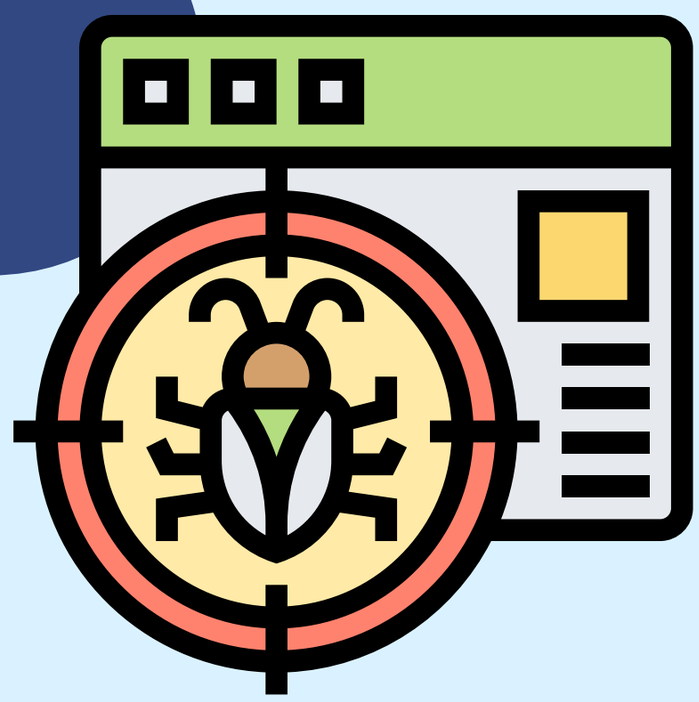
Programele malware

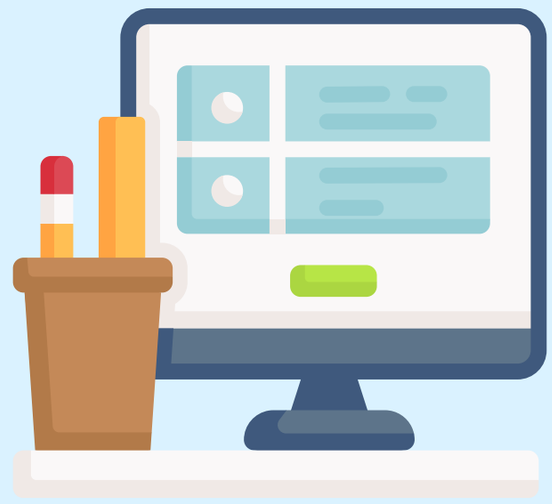


Un **program malware** (software rău intenționat) reprezintă o aplicație sau script conceput cu scopul de a provoca modificarea sau ștergerea datelor informatice, deteriorarea sau restricționarea accesului la calculatoare sau rețele.

Principalele tipuri de programe malware:

