Glossaire

Adresse IP

Adresse d'un appareil connecté dans un réseau informatique. Cette dernière est basée sur le protocole Internet (Internet Protocol). À chaque appareil connecté au réseau correspond une adresse IP qui permet de l'identifier et de le rendre adressable et accessible.

Voir également : Transmission Control Protocol/Internet Protocol (TCP/IP) (https://www.ebas.ch/fr/glossary/transmission-control-protocol-internet-protocol-tcp-ip/) , Domain Name System (DNS) (https://www.ebas.ch/fr/glossary/domain-name-system/)

Adresse MAC

L'adresse MAC est le numéro d'identification d'un appareil réseau (p. ex. d'une carte wifi). Il s'agit d'un numéro de référence généralement attribué en usine. Cette adresse peut être comparée au numéro de châssis d'un véhicule.

Advanced Encryption Standard (AES)

Méthode de chiffrement des données. L'AES s'utilise par exemple pour chiffrer les données transmises dans un réseau WLAN (WPA2, WPA3). De cette manière tout le trafic échangé entre un router WLAN et un dispositif sans fil connecté au réseau est ainsi chiffré.

Voir également : Wi-Fi Protected Access (WPA) (https://www.ebas.ch/fr/glossary/wi-fi-protected-access-wpa-wpa2-wpa3/) , Wireless Local Area Network (WLAN) (https://www.ebas.ch/fr/glossary/wireless-local-area-network-wlan-wi-fi/)

Adware

Le terme adware est un mot-valise anglais, contraction de « advertisement » (soit publicité en français) et « software » (logiciel). En plus de sa fonction principale, ce type de programme affiche de la publicité destinée à l'utilisateur, ou installe des logiciels supplémentaires conçus pour afficher de la publicité.

Voir également : Malware (https://www.ebas.ch/fr/glossary/malware/)

American Standard Code for Information Interchange (ASCII)

Ce système de codage comprend 95 caractères imprimables et 33 caractères non imprimables. Les caractères imprimables comprennent l'alphabet latin (A-Z, a-z), les dix chiffres arabes (0-9), ainsi que les signes de ponctuation et autres caractères spéciaux.

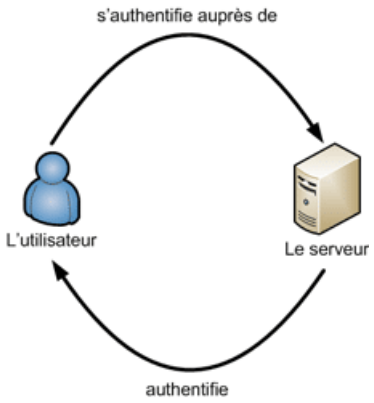
Voir également : Unicode (https://www.ebas.ch/fr/glossary/unicode/)

Applications de contrôle à distance et de configuration de terminal (Terminal Server) (RDP)

Applications permettant aux utilisateurs de contrôler des systèmes informatiques à distance. Il s'agit en premier lieu de transmettre l'affichage de l'écran, les saisies sur le clavier et les mouvements de la souris sur de longues distances, entre le système contrôlé et l'utilisateur.

Authentification

Procédé permettant de vérifier l'identité prétendue d'une personne ou d'un dispositif au moyen d'un ou de plusieurs éléments (p. ex. mot de passe, carte à puce ou empreinte digitale).



Voir également : Authentification à deux facteurs (2FA) (https://www.ebas.ch/fr/glossary/authentification-a-deux-facteurs-2fa/) , Autorisation (https://www.ebas.ch/fr/glossary/autorisation/)

Authentification à deux facteurs (2FA)

Dans la méthode d'authentification à deux facteurs, l'utilisateur souhaitant se connecter à son compte doit saisir, en plus du premier élément de sécurité (généralement un mot de passe), un deuxième élément de sécurité indépendant. Il peut s'agir par exemple d'un code numérique envoyé sur votre téléphone mobile ou généré directement par ce dernier.

Voir également : Ouvrir une session (https://www.ebas.ch/fr/glossary/ouvrir-une-session-se-connecter-se-loguer/) , Authentification (https://www.ebas.ch/fr/glossary/authentification/)

Autorisation

Attribution de droits d'accès. En fonction de ses droits d'accès, un utilisateur est autorisé, après avoir été identifié et authentifié avec succès, à accéder à des ressources (p. ex. fichiers, logiciels, paiement, etc.).

Voir également : Authentification (https://www.ebas.ch/fr/glossary/authentification/)

Backdoor

Terme anglais signifiant « porte dérobée ». Pour un software, une backdoor désigne un accès secret qui permet au fabricant (ou tiers) de s'introduire dans le logiciel ou d'accéder aux données de l'utilisateur depuis l'extérieur.

