Zemītes sākumskolas

DROŠAS INTERNETA LIETOŠANAS PAMATNOTEIKUMI

- Nedod citām personām savu personas apliecību (eID karti) ar PIN kodiem vai internetbanku piekļuves līdzekļus.
- Neievieto tīmeklī dokumentu kopijas (pase, eID karte, vadītāja apliecība u.c.) un nesūti tās pa e-pastu, saziņas lietotnēs vai sociālajos tīklos.
- Nepārsūti paroles un citu privātu informāciju e-pasta vēstulēs vai saziņas lietotņu (WhatsApp, Viber, Messenger u. c.) un sociālo tīklu (Facebook, Twitter u. c.) ziņojumos.
- E-pasta vēstule, kas nosūtīta no attiecīgā datora, nepazūd, tās kopijas var tikt saglabātas vairākās vietās.
- Saņemot e-pasta vēstules ar aizdomīgu saturu, nedrīkst atvērt tai pievienotos pielikumus.
- Neizpaud savus personas datus, nepārliecinoties par pieprasījuma īstumu.
- Nestāsti tīmeklī un sociālajos tīklos pārāk daudz par savu dzīvi, jo īpaši par finansiālo situāciju, jauniegūtajām lietām, izbraukšanu no mājām u.tml.
- Pārdomā, kādas fotogrāfijas publicēt tīmeklī un kā to publiskošana kādu dienu var ietekmēt tavu dzīvi, piemēram, attiecības ar draugiem, radiniekiem, kolēģiem, esošajiem vai nākamajiem darba devējiem.
- Datorā, kurš ir pieslēgts internetam, noteikti jābūt instalētai antivīrusu programmai

PRINCIPI, KAS JĀIEVĒRO, RŪPĒJOTIES PAR MOBILĀS IERĪCES DROŠĪBU

- Uzinstalē programmatūras un operētājsistēmas atjauninājumus vienmēr, kad ierīce vai programmatūras ražotājs to piedāvā.
- Tā kā mobilās ierīces satur svarīgus datus (adrešu grāmatiņu, fotogrāfijas, video, dokumentus un citus datus), ir jāizturas atbildīgi pret ierīci un nedrīkst atstāt to bez uzraudzības. Ja ierīce tiek pazaudēta vai nozagta, nekavējoties jābloķē SIM karte un pati ierīce (IMEI kods) – to var veikt, sazinoties ar savu mobilo sakaru sniedzēju.
- Aizsargā savu mobilo ierīci ar drošības kodu, piemēram, izmantojot pirkstu nospiedumu, norādot skaitļu kombināciju (PIN) vai speciālu zīmējumu, kas jāievada, lai atbloķētu ekrānu.
- Ja izmanto valsts vai pašvaldības iestādes mobilo lietotni, kurā nepieciešama autentificēšanās, pēc lietotnes izmantošanas jāatceras iziet no tās, izvēloties atbilstošo komandu, piemēram, “„Iziet”, “Beigt darbu”, “Atslēgties”.

KUR VĒRSTIES PĒC PALĪDZĪBAS DROŠĪBAS JAUTĀJUMOS?

- Ja tev ir aizdomas, ka dators ir inficēts, vai rodas citas ar IT drošību saistītas problēmas, pēc padoma un palīdzības gadījumā vari vērsties Informācijas tehnoloģiju drošības incidentu novēršanas institūcijā cert.lv.
- Ja redzi, ka tiek izplatīta pretlikumīga informācija, piemēram, aicinājums uz vardarbību, naida kurināšana, finanšu krāpniecība u. tml., vai vēlies saņemt atbildes uz dažādiem ar drošību internetā saistītiem jautājumiem, sazinies ar skolotāju.
- Ja esi kļuvis par krāpniecības upuri, vērsies Valsts policijā.