Le nostre sedi:

inlingua Padova
via Niccolò Tommaseo, 67
35131 Padova

inlingua Treviso
via Rosa Zalivani, 2
31100 Treviso

Ci trovi online:

www.inlinguapadova.it

@inlinguapadovatreviso

inlingua Padova Treviso

Contatti:

Federica Bennici

Padova:
segreteria@inlinguapadova.it
049/8076060

Treviso:
segreteria@inlinguatreviso.it
0422/56542

Lun - Ven
09:00 - 13:00
14:30 - 19:00

Sabato
09:00 - 12:00

351/9265360

GLOSSARIO DI CYBER SECURITY

Benvenuti nel mondo di Internet: un universo vasto e affascinante dove l'innovazione non ha confini. Ma attenzione, come in ogni grande avventura, ci sono pericoli nascosti lungo il cammino.
Questa nostra guida vi aiuterà a navigare in sicurezza, armandovi con la conoscenza necessaria per affrontare pericoli reali in questo mondo virtuale.
Preparatevi a diventare esploratori digitali informati e protetti!

Malware
Programmi creati per fare danni ai computer o rubare informazioni, un po' come i virus del mondo reale ma per i computer.

Phishing
Trucchi usati per farvi credere di essere su un sito sicuro o ricevere un'email amica, per rubarvi informazioni private.

Ransomware
Un tipo di malware che "rapisce" i vostri file, criptandoli così che non possiate più accedervi, e poi vi chiede soldi per "liberarli".

Firewall
Un guardiano digitale che controlla chi può entrare o uscire dalla vostra rete internet, bloccando gli intrusi.

Encryption
Traduce le informazioni in un codice segreto, così che solo chi ha la "chiave" giusta può leggerle.

VPN (Virtual Private Network)
Tecnologia che permette di creare una connessione sicura e crittografata su una rete meno sicura, come Internet.

Two-factor Authentication (2FA)
Un extra passo di sicurezza che richiede due prove di chi siete, come una password e un codice inviato al vostro telefono.

Zero-day exploit
Un attacco che sfrutta una falla di sicurezza non ancora conosciuta dai buoni, un po' come un ladro che trova una porta segreta in una casa.

DDoS (Distributed Denial of Service)
Un attacco che manda così tante richieste a un sito web da renderlo inutilizzabile, come una folla che blocca l'ingresso di un negozio.

Vulnerability Assessment
Questo processo cerca i punti deboli nel tuo computer o rete, per poi decidere quali correggere per primo, rendendolo più sicuro.

Botnet
Un esercito di computer infettati usati per attacchi o spam, controllati da un cybercriminale.

Spoofing
Quando qualcuno finge di essere un'altra persona o dispositivo in rete per ingannarvi.

Trojan Horse (Trojan)
Un malware mascherato da software sicuro, come il Cavallo di Troia della mitologia che nascondeva i soldati al suo interno.

Social Engineering
L'arte di manipolare le persone per far svelare informazioni segrete, come un truffatore che convince la vittima a dargli i propri dati.

SIEM (Security Information and Event Management)
Strumenti che aiutano a vedere in tempo reale se ci sono minacce alla sicurezza, un po' come avere una telecamera di sicurezza che vi avvisa se qualcosa non va.

Brute Force Attack
Tentare tutte le combinazioni di password possibili fino a indovinare quella giusta, come provare ogni chiave su una serratura fino a trovare quella che apre.

Spyware
Software spia che raccoglie segretamente informazioni su di voi senza che lo sappiate.

Adware
Programmi che vi mostrano pubblicità invadenti, spesso senza il vostro permesso.

Patch Management
Il processo di aggiornamento e correzione dei programmi per tappare le falle di sicurezza, come mettere una toppa su un buco.

Penetration Testing (Pen Testing)
Testare un sistema per scoprire se ci sono debolezze che potrebbero essere sfruttate dai cybercriminali, un po' come fare la prova del nove della sicurezza.