POPULAR BANK

Information Security Guide
Security Slopes

GLOSSARY

BANDWIDTH:
It refers to the amount of data that can be transferred between two points in a network in a specific time. Bandwidth is typically measured in bits per second (bps) and expressed as a bit rate; denotes the transmission capacity of a connection and is an important factor in determining the quality and speed of a network.

AUTHENTICATION:
Authentication is the process of detecting and verifying the identity of a user by validating the credentials (username and password) and consulting a specific authority.

BIDIRECTIONAL AUTHENTICATION:
It refers to the automatic and simultaneous recognition process that is carried out between a system and the user, through a device with an integrated microprocessor. It is useful to legitimize the parties involved in remote channel transactions.

BACK DOOR:
Malicious programs designed with the intention of opening a secret "back door" in computers, to allow access to the creator of this program without being detected.

BLUE JACKING:
It is a technique consisting of sending unsolicited information between devices using Bluetooth. For example, laptops, tablets, or mobile phones. Normally a bluejacker only sends text messages, although through smartphones it is also possible to send images, sound, and files. It does not intercept information, but it can cause damage to the device's system.

BOTNET:
Short name for robot network or robotic network, it is also known as a zombie army. It refers to the network of vulnerable and unprotected computers connected to the Internet, which are remotely controlled by spammers to program them to send millions of emails.
After scanning the Internet and finding vulnerable computers, spammers install malicious programs (malware) on them or trick users into downloading music or games for free.

BIT:
Contraction of the Anglo-Saxon term binary digit (binary digit), it is the basic unit of information for computers and telecommunications; It is the amount of information stored by a digital device or physical system that exists in one of two possible stages, such as, for example, two levels of current or intensity of electricity, two positions in a switch, two directions of polarity, etc.

In the computer environment, a bit is the variable with two conditions that are frequently interpreted as binary digits 0 and 1, the logical True/False duality, the algebraic signs +/−, the activation modes (on/off), among others.

BYTE:
In the computer and telecommunications environment, it is the unit of digital information that consists of eight (8) bits. From there kilobyte, megabyte, terabytes, or petabytes are derived. It was created by Dr. Werner Buchholz, during the design phase of the IBM Stretch computer, in July 1956.

CACHÉ:
Temporary memory of computers. It is the one that serves to store the suspended information before executing any definitive action with respect to it, such as cutting and pasting data from one place to another. It is the one that stores the sequence of previous steps that a user has carried out in any program and that is reversed by simply pressing the arrow or undo button (“undo”).

MESSAGES CHAIN:
These are email messages in which you encourage them to forward the message to more recipients so that they, in turn, also forward it. It is one of the possible sources of saturation of the service with email, since they often carry fake news, may contain malicious programs, etc.

DIGITAL CERTIFICATE:
It is an authorized signature that identifies a valid entity. These are issued by certifying entities, which are used to authenticate an entity or persons. The security of the certificate is protected by cryptographic techniques of the highest level.

ENCRYPTION:
Data encoding using various mathematical techniques that guarantee its confidentiality and the integrity of the information during the transmission and storage process.

MALICIOUS CODE:
Any program that is installed with the intention of causing damage or stealing information. They are generally designed to run without user intervention or consent.

PASSWORD OR SECRET KEY:
A set of letters, numbers, and symbols used to authenticate users to a computer system. To be effective, best practices recommend composing it in a way that is robust and difficult to crack. For example:

- Common name –» Clownfish
- Scientific name –» Amphiprion akallopisos
- Strong password –» @mph1pr10n@k@110p1505
- (substitutes the letter “a” for @, the “i” for 1 and the “s” for 5)

DATA COMPROMISE:
It refers to the organized theft of information from ATMs, debit, or credit cards, mainly from businesses, by detecting and taking advantage of weaknesses in the business systems and processing subcontractors, or computers, storage devices or industrial espionage promoted by third parties.

COOKIES:
They are small data files that the server of an Internet page sends to the visiting computer, through the browser, and retrieves later with each new connection. These are stored on the hard drive of the Internet user's computer or cell phone and allow the PER (site) to recover the characteristics and/or browsing preferences of the previous session.
Those used by Popular Bank Ltd. Inc. are not invasive, malevolent, or harmful and do not collect personal data. However, if you want, you can disable them by following the browser's instructions. You can also permanently delete the ones you have stored on your computer, or cell phone, by accessing the corresponding directory and selecting the options that delete it or do not allow it to be stored.

ELECTRONIC MAIL:
It is the system of personal communication by computer via computer networks. Through it you can send not only text, but all kinds of digital documents.

CRACKER:
Abbreviation of the term in English criminal hacker, refers to a person who uses his vast knowledge of systems, networks, and computers to obtain personal profit by breaking into the information systems of companies without authorization, with the aim of evading security systems and destroying, expose or steal their information.

CRYPTOGRAPHY:
Discipline that deals with the security of electronic transmission and storage of information.

DDOS:
Acronyms for “distributed denial of service” or “denial of service”. It consists of the massive and simultaneous sending of requests to the systems to block or saturate the operation of the equipment and disable them from providing the proper service to the users.

POS DEVICE:
Device by which sales transactions can be debited directly to a customer's bank account or credit card. They are installed in all physical commercial establishments and, through them, the business swipes credit and/or debit cards when making a payment. In the virtual deployment, the cash out is done by asking the Internet user to enter the data corresponding to the address where the credit card statements are sent.

