Nume și prenume elev:

Clasa:

Data:

Siguranța online

Programele, induse în special prin , care pot face rău utilizatorilor (stricând, distrugând sau obținând acces neautorizat la date) sunt identificate prin termenul general de software rău intenționat sau (Malicious Software). Înțelegem prin acces neautorizat că acesta poate lua, fără voia proprietarului ( ), informații personale (, starea de sănătate, parole, date bancare etc.).

Dintre acestea, amintim:

- : program care se agață de fișiere și le atacă (în special pe cele ale sistemului de operare), se multiplică, se autodiversifică (se mutează) răspândindu-se în întregul sistem de fișiere și blochează sistemul sau îl încetinește progresiv, până la blocare; unele comportamente anormale ale sistemului îi trădează prezența, iar programele antivirus îl pot inactiva de la bun început sau îl pot elimina pe măsură ce îi detectează prezența;
- *(worm):* program de sine stătător care circulă de obicei în rețelele de calculatoare neprotejate prin programe antivirus corespunzătoare, încărcând rețeaua și blocând traficul în rețea;
- : program nelegitim înglobat într-o aplicație de interes, aplicație care are un scop legitim de utilizare; la instalarea aplicației, calul troian se activează și atacă sistemul, întocmai ca și corespondentul său antic folosit în războiul troian, sustrage date, face operații nepermise, de cele mai multe ori fără a-și face simțită prezența;
- *(phishing):*proces de obținere ilegală a unor informații personale prin trimiteri (linkuri) aparent de încredere, în cadrul unei comunicări electronice; Phishing-ul are loc pe e-mail sau pe mesageria instant, redirecționând utilizatorii către un website unde li se cere să-și introducă datele;
- *(ransomware):* software rău intenționat care poate prelua controlul dispozitivului digital, poate cripta informații importante ale utilizatorului (poze, documente etc.) acestea devenind inutilizabile și cerând plata unei sume pentru aducerea dispozitivului la funcționarea normală și la decriptarea datelor; infectarea se face prin deschiderea unor atașamente venite prin email, prin instalarea unei aplicații infectate (tip cal troian) sau prin vizitarea unor site-uri periculoase;
- *(browser hijaker):*program care se atașează browserului de internet (deseori cu acceptul utilizatorului) care schimbă configurația browserului, pentru a redirecționa utilizatorii către site-uri care încearcă în mod ilegal să își sporească popularitatea;
- *(adware)*: programe care afișează pe dispozitiv reclame nesolicitate și neincluse în oferta unui program instalat;

LIVEWORKSHEETS

- *(spam):* atacuri în sfera comunicațiilor prin email, în care se trimit mesaje nesolicitate, de cele mai multe ori cu caracter comercial, mesaje ce invadează căsuța poștală a utilizatorului și îl agresează prin apariții repetate, obsedante;
- *(scam)*: scheme complexe (spam + virus + phishing) de dezinformare, dirijare a activității online și capturare de date personale (CNP, număr card, PIN-uri și altele) prin care inițiatorii obțin bani de la utilizatorii creduli.

Căile de a evita efectele unor atacuri informatice sunt multiple:

- utilizarea pe dispozitiv, a unui , corect instalat și actualizat (căruia i se adaugă, prin actualizări, elemente de securitate suplimentare);
- instalarea, pe bază de abonament, a unui cunoscut prin bunele sale rezultate de combatere a virușilor și altor capcane informatice și actualizarea frecventă a acestuia;
- , atentă, a adreselor de internet vizitate, a linkurilor cărora le dăm curs, a atașamentelor venite pe email sau a trimiterilor promovate prin mesageria instant, tratarea cu a tentațiilor de mari premii oferite prin vizitarea unor site-uri și completarea unor date "de transmitere a premiilor" etc.

Bibliografie: Pedagogie digitală - supor de curs - Rodica Pintea - 2021

LIVEWORKSHEETS