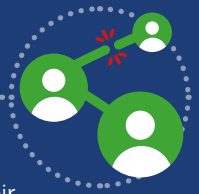
GLOSSARY OF COMMON TECHNICAL TERMS

Advanced Persistent Threat



Often a targeted attack, patiently mapping out weaknesses in the network and going through many stages to overcome security controls. Their aim? To gain unauthorised access to systems and remain undetected for a significant period of time. Cyber criminals will usually observe and monitor user activity and steal information, however they are capable of greater disruption.

Brute Force

Using computing power to guess multiple combinations of passwords against a single account until the attacker gains access. To narrow down the search, the program is instructed to run through the dictionary, common passwords and key words found from social media.

Corporate Account Takeover

Cyber criminals gain access to business finances from obtaining valid user credentials. They can make transactions, transfer funds, pay clients, just as any ordinary user would – costing a business £millions. Furthermore, customer information can become compromised and used to facilitate further attack.

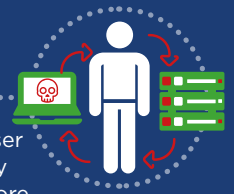
Credential Stuffing

Having acquired a list of usernames and passwords, cyber criminals run automated checks against multiple online accounts until they break in, stealing information and /or money. Hackers rely on password reuse to achieve their objectives.

Domain

policedsc.com, for example, is the domain for PDSC and is used for both website (https://www.policedsc.com/) and email (contact@policedsc.com). The Domain tells the browser what website to display to the user or what mail server to send emails to.

Man-in-the-Browser Attack



Malware utilising vulnerabilities in the browser to capture information, observe user activity and to modify transactions and "forms" before they reach the intended destination. A hack such as this will often bypass security features (e.g. HTTPS and Passwords) and go undetected. Online banking can be particularly vulnerable to this threat.

Password Spraying

Trying a select list of commonly used passwords in conjunction with acquired usernames, forcing their way into many online accounts.

Session Hijacking

Once a legitimate user logs in to their account, the cyber criminal steals the established session ID to impersonate the legitimate user with full access, compromising confidential information and even stealing funds.

Shoulder Surfing

Information captured over one's shoulder. A classic example, strangers viewing the PIN number whilst at the ATM. Catching up with work whilst on public transport always seems productive, however, in doing so the information portrayed onscreen lays bare for all to see and potentially steal. Be alert as to who may be looking at your screen when working on the move or in public spaces.

Spoofing

A term used when something is copied and portrayed as genuine for unsolicited purposes – to gain information or spread malware. Cyber criminals often spoof domains to manipulate users into visiting their website as opposed to the legitimate one; or send emails appearing to be a member of the team.

Vulnerability

When software or an operating system is exposed to cyber threats because of an issue found in its programming and the end user has failed to patch.

Wireless Fidelity (Wi-Fi)

Connecting to the router (which provides access to the internet) without the use of cables.

Zero Day Attack

When a cyber criminal takes advantage of a vulnerability in software that is yet to be fixed by the manufacture.

www.policedsc.com

PDSC
POLICE DIGITAL SECURITY CENTRE