Voir également : Malware (https://www.ebas.ch/fr/glossary/malware/)

Backup

Sauvegarde de données au cours de laquelle des informations ou données électroniques sont copiées sur un support de stockage (p. ex. sur un disque dur externe). En règle générale, les backups doivent être effectués à intervalles réguliers.

Banques en ligne

Les banques en ligne ne proposent leurs produits que sur Internet. Elles ne possèdent pas de filiales physiques, ce qui leur permet d'être très compétitives par rapport aux frais bancaires. En raison des possibilités de contact très limitées, l'assistance offerte en cas de problème peut être très inférieure à celle des instituts bancaires traditionnels.

Bit

Il s'agit de la plus petite unité informatique existant au niveau de la transmission électronique des données. Dans un bloc d'information, il ne peut prendre que deux valeurs, le 0 et le 1.

Blockchain

Chaîne de blocs d'informations reliés entre eux et sécurisés par une empreinte cryptographique. L'application la plus connue de la technologie blockchain est le bitcoin, où la chaîne de blocs représente un registre de compte sécurisé contenant l'historique des transactions.

Voir également : Cryptomonnaie (https://www.ebas.ch/fr/glossary/cryptomonnaie/)

Bluetooth

Standard de communication sans fil de courte distance. Il permet d'obtenir un débit de transmission allant jusqu'à 1MBit par seconde et une portée pouvant aller jusqu'à 100 mètres.

Botnet

Il s'agit de réseaux constitués le plus souvent de plusieurs milliers de dispositifs infectés reliés entre eux à la suite d'une attaque par un logiciel malveillant (malware). Pour créer de tels réseaux, les cyberpirates installent, la plupart du temps à l'insu de leurs propriétaires, des bots sur les dispositifs cibles (un bot est un programme informatique automatique), pour les utiliser à des fins malveillantes, telles que lancer des attaques DDoS, relayer du spam ou miner de la cryptomonnaie. La plupart des bots peuvent être surveillés et recevoir des ordres du maître du réseau à travers un canal de communication.

Voir également : Distributed Denial-of-Service (DDoS) (https://www.ebas.ch/fr/glossary/distributed-denial-of-service-ddos/) , Cryptomonnaie (https://www.ebas.ch/fr/glossary/cryptomonnaie/) , Malware (https://www.ebas.ch/fr/glossary/malware/)

Cache

Le cache ou mémoire cache est une mémoire rapide qui permet d'accéder rapidement à des données (lors d'accès répétés). Dans le cadre d'Internet, les navigateurs stockent les contenus des pages visitées de manière à ne pas avoir à les télécharger une nouvelle fois lors d'une prochaine visite et de pouvoir les afficher plus rapidement.

Carding

Ce terme est utilisé pour décrire la détention, la diffusion et l'utilisation de cartes bancaires ou de numéros de cartes bancaires volés. Le carding comprend également l'utilisation illicite de données personnelles et le blanchiment d'argent.

Centre national pour la cybersécurité (NCSC)

Dal 1.1.2024 il Centro nazionale per la cibersicurezza (NCSC) ha cambiato nome in Ufficio federale della cibersicurezza (UFCS).

Cheval de Troie

Malware qui se fait passer en premier plan comme une application utile ou un jeu mais qui en réalité ne l'est pas et exécute d'autres fonctions en arrière-plan. Les trojans peuvent par exemple espionner, modifier, supprimer ou transférer à des cyberpirates des mots de passe et d'autres données confidentielles.

Voir également : Malware (https://www.ebas.ch/fr/glossary/malware/)

Cookie

Il s'agit de fichiers texte générés lors du chargement des pages web puis stockés sur les dispositifs des internautes, ce qui permettra de les reconnaître lors de leur prochaine visite sur le même site. Ils pourront ainsi accéder automatiquement à leurs comptes ou retrouver les articles qu'ils avaient sélectionnés dans leur panier.

Or les cookies peuvent aussi être utilisés par des réseaux publicitaires pour enregistrer le comportement des utilisateurs et afficher des publicités ciblées.

Crypto-Wallet

Les cryptoactifs sont stockés sous forme numérique dans des portefeuilles ou wallet dont l'accès est protégé par des codes d'accès.

Voir également : Cryptomonnaie (https://www.ebas.ch/fr/glossary/cryptomonnaie/)

Cryptographie

Science du chiffrement utilisée pour transmettre et conserver des informations de manière à les rendre inaccessibles à d'autres.

