: Malware (https://www.ebas.ch/en/glossary/malware/)

Exploit

An **exploit** is a term denominating malicious software which specifically exploits a certain vulnerability to compromise a system.

Fingerprint

This is a process which makes it possible to check a cryptographic key without having to match the whole key. This can for instance be used to check the authenticity of a certificate upon which a TLS/SSL connection is based. A fingerprint is usually displayed as a hexadecimal character string consisting of the letters A-F and the numbers 0-9.

Firewall

This is a security system which protects a computer network or an individual device against unwanted network access.

Hyperlink

This is a cross reference, for instance to websites, which makes it possible to jump to another electronic document or a different location inside a document when clicked. On the WWW, the target addresses of such jumps could also be other websites.

Impersonation

Presenting yourself under a false identity. In the context of e-banking, this means that a third party logs into a financial institution's site with someone else's access data and therefore under someone else's name. This then gives the third party unlimited account access. For the financial institution, it becomes exceedingly difficult to distinguish whether they are communicating with customers themselves, with an intermediary on their behalf, or with a criminal attacker. Impersonation is used in classic-style phishing (https://www.ebas.ch/en/phishing/) attacks and when third party providers access bank accounts (https://www.ebas.ch/en/third-party-access-to-bank-accounts/) .

Internet of Things (IoT)

Collective term for technologies facilitating the connection of physical or virtual objects in a network to allow them to communicate with each other. Such devices are generally fitted with sensors to record information from their environment, and embedded software to link and exchange data with other devices and systems. Some typical examples are home control (heating), health monitoring (sports watches) or environmental monitoring (weather stations).

Internet protocol address

This is an address in computer networks based on the Internet Protocol (IP). It is allocated to devices connected to the Net, and renders devices addressable, and hence reachable.

See also: Transmission Control Protocol/Internet Protocol (TCP/IP) (https://www.ebas.ch/en/glossary/transmission-control-protocol-internet-protocol/) , Domain Name System (DNS) (https://www.ebas.ch/en/glossary/domain-name-system/)

Investment fraud

Investment fraud refers to a type of fraud where investors are persuaded to invest in projects or products with the help of fake or misleading information. Such investment opportunities are often fictitious, severely over-valued or have their risks deliberately concealed. Such scams aim to obtain money from investors by promising unrealistically high yields or benefits.

Jailbreak

Non-authorised removal of usage restrictions, in particular with smartphones. With a Jailbreak, special software is used to modify the operating system to obtain access to internal functions and the file system. As a result, the security and stability of your operating system can be severely affected.

Java

This is an object-orientated and platform-independent programming language. To run Java programs, the Java runtime environment will have to be installed on a computer.

JavaScript

This is a script language for the dynamic design of websites. JavaScript makes it possible to change or reload content, so that search suggestions for instance can already be displayed while inputting a term.

Key loggers

Malware logging the keyboard entries of users hoping to capture log-in data, for instance passwords, this way.

See also: Malware (https://www.ebas.ch/en/glossary/malware/)

Local Area Network (LAN)

This is a local network. Inside such a network, work stations, servers and auxiliary devices are connected to each other across a distance of up to a few hundred meters, usually inside a building or group of buildings.

See also: Wireless Local Area Network (WLAN) (https://www.ebas.ch/en/glossary/wireless-local-area-network/)

Logging in

This is the process of logging in, for instance to use a device or an online service. This process usually serves to advise the system that a session is about to start now, and that users would like to be connected to one of their user accounts, e. g. their e-banking account.

See also: Logging out (https://www.ebas.ch/en/glossary/logging-out/) , Authentification (https://www.ebas.ch/en/glossary/authentification/)

Logging out

This is when users log out of systems. Users instruct the system to terminate the current session this way.

See also: Logging in (https://www.ebas.ch/en/glossary/logging-in/)

Macro

Some programs (for instance Microsoft Office, Adobe Acrobat) allow users to automate certain actions using small programs – so-called macros, actions or scripts. However, attackers also like to abuse these to embed malicious code (malware) in seemingly innocuous-looking documents.

See also: Malware (https://www.ebas.ch/en/glossary/malware/)

Malware

The term is made up of the terms “malicious” and “software”. Malware is the generic term for software which executes malicious functions on a device (such as viruses, worms, Trojans, ransomware).