ENCRYPTATION:
The process that converts your data into an encrypted code before sending it over the Internet, preventing unauthorized users from reading it later.

EXTENTION:
Refers to the last three (3) letters after the dot in the full name of a file. They are normally used by the operating system to associate that file with a particular program. Thus, for:

- For the MS-Word documents, the extension is .doc or .docx,
- For the MS-Excel spreadsheets, the extension is .xls or .xlsx,
- And for MS-PowerPoint presentations, the extension is .ppt or .pps

CONTENT FILTERING:
They are technologies that allow establishing what content is allowed to be shown to a user when browsing the internet. It also applies to email filtering, which prevents the entry of emails considered inappropriate (spam, viruses, unethical material, etc.).

ELECTRONIC SIGNATURE:
Digital information associated with a particular operation carried out on the Internet that, together with the certificates, allows guaranteeing the identity of the participants in a transaction.

WORM:
It is a type of malware that can reproduce itself and whose main function is to cause a rejection of service. This type of program, when played, uses disk space, and slows down your computer's processing speed.

HACKER:
Person who has computer knowledge, sometimes very deep, whose sole objective is to highlight his ability to infiltrate company networks and go unnoticed by security filters to access their information systems.

HOAX:
It is an attempt to make a group of people believe that something false is real. It is very commonly used by sending mass emails.

SOCIAL ENGINEERING:
Techniques that attempt to attack the security of computer systems by tricking their users and administrators using persuasion or using a false identity to obtain confidential information.

INTERNET USER:
Person who accesses the Internet through a computer with a connection service and a browser program, also known as a browser.

INTRUSION:
Computer attack in which the attacker gains complete control over the computer.
During an intrusion, the attacker can obtain and alter all the data on the computer, modify its operation and even attack new computers.

PER
Acronym for page or pages on the network, or on the Internet, Spanish term to define webpage, web, website, or site according to the Foundation for an Urgent Spanish (Fundéu).

FIREWALL:
Equipment or security system that allows controlling which equipment and which services can be accessed within a network. It can be a specialized security equipment, or a program installed on a computer (personal firewall).

PIN (PRIVATE IDENTIFICATION NUMBER):
Private identification numbers, for its acronym in English.

PLUG-IN:
Programming module that adds specific functionality to the Internet browser. The most common, for example, in Flash or HTML5 format, allow you to view videos or listen to music.

ANTI SPY PROGRAM:
It is a specialized program, designed to protect your computer from attacks and unauthorized automatic installation of applications that collect and forward your personal information.

ANTIVIRUS PROGRAM:
It is a program designed to detect and prevent malware from entering the computer, its possible spread and infection of other computers connected to the same network. Malware can spread quickly, so you should ensure your antivirus is running regularly and up to date.

IDENTITY THEFT:
Fraud that is perpetrated using another person's data without their consent, to compromise services or establish a new relationship.

Some signs that will alert you to possible identity theft are that you:

- Stop receiving your card(s) or account(s) statement,
- Receive a credit denial for no reason,
- Have inaccurate information on your credit report,
- Receive notice of open accounts, or contracted debts, without asking for them,
- Receive credit cards that you didn't apply for.

Minimize the risks of identity theft:

- Regularly review the charges on your account(s) or credit card(s),
- Notify us of any suspicious activity you detect on your account(s) or credit card(s) to our Customer Service lines:

  Dominican Republic (809) 544-6970
  Panamá (507) 297-4100 Ext.:29935
  Contact us through the following emails: contactenos@popularbank.com.pa
- Claim in a timely manner any charges that you do not acknowledge having made,
- Close your account(s) or credit card(s) if you suspect they have been compromised or exposed.

PRIVACY EVENT/BREACH:
A breach of privacy is a situation in which sensitive information controlled by Popular (or a third party acting on its behalf) is lost, misused, or disclosed to third parties without proper authorization. The information may be in any form, including printed paper or any electronic format or, alternatively, encrypted data. The rupture can occur within the financial institution or in a provider that operates on its behalf.

INTERMEDIARY SERVER:
Computer system whose mission is to act as an intermediary between one system and another through the Internet. Among the missions of an intermediary server are to speed up your access to the Internet, filter the content that has been accessed and protect the systems by avoiding direct communication.

SPAMMER:
Person who is dedicated to sending emails with advertising not requested by users.

SSL:
Or Secure Socket Layer, for its acronym in English, means Secure Connection Layers and refers to a high-level security protocol for communications through the Internet.
SSL provides an encrypted session between the server and the browser and helps ensure that sensitive information (personal or financial data) remains confidential during transmission.

TLS:
Transport Layer Security, or TLS, is an enhanced version of SSL, which works much like SSL, using encryption to protect the transfer of data and information.

TROYAN:
Malicious code camouflaged inside another seemingly useful and harmless program, until the instructions of the person who created the code are executed. These can remain silent and undetectable, until they are activated using operating system functions such as date, time, or the fulfillment of some other type of event on the computer.

SECURITY VULNERABILITIES:
It refers to flaws, defects or programming errors which can be exploited by malicious users without authorization, to access computer networks or servers. As these vulnerabilities become known, programming companies develop patches, improvements (updates) or fixes to correct these vulnerabilities.

VIRUS:
It is the most well-known threat faced by servers, browsers, Internet pages and computers. Viruses are programs that are installed on the computer, usually hidden from the user, for malicious purposes (for example, destroying files or the disk, spreading to other computers, or causing the computer to malfunction). They generally don't act until the containing program is executed or until some condition (a specific date or time) is met.