Cryptominage

Le cryptominage consiste à générer des unités (coins) d'une cryptomonnaie (p. ex. Bitcoin) et à vérifier de nouvelles transactions. Comme les cryptomonnaies ne sont généralement pas émises par une instance supérieure, elles sont générées par des cryptomineurs qui enregistrent, vérifient et comptabilisent toutes les transactions.

Voir également : Cryptomonnaie (https://www.ebas.ch/fr/glossary/cryptomonnaie/)

Cryptomonnaie

Les cryptomonnaies sont des actifs ou des moyens d'échange ou de paiement numériques qui utilisent des procédés cryptographiques pour garantir la sécurité du système de paiement. Après avoir paralysé un système avec un logiciel malveillant, les cybercriminels exigent généralement un paiement en cryptomonnaie (p. ex. bitcoins) pour empêcher toute traçabilité.

Darknet

Le darknet permet aux internautes d'agir de manière pratiquement anonyme. Cette partie occulte d'Internet est utilisée par des personnes qui accordent une importance particulière à leur vie privée ou qui vivent dans un système politique répressif – mais aussi très souvent par des criminels.

Distributed Denial-of-Service (DDoS)

Une attaque DDoS (ou par déni de service distribuée) est une attaque portée contre le site web ou le serveur d'une entreprise. De nombreux dispositifs (appartenant généralement tous à un botnet) se mettent alors à bombarder leur cible de requêtes. Objectif : saturer le site ou le serveur pour le perturber ou le rendre indisponible. Les attaques DDoS portées contre les entreprises sont souvent des tentatives de chantage. Si l'entreprise ne paie pas, les cybercriminels menacent de répéter leur attaque.

Voir également : Botnet (https://www.ebas.ch/fr/glossary/botnet/)

Domain Name System (DNS)

Le système de noms de domaine est un service permettant de traduire un nom de domaine (p. ex. www.ebas.ch) en une adresse IP (217.26.54.120).

Dropper et injecteur

Un dropper est un petit programme malveillant dont la tâche consiste à exécuter un malware généralement plus important sur un système.

Un injecteur est un dropper chargé de télécharger un programme malveillant depuis le réseau Internet.

Voir également : Malware (https://www.ebas.ch/fr/glossary/malware/)

Empreinte numérique

Procédé permettant de vérifier une clé de chiffrement, sans devoir nécessairement contrôler l'ensemble de la clé. De cette manière, il est possible par exemple de vérifier l'authenticité d'un certificat sur lequel repose une connexion TLS/ SSL. Une empreinte électronique se présente la plupart du temps comme une chaîne hexadécimale composée de chiffres de 0 à 9 et de lettres de A à F.

Exploit

Un **exploit** désigne un programme malveillant exploitant une faille donnée dans le but de compromettre un système.

Faille de sécurité

Une faille de sécurité désigne une faille constatée dans un matériel ou un logiciel informatique permettant, dans certaines conditions, de déclencher dans le système un comportement imprévu ou involontaire.

Voir également : Vulnérabilité (https://www.ebas.ch/fr/glossary/vulnerabilite/)

Faille zero-day

Ce terme indique une faille de sécurité dans un logiciel, pour laquelle le fabriquant n'a pas encore publié de correctif. La référence au jour zéro signifie que la faille a été découverte et que des cybercriminels peuvent l'exploiter pour porter des attaques.

Voir également : Exploit (https://www.ebas.ch/fr/glossary/exploit/) , Malware (https://www.ebas.ch/fr/glossary/malware/) , Patch (https://www.ebas.ch/fr/glossary/patch/) , Ransomware (https://www.ebas.ch/fr/glossary/ransomware-rancongiciel/) , Faille de sécurité (https://www.ebas.ch/fr/glossary/faille-de-securite/) , Vulnérabilité (https://www.ebas.ch/fr/glossary/vulnerabilite/)

Fermer une section

Procédure de déconnexion d'un utilisateur. En se déconnectant, l'utilisateur donne l'ordre au système de terminer sa session.

Voir également : Ouvrir une session (https://www.ebas.ch/fr/glossary/ouvrir-une-session-se-connecter-se-loguer/)

Filtre anti-spam

Sert à filtrer les courriels de spam non sollicités dans la boîte de réception.

Voir également : Spam (https://www.ebas.ch/fr/glossary/spam/)

Fournisseur d'accès à Internet

Le fournisseur d'accès à Internet est l'organisme ou l'entreprise qui permet à l'utilisateur de se connecter au réseau Internet avec son dispositif.

Fraude à l'investissement

La fraude à l'investissement est une forme d'escroquerie qui consiste à inciter des personnes, par des informations mensongères ou trompeuses, à investir dans des projets ou des produits. Ces opportunités d'investissement sont souvent fictives ou très surévaluées et les risques sont délibérément dissimulés. Le but de cette arnaque consiste à extorquer de l'argent aux investisseurs en leur promettant des gains ou des avantages souvent irréalistes.