See also: Adware (https://www.ebas.ch/en/glossary/adware/) , Back door (https://www.ebas.ch/en/glossary/back-door/) , Botnet (https://www.ebas.ch/en/glossary/botnet/) , Drive-By Download (https://www.ebas.ch/en/glossary/drive-by-download/) , Key loggers (https://www.ebas.ch/en/glossary/key-loggers/) , Ransomware (https://www.ebas.ch/en/glossary/ransomware/) , Rootkit (https://www.ebas.ch/en/glossary/rootkit/) , Scareware (https://www.ebas.ch/en/glossary/scareware/) , Session Riding (https://www.ebas.ch/en/glossary/session-riding/) , Spyware (https://www.ebas.ch/en/glossary/spyware/) , Trojan Horse (https://www.ebas.ch/en/glossary/trojan-horse/) , Virus (https://www.ebas.ch/en/glossary/virus/) , Worm (https://www.ebas.ch/en/glossary/worm/)

Man-in-the-Middle (MitM)

With a Man-in-the-Middle attack, a third party or a malware will intervene into an e-banking session by interposing itself unnoticed between a user’s device and a financial institution’s server, to then take control of data traffic.

See also: Phishing (https://www.ebas.ch/en/glossary/phishing/) , Pharming (https://www.ebas.ch/en/glossary/pharming/)

Media Access Control Address

This is the individual identification number of a network device (e. g. WLAN connection). This ID is usually set at the factory. It could be compared to a car’s chassis number.

Money Mule

The term Money Mule (https://www.ebas.ch/en/money-mules-financial-agents/) (and also financial agent) denotes people receiving funds into their own bank account to pass them on abroad against a fee. These funds almost always come from illegal deals. Money mules are generally recruited via lucrative job ads offering fast and high earning potentials. Anyone participating in such “deals” and transactions risks prosecution for aiding and abetting money laundering transactions.

Online banks

Internet banks offer their products exclusively via the Internet. Internet banks have no physical branches, keeping their fees for the products on offer relatively low. Due to the limited points of contact available, the level of support offered can be drastically different from those of traditional financial institutions.

Operating system

A program run on a device to manage system resources, such as processor, storage media and input and output devices, and which offers these resources to application programs (software). Some well-known operating systems are Windows, macOS, Linux, Android and iOS.

Password

Serves for authentication. This means agreeing on and using a character string for someone, usually a person, to identify themselves and confirming their own identity this way.

A good password (https://www.ebas.ch/en/4-protecting-online-access/) should have at least 12 characters and consist of numbers, upper and lower case letters as well as special characters.

See also: Authentification (https://www.ebas.ch/en/glossary/authentification/)

Patch

This is a program correction which repairs bugs in software. Most patches are offered free-of-charge for download by software manufacturers on their website, or distributed automatically.

See also: Upgrade (https://www.ebas.ch/en/glossary/upgrade/)

Pharming

Just like classic phishing, pharming belongs to the Man-in-the-Middle group of attacks. With pharming, you will be redirected to a fake website by means of an IP address and domain allocation manipulation.

See also: Man-in-the-Middle (MitM) (https://www.ebas.ch/en/glossary/man-in-the-middle/)

Phishing

This term is made up from the words “password” and “fishing”. Attackers use phishing (https://www.ebas.ch/en/phishing/) to obtain confidential data from unsuspecting Internet users. These might for instance involve access data for your e-banking facility or account information of online shops. Perpetrators abuse their victims’ good faith and helpfulness by purporting to be, say, an employee of a trustworthy financial institution.

There are a variety of other variations such as Vishing (voice phishing or phone phishing), Smishing (SMS / text phishing) and QR phishing in addition to classic phishing via e-mail.

See also: Man-in-the-Middle (MitM) (https://www.ebas.ch/en/glossary/man-in-the-middle/)

Provider

This is the provider of access to the Internet, i.e. the organisation or company enabling users to connect their device to the Internet.

Quick Response code

Originally, QR codes (https://www.ebas.ch/qrcode) were used to mark assemblies and components in the car manufacturing sector. Nowadays, QR codes are also used for invoices (QR invoices (https://www.ebas.ch/en/qr-invoices/)) as well as in the publishing and marketing sectors to link physical objects (products, print media, posters, etc.) with the online world and make additional information available this way. As the contents of QR codes cannot readily be decoded by humans, these codes have to be scanned in first, e. g. using a smartphone.

Users cannot usually see what kind of information is coded into them before scanning in a QR code. If possible, they should therefore use a QR code scanner (app) which displays the decoded contents first and asks them whether they would actually like to visit a link or execute a certain action.

Example QR code by “eBanking – but secure!”

Ransomware

This is malware which encrypts files on a device and any network drives and storage media connected with it (e. g. external hard drives, cloud storage media) and demands a ransom payment.

See also: Malware (https://www.ebas.ch/en/glossary/malware/)

Remote Desktop and terminal server applications (RDP)

Applications enabling users to operate computer systems remotely. Primarily, this serves to transmit monitor displays, keystrokes and mouse movements across longer distances between a system and its users.