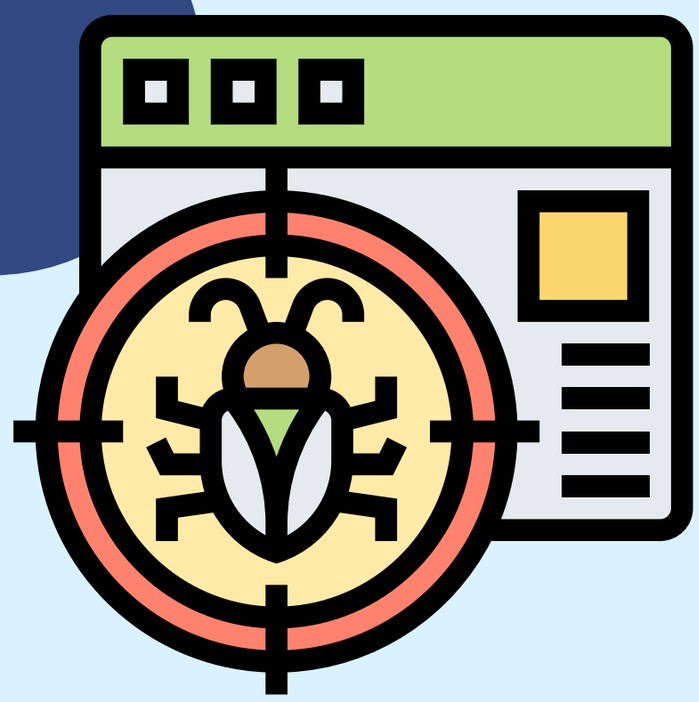
- **Viruși** - se replică modificând alte programe de calculator prin introducerea propriului cod.
- **Troieni** - dau impresia că efectuează operațiuni legitime, pe când încearcă, de fapt, să exploateze vulnerabilitățile sistemului și să permită accesarea sistemului în mod ilegal.
- **Viermi** - aplicații cu efecte distructive care infectează sistemul informatic și se propagă prin Internet.
- **Ransomware** - criptează sau blochează accesul la fișiere și solicită o răscumărare pentru a elimina restricțiile.
- **Criptomineri** - aplicații care utilizează resursele informatice pentru a mina criptomonede pentru infractorii cibernetici.
- **Adware** - programe care transmit în mod agresiv reclame utilizatorilor.
- **Spyware** - captează diverse informații despre activitatea utilizatorilor pe Internet.
- **Rogueware** - programe care induc în eroare utilizatorii pentru a plăti pentru eliminarea unor infecții false detectate în sistemul de operare.

RECOMANDĂRI privind prevnirea infecției cu programe malware:



- **Instalați o soluție antivirus** - pentru a detecta și elimina programele de tip malware în timp real.
- **Instalați o aplicație de tip firewall** - pentru a inspecta traficul de pe paginile web, e-mailuri și aplicații.
- **Actualizați aplicațiile și sistemele de operare -** pentru a remedia eventualele vulnerabilități existente.

Programele malware



- **Dezactivați execuția automată a script-urilor pe site-uri web -** pentru a preveni instalarea de programe malware.
- **Folosiți aplicații de filtrare a e-mail-urilor -** pentru a recunoaște și detecta mesajele și fișierele atașate infectate.
- **Evitați să utilizați conturi de administrator -** pentru a preveni faptul în care programele malware să obțină privilegii de administrator. Utilizarea unor conturi cu drepturi limitate în locul unui cont de administrator va bloca accesul la zonele sensibile ale sistemului de operare și va bloca implicit atacurile ce vizează serviciile sistemului de operare, fișierele sau bibliotecile sale.
- **Faceți copii de siguranță a datelor -** pentru a le restabili în cazul unei infecții cu malware. Aceste copii trebuie stocate pe suporturi magneto-opticede încredere și depozitate în locuri sigure și eventual criptate pentru a evita accesul neautorizat.
- **Folosiți instrumente avansate -** pentru a detecta programele malware, cum ar fi sistemele de detectare și prevenire a intruziunilor (IDPS).
- **Monitorizați jurnalele (Logs) -** utilizând soluții de gestionare a incidentelor și evenimentelor de securitate (SIEM).
- **Utilizați politici de securitate -** care specifică pașii care trebuie urmați în cazul unei infectări.
- **Reduceți accesul la funcțiile powershell -** pentru a limita posibilitatea de execuție a codului rău intenționat în consolă.
- **Nu dați click pe link-uri și nu descărcați fișiere atașate în e-mail-uri sau mesaje** - dacă nu sunteți siguri de sursa acestora.
- **Restricționați conținutul pe web** - utilizați instrumente precum ad-blockers pentru a limita posibilitatea de a executa coduri rău intenționate în timp ce vizitați anumite site-uri web.
- **Raportați incidentele de securitate -** Centrului guvernamental de răspuns la incidente cibernetice, incidents@cert.gov.md, https://stisc.gov.md.