Hyperlien

Sur les sites web par exemple, un hyperlien est une référence qui permet de passer en un clic à un autre document électronique ou à un autre emplacement au sein d'un même document. Sur le web, les objets cibles peuvent se trouver sur d'autres sites web.

Infection par « drive-by download »

Ce terme désigne l'infection d'un dispositif par un malware lors d'une simple visite sur un site web. Il s'agit pour la plupart de sites sérieux ayant été piégés par des cybercriminels dans le but de propager leurs logiciels malveillants. Le simple fait de se rendre sur un site contaminé suffit pour infecter le dispositif.

Voir également : Malware (https://www.ebas.ch/fr/glossary/malware/)

Ingénierie sociale

Ce type d'attaque est davantage axé sur la dimension psychologique que technologique. Il s'agit d'une méthode d'espionnage répandue qui vise à obtenir l'accès à des données confidentielles. La cible de l'attaque est toujours la personne humaine. Pour soutirer des informations confidentielles, les arnaqueurs appellent leurs victimes au téléphone et exploitent très souvent leur bonne foi, leur serviabilité, mais aussi leur insécurité en se faisant passer pour quelqu'un d'autre, ou en recourant à des attaques de hameçonnage.

Internet des objets, Internet of Things (IoT)

Terme collectif désignant les technologies qui permettent de mettre en réseau des objets, qu'ils soient physiques ou virtuels, et de les faire communiquer entre eux. Les appareils disposent en général de capteurs pour collecter toutes sortes de données sur l'environnement qui les entoure, ainsi que de logiciels embarqués pour échanger ces données avec d'autres dispositifs et systèmes. Parmi les exemples les plus courants, citons la domotique (chauffage), la surveillance des paramètres de santé (montres connectées) ou la surveillance de l'environnement (stations météo).

Jailbreak

Élimination non autorisée des restrictions d'utilisation de smartphones en particulier. Cette manipulation consiste à modifier le système d'exploitation à l'aide d'un logiciel spécifique pour accéder à des fonctionnalités internes telles que le système de fichiers. Le jailbreak peut nuire considérablement à la sécurité et à la stabilité du système d'exploitation.

Java

Langage de programmation informatique orienté objet et indépendant vis-à-vis de la plateforme. Pour exécuter les programmes Java sur un ordinateur, il est nécessaire d'installer au préalable l'environnement d'exécution Java.

JavaScript

Langage de programmation de script utilisé pour dynamiser l'affichage des pages web. JavaScript permet de modifier ou de recharger des contenus et notamment d'afficher des suggestions pendant la saisie d'un mot-clé par exemple.

Keylogger

Logiciel malveillant chargé de consigner les frappes de l'utilisateur sur le clavier dans le but de se procurer des identifiants de connexion et notamment des mots de passe.

Voir également : Malware (https://www.ebas.ch/fr/glossary/malware/)

La signature numérique

Il s'agit d'un sceau numérique permettant d'établir un lien univoque et non manipulable entre une personne physique et un document électronique (p. ex. un courriel). Une empreinte numérique (ou « hash ») est obtenue à partir du document signé suite à une transformation mathématique. Cette valeur de hash est ensuite chiffrée avec la clé de signature secrète de l'expéditeur et envoyée au destinataire en même temps que le document original. Celui-ci utilise ensuite le même procédé de calcul mathématique pour obtenir une valeur de hash à partir du document. Avec la clé publique de l'expéditeur, il va également déchiffrer la valeur de hash qu'il a reçue de la part de l'expéditeur. Si ces deux valeurs sont identiques, il peut être certain de l'intégrité du document et que l'expéditeur est bien qui il prétend être.

Local Area Network

L'acronyme anglais LAN désigne un réseau informatique local. Dans ce type de réseau, les stations de travail, serveurs et autres périphériques se trouvent à quelques centaines de mètres de distance (au maximum), et généralement dans le même bâtiment ou complexe.

Voir également : Wireless Local Area Network (WLAN) (https://www.ebas.ch/fr/glossary/wireless-local-area-network-wlan-wi-fi/)

Macro

Certains logiciels (p. ex. la suite Microsoft Office, Adobe Acrobat) permettent aux utilisateurs d'automatiser un certain nombre de tâches au moyen de petits programmes appelés « macros » ou « scripts ». Or, ces macros sont souvent utilisées par des escrocs pour introduire un code malveillant (malware) dans des documents à l'apparence inoffensive.