Rootkit

This is a software aiming to hide certain files, folders, processes or system entries from users and often also from your security software (anti-virus software). A rootkit in itself is not actually “harmful”, but an indication that malware is present on a computer.

See also: Malware (https://www.ebas.ch/en/glossary/malware/)

Scamming

Scamming is a colloquial term for “deceit” practised in a variety of contexts on the Internet. The primary aim is to defraud people of their money. One widespread method for instance is “romance scamming”. In this case, relationships are established by fooling people into believing that they are in love with the scammer and then asking them for money.

See also: Phishing (https://www.ebas.ch/en/glossary/phishing/) , Money Mule (https://www.ebas.ch/en/glossary/money-mule/) , Social engineering (https://www.ebas.ch/en/glossary/social-engineering/)

Scareware

This term is made up from the words “scare” and “software”. Based on misleading alert messages pointing e. g. to an infection of your device, you are supposed to become so scared and unsettled that you feel actually pressured, for instance into buying a dubious “anti-virus program” (which is then useless).

See also: Malware (https://www.ebas.ch/en/glossary/malware/)

Secure Sockets Layer (SSL)

This is the description of the predecessor of Transport Layer Security (TLS).

See also: Transport Layer Security (TLS) (https://www.ebas.ch/en/glossary/transport-layer-security/)

Security gap

A security gap is a term denominating a vulnerability found in any hardware or software which could trigger unexpected, unwanted system behaviour under certain conditions.

See also: Vulnerability (https://www.ebas.ch/en/glossary/vulnerability/)

Service Set Identifier (SSID)

This is the name of a WLAN.

See also: Wireless Local Area Network (WLAN) (https://www.ebas.ch/en/glossary/wireless-local-area-network/)

Session Riding

Contrary to phishing and pharming, session riding does not constitute a Man-in-the-Middle attack. Instead of diverting log-in information via an attacker, with session riding, any communication with a financial institution is manipulated straight on the victim’s device. To manipulate communications this way, malware which has infected a user’s device is to blame.

See also: Malware (https://www.ebas.ch/en/glossary/malware/)

Social engineering

This is an attack which does not really take place by technical, but by psychological means. It is a wide-spread method of snooping on confidential information. This always targets humans. To obtain such confidential information, it is not only people's credulity and helpfulness which are being exploited, but also their insecurities. Anything from faked telephone calls to people pretending to be someone else and phishing attacks is possible.

Spam

This is the umbrella term for unwanted e-mails which often contain advertising materials. Phishing mails, aiming to steal personal data from the recipient, also count as spam.

See also: Spam filter (https://www.ebas.ch/en/glossary/spam-filter/)

Spam filter

Filters unwanted spam e-mails from your inbox.

See also: Spam (https://www.ebas.ch/en/glossary/spam/)

Spyware

This is malware capturing information about a device and user online behaviour without their knowledge, and then passing it on. The recipients of this information can then reconstruct a user's habits when surfing and online shopping. Such spyware is usually set up when shareware or freeware software is installed on a device, too.

See also: Malware (https://www.ebas.ch/en/glossary/malware/)

Transaction number (TAN)

This is a kind of one-off password which is used in addition to a password or PIN. TANs can be generated and displayed to users in different ways - e. g. mobile TANs (mTAN) which is transmitted by financial institutions to users via a SMS, or photo TANs, which are displayed after decrypting a coloured mosaic pattern.

Transmission Control Protocol/Internet Protocol (TCP/IP)

This is a protocol suite comprising the underlying communication protocols of the Internet. These are also frequently used inside private networks.

Transport Layer Security (TLS)

This is a hybrid encryption protocol for secure data transmission on the Internet.

See also: Secure Sockets Layer (SSL) (https://www.ebas.ch/en/glossary/secure-sockets-layer/)

Trojan Horse

Malware disguising itself as something useful or a game, however with completely different objectives in reality. Trojans can for instance capture, change or delete passwords or other confidential data, or transmit them to an attacker.

See also: Malware (https://www.ebas.ch/en/glossary/malware/)

Two-factor authentification (2FA)

With so-called two-factor authentification, a second, independent security component is requested in addition to the first security component (generally a password) . This might be a code sent to your mobile phone or generated directly on your device.

See also: Logging in (https://www.ebas.ch/en/glossary/logging-in/) , Authentification (https://www.ebas.ch/en/glossary/authentification/)

Unicode

An international standard, which lays down a digital code for all meaningful characters or text elements of all known written cultures and character systems for the long term. The purpose is to do away with different and incompatible codings in different countries or cultural areas, Unicode is continuously complemented by additional scripts.

