DICȚIONAR DE TERMENI

TOUCHED România

orange Fundația

Identitatea online reprezintă felul în care o persoană se prezintă și este văzută în mediul digital, incluzând profilele de pe rețelele sociale, adresele de e-mail, numele de utilizator, activitatea online, precum și conținutul vizual sau informațiile financiare partajate. Această identitate poate fi diferită de cea din viața reală, deoarece utilizatorii au posibilitatea de a controla modul în care se prezintă. Totuși, identitatea online joacă un rol crucial în interacțiunile digitale și poate influența modul în care persoana este percepută și ce reputație are.

Securitatea cibernetică se referă la măsurile și practicile pe care oamenii le pot adopta pentru a-și proteja informațiile personale, dispozitivele (computerele si telefoanele) și activitățile online (cumparaturi online, plata facturilor si chiar navigarea pe internet) de amenințările cibernetice. Aceasta include protejarea identității, a datelor personale și a confidențialității în fața potențialelor atacuri, a virusilor, fraudelor sau abuzurilor online.

Cyberbullyingul, sau hărțuirea cibernetică, este o formă de abuz care are loc online, folosind tehnologia digitală, cum ar fi rețelele sociale, aplicațiile de mesagerie, jocurile online sau alte platforme de comunicare. Aceasta presupune trimiterea repetată și intenționată de mesaje menite să intimideze, insulte, amenințe sau să umilească o persoană. Astfel de acțiuni pot include mesaje amenințătoare sau jignitoare, distribuirea de imagini sau videoclipuri compromițătoare fără consimțământul persoanei afectate, răspândirea de zvonuri false pentru a-i compromite reputația sau excluderea acesteia din grupuri sociale.

Phishingul este un tip de atac cibernetic care încearcă să fure informații personale, cum ar fi parole, numere de carduri de credit sau alte date sensibile, prin mesaje înșelătoare. Aceste mesaje, care pot veni sub formă de e-mailuri, SMS-uri sau site-uri web false, par să provină de la surse de încredere, cum ar fi bănci sau companii bine cunoscute, dar în realitate sunt create de atacatori pentru a păcăli oamenii. Victimele sunt adesea îndemnate să acceseze un link sau să deschidă un atașament, ceea ce poate instala un software răuvoitor pe dispozitivul lor sau le poate trimite către un website fals, unde li se cere să își introducă datele personale.

Parola este un șir de caractere (litere, cifre, simboluri) folosit pentru a verifica identitatea unei persoane atunci când aceasta încearcă să acceseze un sistem, un cont sau un serviciu digital. Scopul parolei este de a proteja datele și informațiile de accesul neautorizat, asigurându-se că doar persoanele care cunosc parola corectă pot accesa resursele protejate. O parolă puternică este de obicei complexă, având o combinație de caractere mari și mici, cifre și simboluri, pentru a reduce riscul de a fi ghicită sau spartă de atacatori.

Un **utilizator** este o persoană sau o entitate care interacționează cu un sistem, aplicație, platformă sau serviciu digital. În domeniul informatic, utilizatorul este cel care folosește un computer, un dispozitiv mobil sau orice alt tip de tehnologie pentru a accesa și a utiliza software-ul sau resursele disponibile. De obicei, fiecare utilizator are un cont unic, protejat printr-un nume de utilizator și o parolă, care îi oferă acces personalizat la anumite funcții, date sau servicii, în funcție de drepturile și permisiunile atribuite.

Dispozitivele electronice sunt aparate care funcționează pe baza principiilor electronicii, ce pot include o gamă largă de echipamente, de la telefoane mobile, computere, tablete și televizoare, până la electrocasnice inteligente, ceasuri inteligente și console de jocuri. Dispozitivele electronice sunt esențiale în viața cotidiană, facilitând comunicarea, divertismentul, educația și diverse alte activități prin intermediul tehnologiei.

Software-ul reprezintă un ansamblu de programe și instrucțiuni care permit unui computer sau unui dispozitiv electronic să execute diverse funcții, de la rularea sistemelor de operare până la utilizarea aplicațiilor pentru sarcini specifice, cum ar fi editarea de texte sau navigarea pe internet. Este componenta intangibilă a unui sistem, care coordonează și ghidează funcționarea hardware-ului, facilitând astfel interacțiunea utilizatorilor cu tehnologia.