Voir également : Malware (https://www.ebas.ch/fr/glossary/malware/)

Malware

Le terme « malware » est un mot-valise anglais, contraction de « malicious » (malveillant) et « software », rendu en français par le terme « maliciel ». Malware est le terme générique pour désigner les logiciels malveillants qui exécutent des fonctions nuisibles sur un dispositif (ex. virus, vers, chevaux de Troie, rançongiciels...).

Voir également : Adware (https://www.ebas.ch/fr/glossary/adware-logiciel-publicitaire/) , Backdoor (https://www.ebas.ch/fr/glossary/backdoor/) , Botnet (https://www.ebas.ch/fr/glossary/botnet/) , Infection par « drive-by download » (https://www.ebas.ch/fr/glossary/infection-par-drive-by-download/) , Keylogger (https://www.ebas.ch/fr/glossary/keylogger/) , Ransomware (https://www.ebas.ch/fr/glossary/ransomware-rancongiciel/) , Rootkit (https://www.ebas.ch/fr/glossary/rootkit/) , Scareware (https://www.ebas.ch/fr/glossary/scareware/) , Session-Riding (https://www.ebas.ch/fr/glossary/session-riding-detournement-de-session/) , Spyware (https://www.ebas.ch/fr/glossary/spyware/) , Cheval de Troie (https://www.ebas.ch/fr/glossary/cheval-de-troie-trojan/) , Virus (https://www.ebas.ch/fr/glossary/virus/) , Ver (https://www.ebas.ch/fr/glossary/ver/)

Man in the middle (MitM)

Dans une attaque « man in the middle », ou en français « attaque de l'homme du milieu » (HDM), un malware (ou tiers) vient interférer dans une session d'e-banking. Concrètement, il s'interpose entre le dispositif de l'utilisateur et le serveur de l'institut financier pour contrôler le trafic de données.

Voir également : Phishing (https://www.ebas.ch/fr/glossary/phishing-hameconnage/) , Pharming (https://www.ebas.ch/fr/glossary/pharming/)

Mise à jour (logicielle)

Un actualisation souvent aussi servant à réparer les bugs (erreurs) des logiciels. La plupart des mises à jour logicielles sont téléchargeables gratuitement sur les sites web des éditeurs de logiciels ou diffusés de façon automatique.

Voir également : Patch (https://www.ebas.ch/fr/glossary/patch/) , Upgrade (https://www.ebas.ch/fr/glossary/upgrade/)

Money mule

Les mules (https://www.ebas.ch/fr/money-mules-agents-financiers/) ou passeurs sont des personnes qui se chargent, moyennant une rémunération, de recevoir des capitaux sur leur compte bancaire et de les faire suivre dans un pays étranger. Dans la quasi-totalité des cas, ces capitaux sont le fruit d'activités illégales. Ces « money mules » sont la plupart du temps recrutées par le biais d'offres d'emploi promettant des revenus à la fois rapides et élevés. Quiconque participe à de telles « affaires » risque une procédure pénale pour complicité de blanchiment d'argent.

Mot de passe

Moyen d'authentification consistant en une chaîne de caractères utilisée par un sujet, en général une personne, pour s'identifier et confirmer son identité.

Un bon mot de passe (https://www.ebas.ch/fr/les-conseils-a-suivre-pour-ouvrir-une-session-de-banking/) doit être composé au minimum de 12 caractères, dont des chiffres, des minuscules, des majuscules et des caractères spéciaux.

Voir également : Authentification (https://www.ebas.ch/fr/glossary/authentification/)

Navigateur

Programme dédié à l'affichage des pages web sur le World Wide Web (www) ou de documents et autres données. Les principaux navigateurs dans le domaine d'Internet sont Google Chrome, Mozilla, Firefox, Microsoft Edge et Apple Safari.

Voir également : World Wide Web (WWW) (https://www.ebas.ch/fr/glossary/world-wide-web-www/)

Nom de domaine

C'est le nom sous lequel on peut accéder à une ressource (comme un site web par exemple). Chaque nom de domaine est composé de plusieurs éléments séparés par des points. Par exemple, le nom de domaine de ce site est www.ebas.ch (http://www.ebas.ch) .

Nom d'utilisateur

C'est le nom par lequel un utilisateur s'identifie auprès d'un système. Au moment de créer un compte sur un programme ou un service (tel que l'e-banking par exemple), il est généralement nécessaire de saisir un nom d'utilisateur et un mot de passe. Ensemble, ils constituent les identifiants qui permettront à l'utilisateur de s'identifier par la suite.