See also: American Standard Code for Information Interchange (ASCII) (https://www.ebas.ch/en/glossary/american-standard-code-for-information-interchange/)

Uniform Resource Locator (URL)

Denotes the address of a website - e. g. https://www.ebas.ch (https://www.ebas.ch) . In contrast to a domain, a Url also comprises the protocol (e. g. https://) and potentially details such as the port (e. g. :80)

See also: Domain (Domain name) (https://www.ebas.ch/en/glossary/domain/)

Update

program actualisation which often also repairs bugs in software. Most updates are offered free-of-charge for download by software manufacturers on their website, or distributed automatically.

See also: Patch (https://www.ebas.ch/en/glossary/patch/) , Upgrade (https://www.ebas.ch/en/glossary/upgrade/)

Upgrade

Expansion/extension of a system or software. The term “upgrade” was first only used for a hardware-related extension, although it is now (almost) synonymous with “update”. Some software providers differentiate between a free-of-charge update (usually provided to resolve errors, etc.) and a fee-based upgrade (usually also containing some additional features).

See also: Patch (https://www.ebas.ch/en/glossary/patch/)

User name

This is the name used by users to identify themselves in a system. When logging into a program or service (e. g. when e-banking), you will usually be asked for a user name and password. These will serve to identify authorised users.

See also: Authentification (https://www.ebas.ch/en/glossary/authentification/) , Logging in (https://www.ebas.ch/en/glossary/logging-in/)

Virtual Private Network (VPN)

Designates a virtual private (self-contained) communications network. VPNs are generally used to connect a device via an existing (unsecured) network, for instance the Internet, to another (secured) one, for instance a company network, in a safe manner. In the process, content is protected by way of encryption (end to end encryption) during transmission.

Virus

Although every user is still aware of this term, there are generally hardly any real (company) viruses in circulation any longer today. A classic (computer) virus infects existing files on a device in the hope that one of them is passed on to another user. If malware does not make any attempt to actively distribute itself, you call it a virus. If malware however is able to also spread automatically, e. g. by e-mail, you call it a worm.

See also: Malware (https://www.ebas.ch/en/glossary/malware/) , Worm (https://www.ebas.ch/en/glossary/worm/)

Vulnerability

A vulnerability is a term denominating a vulnerability found in any hardware or software which could trigger unexpected, unwanted system behaviour under certain conditions.

Wi-Fi Protected Access

Wi-Fi Protected Access is a method of encryption used for wireless networks (Wi-Fi) which in contrast to WEP provides additional protection via a dynamic key. WPA2 is the successor of WPA, although vulnerabilities are still known for both WPA and WPA2. Because of various attacks on the WPA and WPA2 process, it is preferable to use their successor WPA3.

See also: Advanced Encryption Standard (AES) (https://www.ebas.ch/en/glossary/advanced-encryption-standard/) , Wireless Local Area Network (WLAN) (https://www.ebas.ch/en/glossary/wireless-local-area-network/)

Wireless Local Area Network (WLAN)

This is a cable-free, local network or a wireless network. This can also be called Wi-Fi.

See also: Advanced Encryption Standard (AES) (https://www.ebas.ch/en/glossary/advanced-encryption-standard/) , Local Area Network (LAN) (https://www.ebas.ch/en/glossary/local-area-network/) , Service Set Identifier (SSID) (https://www.ebas.ch/en/glossary/service-set-identifier/) , Wi-Fi Protected Access (https://www.ebas.ch/en/glossary/wi-fi-protected-access/)

World Wide Web (WWW)

The WWW was developed by the European Research Centre for Nuclear Physics (CERN) in Lausanne (Switzerland) as a hypermedia system for the Internet in 1993. The other agency involved in this development was the NCSA (National Center for Supercomputing Applications, University of Illinois, USA). By now, the WWW Consortium (W3C) is developing the WWW further.

See also: Browser (https://www.ebas.ch/en/glossary/browser/)

Worm

Worms, just like viruses, are no longer such a widespread type of malware today. A worm is a small program which distributes copies by itself, e. g. via e-mail, SMS or via a vulnerability.

See also: Malware (https://www.ebas.ch/en/glossary/malware/) , Virus (https://www.ebas.ch/en/glossary/virus/)

Zero-Day-Gap

A vulnerability inside a software not yet known to the manufacturer, so that there is no patch yet. “Zero Day” means that there are “zero days” between the discovery of this vulnerability and the first attack.

See also: Exploit (https://www.ebas.ch/en/glossary/exploit/) , Malware (https://www.ebas.ch/en/glossary/malware/) , Patch (https://www.ebas.ch/en/glossary/patch/) , Ransomware (https://www.ebas.ch/en/glossary/ransomware/) , Security gap (https://www.ebas.ch/en/glossary/security-gap/) , Vulnerability (https://www.ebas.ch/en/glossary/vulnerability/)