Hardware-ul reprezintă ansamblul componentelor fizice și tangibile ale unui computer sau dispozitiv electronic, cum ar fi unitatea centrală de procesare (CPU), memoria RAM, hard disk-urile, placa de bază, monitorul, tastatura și alte periferice. Aceste componente lucrează împreună pentru a executa instrucțiunile furnizate de software, permițând astfel funcționarea și interacțiunea cu dispozitivul. În esență, hardware-ul formează "corpul" unui sistem, oferind suportul fizic necesar pentru rularea programelor și aplicațiilor software.

Backup-ul reprezintă procesul de creare a unei copii de rezervă a datelor importante, pentru a le proteja împotriva pierderii sau deteriorării. Această copie poate fi stocată pe un dispozitiv separat, cum ar fi un hard disk extern, un server, un serviciu de stocare în cloud sau alte medii de stocare. Backup-ul este esențial pentru a asigura recuperarea datelor în caz de defecțiuni hardware, atacuri cibernetice, ștergere accidentală sau alte incidente care ar putea duce la pierderea informațiilor. Realizarea regulată a backup-urilor este o practică importantă pentru securitatea și integritatea datelor.

Hackerii sunt persoane care folosesc abilități tehnice pentru a pătrunde ilegal în sisteme și rețele, de obicei cu scopuri răuvoitoare sau personale. Ei se folosesc de vulnerabilități pentru a obține acces neautorizat la date confidențiale, a fura informații sensibile, a compromite securitatea sistemelor sau a provoca daune. Activitățile lor pot include furtul de identitate, răspândirea de de software răuvoitor(malware) sau software care blochează datele (Ransomware) și alte atacuri cibernetice care pot duce la pierderi financiare și distrugerea datelor victimelor. Spre deosebire de hackerii etici, care își folosesc cunoștințele pentru a îmbunătăți securitatea, hackerii rău intenționați acționează cu scopul de a provoca daune și pierderi, punând în pericol integritatea și confidențialitatea informațiilor.

Virușii cibernetici sunt programe malițioase care infectează computere și rețele pentru a le deteriora sau controla fără permisiunea utilizatorului. Ei se răspândesc prin fișiere infectate, e-mailuri sau linkuri, și pot cauza daune precum ștergerea de date, încetinirea performanței computerului sau furtul de informații. Pentru a te proteja de viruși, este important să folosești un software antivirus actualizat și să eviți deschiderea fișierelor sau accesarea linkurilor suspecte.

O rețea Wi-Fi este un sistem care permite dispozitivelor să se conecteze la internet sau între ele prin intermediul semnalelor radio, fără a folosi cabluri. Este folosită pentru a accesa internetul în locuințe, birouri și locuri publice, oferind conectivitate fără fir.

Spam-ul reprezintă mesaje nedorite trimise în masă prin e-mail, SMS sau online, adesea pentru a promova produse sau servicii fără acordul tău. Acestea pot conține oferte false, linkuri periculoase sau chiar încercări de furt de date.

Bluetooth este o tehnologie wireless care permite dispozitivelor, precum telefoane, căști sau laptopuri, să comunice între ele pe distanțe scurte, fără a folosi cabluri. E folosit pentru transfer de fișiere, conectarea căștilor, boxelor sau altor gadgeturi.

Pairing este procesul de conectare între două dispositive, telefoane, de obicei prin Bluetooth, pentru a putea comunica și transfera date între ele. După ce sunt conectate, dispozitivele se pot conecta automat în viitor.

Resurse

https://dnsc.ro/vezi/document/scam-phishing-vishing - Directoratul National de Securitate Cibernetica

https://www.politiaromana.ro/ro/comunicate/politia-romana-directoratul-national-de-securitate-cibernetica-si-asociatia-romana-a-bancilor-avertizeaza-asupra-riscului-de-frauda-de-tip-spoofing

https://www.politiaromana.ro/ro/comunicate/proiectul-national-sigurantaonline-in-anul-2023

https://sigurantaonline.ro/

https://sigurantaonline.ro/7-sfaturi-utile-pentru-a-te-proteja-eficient-in-mediul-online/