Voir également : Authentification (https://www.ebas.ch/fr/glossary/authentification/) , Ouvrir une session (https://www.ebas.ch/fr/glossary/ouvrir-une-session-se-connecter-se-loguer/)

Numéro de transaction (TAN)

Mot de passe à usage unique ou OTP (One-time password) utilisé en plus du mot de passe ou du code PIN. Les TAN peuvent être générés et visualisés par l'utilisateur de différentes manières. Il existe par exemple les mobile TAN (ou mTAN), que l'institut financier envoie via SMS à l'utilisateur, ou les photo TAN qui s'affichent en décodant une mosaïque de couleurs.

Office fédéral de la cybersécurité (OFCS)

L'Office fédéral de la cybersécurité (OFCS) est le centre de compétences de la Confédération pour la cybersécurité et donc le premier interlocuteur des milieux économiques, de l'administration, des établissements d'enseignement et de la population pour toutes les questions portant sur cette thématique. Il est chargé d'assurer la mise en œuvre coordonnée de la cyberstratégie nationale.

Ouvrir une session

Procédure de connexion pour accéder à un dispositif par exemple ou à un service en ligne. En général, le processus sert à communiquer au système l'ouverture d'une session de travail et qu'un utilisateur souhaite être mis en relation avec son compte utilisateur, comme par exemple le compte d'e-banking.

Voir également : Fermer une section (https://www.ebas.ch/fr/glossary/fermer-une-section-se-deconnecter-se-deloguer/) , Authentification (https://www.ebas.ch/fr/glossary/authentification/)

Pare-feu

Système de sécurité servant à protéger un réseau d'ordinateurs ou un dispositif seul contre des attaques intempestives.

Patch

Correctif servant à réparer les bugs (erreurs) des logiciels. La plupart des patchs sont téléchargeables gratuitement sur les sites web des éditeurs de logiciels ou diffusés de façon automatique.

Voir également : Upgrade (https://www.ebas.ch/fr/glossary/upgrade/)

Pharming

Comme le phishing ou hameçonnage classique, le pharming est une technique de piratage informatique appartenant au groupe des attaques « man in the middle ». Il consiste en un détournement vers un site web frauduleux à travers la manipulation de l'attribution de l'adresse IP et du nom de domaine.

Voir également : Man in the middle (MitM) (https://www.ebas.ch/fr/glossary/man-in-the-middle-mitm/)

Phishing

Le mot anglais « phishing » est formé des mots « password » et « fishing », ce qui signifie la pêche aux mots de passe. À travers le phishing (https://www.ebas.ch/fr/le-phishing/) ou hameçonnage, les hackers tentent d'accéder aux données confidentielles des internautes et ce, à leur insu. Il peut s'agir par exemple d'identifiants pour l'e-banking ou d'informations concernant les comptes utilisateurs de différentes boutiques en ligne. Les malfaiteurs tirent parti de la crédulité et de la serviabilité de leurs victimes en se présentant comme des collaborateurs d'instituts financiers dignes de confiance.

Outre la technique classique du hameçonnage par email, il existe aujourd'hui différentes variantes telles que le phishing par téléphone, en anglais Vishing (Voice-Phishing ou Phone-Phishing), Smishing (phishing par SMS) et le QR-Phishing.

Voir également : Man in the middle (MitM) (https://www.ebas.ch/fr/glossary/man-in-the-middle-mitm/)

Quick Response Code (code QR)

À l'origine, le code QR (https://www.ebas.ch/qrcode) a été développé pour le marquage de modules et de pièces détachées dans la production automobile. Depuis, les codes QR sont utilisés dans la facture QR (https://www.ebas.ch/fr/la-facture-qr/) , les publications et dans le marketing, pour créer un lien entre des objets physiques (produits, presse écrite, affichages, etc.) et le monde de l'Internet, et mettre ainsi à disposition du public des informations plus détaillées. Comme le contenu des codes QR ne peut pas d'emblée être décodé par l'œil humain, le code QR doit tout d'abord être scanné, à l'aide d'un smartphone par exemple.

Ainsi, les utilisateurs ne peuvent généralement pas reconnaître les informations codées contenues dans un code QR. Il convient par conséquent d'utiliser, si possible, un scanner de code QR (application), qui va tout d'abord afficher les contenus décodés puis demander si l'on souhaite visiter un lien ou exécuter une action déterminée.

Exemple du code QR de « eBanking – en toute sécurité ! »

Ransomware

Logiciel malveillant dont la fonction est de verrouiller les données se trouvant sur un dispositif et sur tous les lecteurs réseau et supports de données connectés (p. ex. disques durs externes, espaces de stockage sur le cloud), pour demander ensuite une rançon à l'utilisateur en l'échange de leur déverrouillage.

