National Cyber Security Centre

Advent Glossary

This glossary explains some common words and phrases relating to cyber security, originally published via the **@NCSC** Twitter channel throughout December. The NCSC is working to demystify the jargon used within the cyber industry. For an up-to-date list, please visit **www.ncsc.gov.uk/glossary**.

App

Short for Application, typically refers to a software program for a smartphone or tablet.

Attacker

Malicious actor who seeks to exploit computer systems with the intent to change, destroy, steal or disable their information, and then exploit the outcome.

Breach

An incident in which data, computer systems or networks are accessed or affected in a non-authorised way.

Browser

A software application which presents information and services from the web.

Brute force attack

Using computational power to automatically enter myriad value combinations, usually in order to discover passwords and gain access.

Certificate

A form of digital identity for a computer, user or organisation to allow the authentication and secure exchange of information.

Credentials

A user's authentication information used to verify identity - typically one, or more, of password, token, certificate.

Data at rest

Describes data in persistent storage such as hard disks, removable media or backups.

Dictionary attack

A type of brute force attack in which the attacker uses known dictionary words, phrases or common passwords as their guesses.

Download attack

Unintentional installation of malicious software or virus onto a device without the users knowledge or consent. May also be called a drive-by download.

Exploit

May refer to software or data that takes advantage of a vulnerability in a system to cause unintended consequences.

Hacker

In mainstream use as someone with some computer skills who uses them to break into computers, systems and networks.

Honeypot (honeynet)

Decoy system/network to attract attackers. Limits access to actual systems by detecting, deflecting or learning from an attack. Many honeypots = honeynet.

Insider risks

The potential for damage to be done maliciously or inadvertently by a legitimate user with privileged access to systems, networks or data.

Malvertising

Using online advertising as a delivery method for malware.

Malware

Malicious software - includes viruses, trojans, worms or any code or content that could have an adverse impact on organisations or individuals.

Mitigation

Steps that organisations and individuals can take to minimise and address risks.

Network

Two or more computers linked in order to share resources.

Pentest

Short for penetration test. An authorised test of a computer network or system designed to look for security weaknesses so that they can be fixed.

Pharming

An attack on a network infrastructure that results in a user being redirected to an illegitimate website despite the user having entered the correct address.

Platform

The basic hardware (device) and software (operating system) on which applications can be run.

Router

A network device which sends data packets from one network to another based on the destination address. May also be called a gateway.

Sanitisation

Using electronic or physical destruction methods to securely erase or remove data from memory.

Smishing

Phishing via SMS: mass text messages sent to users asking for sensitive information (eg bank details) or encouraging them to visit a fake website.

Virtual Private Network (VPN)

An encrypted network often created to allow secure connections for remote users, for example in an organisation with offices in multiple locations.

Virus

Programs which can self-replicate and are designed to infect legitimate software programs or systems. A form of malware.

Vulnerability

A weakness, or flaw, in software, a system or process. An attacker may seek to exploit a vulnerability to gain unauthorised access to a system.

Incident

A breach of the security rules for a system or service, such as:

- **attempts to gain unauthorised access to a system and/or data**
- **unauthorised use of systems for the processing or storing of data**
- **changes to a systems firmware, software or hardware without the system owners consent**
- **malicious disruption and/or denial of service**

© Crown Copyright 2018