Voir également : Malware (https://www.ebas.ch/fr/glossary/malware/)

Rootkit

Logiciel dont le but est de cacher à l'utilisateur, mais aussi bien souvent aux programmes de sécurité (antivirus), des données, des dossiers, des processus ou des éléments système. Un rootkit seul n'est pas « nuisible » en soi mais constitue un indice de la présence d'un logiciel malveillant sur l'ordinateur.

Voir également : Malware (https://www.ebas.ch/fr/glossary/malware/)

Scamming

Il s'agit d'un terme générique pour désigner toute sorte d'arnaques sur Internet. L'objectif des criminels est toujours d'extorquer de l'argent aux victimes. Une forme particulièrement répandue de «scam» ou d'arnaque est le «romance scam» qui consiste à établir une relation amoureuse avec une personne pour ensuite lui soutirer de l'argent.

Voir également : Phishing (https://www.ebas.ch/fr/glossary/phishing-hameconnage/) , Money mule (https://www.ebas.ch/fr/glossary/money-mule-passeur-dargent/) , Ingénierie sociale (https://www.ebas.ch/fr/glossary/ingenierie-sociale-social-engineering/)

Scareware

Le terme « scareware » est un mot-valise anglais, contraction de « scare » (qui signifie effrayer) et « software ». Effrayé et déstabilisé par des messages d'alarme trompeurs indiquant que son dispositif par ex. est infecté par un virus, l'utilisateur est par exemple convaincu d'acheter des logiciels antivirus louches (et qui ne servent à rien).

Voir également : Malware (https://www.ebas.ch/fr/glossary/malware/)

Secure Sockets Layer (SSL)

Le protocole SSL est le prédécesseur du Transport Layer Security (TLS).

Voir également : Transport Layer Security (TLS) (https://www.ebas.ch/fr/glossary/transport-layer-security-tls/)

Service Set Identifier (SSID)

C'est le nom d'un réseau sans fil (WLAN).

Voir également : Wireless Local Area Network (WLAN) (https://www.ebas.ch/fr/glossary/wireless-local-area-network-wlan-wi-fi/)

Session-Riding

Contrairement au phishing et au pharming, le détournement de session ne compte pas parmi les attaques « man in the middle ». Au lieu de détourner les données d'identification, l'attaquant manipule la communication entre la banque et le dispositif de la victime directement à partir de ce dernier. Pour que la manipulation soit possible, le cyberpirate doit infecter au préalable le dispositif de sa victime avec un logiciel malveillant.

Voir également : Malware (https://www.ebas.ch/fr/glossary/malware/)

Spam

Terme générique pour les courriers électroniques non sollicités, la plupart du temps à caractère publicitaire. Le spam désigne aussi généralement les mails de phishing, dont le but est de dérober les données personnelles du destinataire.

Voir également : Filtre anti-spam (https://www.ebas.ch/fr/glossary/filtre-anti-spam/)

Spyware

Malware dont le but est d'enregistrer et de transmettre les informations concernant un dispositif et le comportement en ligne de l'utilisateur à son insu. Les destinataires de ces informations peuvent par exemple en déduire les habitudes de l'utilisateur en matière de navigation ou d'achats en ligne. La plupart du temps, ces programmes espions se configurent sur le dispositif pendant l'installation de programmes shareware et freeware.

Voir également : Malware (https://www.ebas.ch/fr/glossary/malware/)

Système d'exploitation

Programme dont la fonction est de gérer les ressources système du dispositif sur lequel il est installé, tels que le processeur, les disques durs ou les périphériques d'entrée/sortie, et de les mettre à la disposition des applications (logiciels). Les systèmes d'exploitation les plus connus sont p. ex. Windows, macOS, Linux, Android et iOS.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Famille de protocoles comprenant les protocoles Internet de base. Ces derniers sont souvent utilisés dans les réseaux privés.

Transport Layer Security (TLS)

Protocole de chiffrement hybride servant à sécuriser le transfert de données sur Internet.

Voir également : Secure Sockets Layer (SSL) (https://www.ebas.ch/fr/glossary/secure-sockets-layer-ssl/)

Unicode

Il s'agit d'un standard international qui associe un code numérique à chaque caractère ou élément textuel porteur de sens de n'importe quel système d'écriture de signe. Le but est d'unifier des systèmes de codage divers et incompatibles utilisés dans les différents pays ou cultures. Unicode est constamment alimenté en caractères provenant de d'autres systèmes d'écriture.

Voir également : American Standard Code for Information Interchange (ASCII) (https://www.ebas.ch/fr/glossary/american-standard-code-for-information-interchange-ascii/)

Uniform Resource Locator (URL)

L'adresse d'un site web, comme par exemple https://www.ebas.ch (https://www.ebas.ch) . . Contrairement au nom de domaine, l'URL comprend également le protocole (p. ex. https://) et éventuellement d'autres indications telles que le port (p. ex. :80).

Voir également : Nom de domaine (https://www.ebas.ch/fr/glossary/nom-de-domaine/)

Upgrade

Amélioration/extension d'un système ou d'un logiciel. Utilisé dans un premier temps pour les évolutions des différents composants hardware, ce terme est pratiquement devenu synonyme aujourd'hui d'update. Certains fabricants de logiciels font une distinction entre les mises à jour gratuites ou updates (qui corrigent généralement les bugs, erreurs, etc.) et les mises à niveau ou upgrades payantes (qui contiennent généralement des fonctions supplémentaires).

Voir également : Patch (https://www.ebas.ch/fr/glossary/patch/)

Usurpation d'identité

C'est le fait de se présenter sous une fausse identité. Dans le contexte de l'e-banking, cela signifie qu'une personne tierce s'identifie auprès d'un institut financier avec des données d'accès qui ne sont pas les siennes et sous un nom étranger, pour obtenir un accès illimité aux comptes. Pour l'institut financier, il est très difficile de déterminer s'il s'agit bien de son client, d'un intermédiaire mandaté par ce dernier ou d'un escroc. L'usurpation d'identité est utilisée dans les attaques de phishing (https://www.ebas.ch/fr/le-phishing/) classique et pour permettre à des prestataires tiers d'accéder à des comptes bancaires (https://www.ebas.ch/fr/autoriser-ou-non-lacces-doperateurs-tiers-a-ses-comptes-bancaires/) .

Ver

Tout comme les virus, le ver n'est pas un malware très répandu aujourd'hui. Un ver est un petit programme qui se propage en envoyant des copies de lui-même, p. ex. par email ou en exploitant des failles de sécurité.

Voir également : Malware (https://www.ebas.ch/fr/glossary/malware/) , Virus (https://www.ebas.ch/fr/glossary/virus/)

Virtual Private Network (VPN)

Désigne un réseau de communication privé virtuel autonome. Un VPN est généralement utilisé pour connecter de manière sécurisée un dispositif via un réseau existant (non protégé), par exemple Internet, à un autre réseau (sécurisé), comme par exemple le réseau de l'entreprise. Pour ce faire, les données échangées sont protégées par cryptage pendant leur transport (chiffrement de bout en bout)

Virus

Si le concept parle encore beaucoup aux utilisateurs, il n'existe aujourd'hui pratiquement plus de véritables virus (informatiques). Le virus (informatique) classique infecte des fichiers présents sur un dispositif dans l'espoir qu'un de ces fichiers soit transmis à un autre utilisateur. On parle de virus lorsque le malware se répand de manière active, spontanément de par lui-même. Lorsque le malware est également capable de se diffuser automatiquement, par email p. ex., on parle alors de ver.

Voir également : Malware (https://www.ebas.ch/fr/glossary/malware/) , Ver (https://www.ebas.ch/fr/glossary/ver/)

Vulnérabilité

Une **vulnérabilité** désigne une faille constatée dans un matériel ou un logiciel informatique permettant, dans certaines conditions, de déclencher dans le système un comportement imprévu ou involontaire.

Wi-Fi Protected Access (WPA)

Le Wi-Fi Protected Access est une méthode de chiffrement pour les réseaux sans fil (WLAN). Contrairement au WEP, le WAP utilise un procédé dit de « clé dynamique », offrant ainsi une protection supplémentaire. Malheureusement, des vulnérabilités sont déjà connues pour le WPA, comme pour le WPA2 son successeur. Suite aux différentes attaques portées contre les procédés WPA et WPA2, il est recommandé d'utiliser leur successeur (WPA3).

Voir également : Advanced Encryption Standard (AES) (https://www.ebas.ch/fr/glossary/advanced-encryption-standard/) , Wireless Local Area Network (WLAN) (https://www.ebas.ch/fr/glossary/wireless-local-area-network-wlan-wi-fi/)

Wireless Local Area Network (WLAN)

Réseau local sans fil. Dans la langue courante, le WLAN est souvent remplacé par le terme wifi.

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

World Wide Web (WWW)

Le World Wide Web a été créé en 1993 par des collaborateurs du CERN (Centre européen de Recherches Nucléaires) à Lausanne en Suisse, comme système hypertexte pour le réseau Internet. Le NCSA (National Center for Supercomputing Applications) dans l'Illinois aux Etats-Unis participa également au développement de la « toile » mondiale. Le système fut ensuite parachevé par le WWW Consortium, également appelé W3C.

Voir également : Navigateur (https://www.ebas.ch/fr/glossary/navigateur/)