Izlūkdienesti kibertelpā

Ieteikumi drošības risku mazināšanai

IZLŪKOŠANA KIBERTELPĀ

Ārvalstu izlūkdienesti arvien intensīvāk izmanto kibertelpu izlūkošanas informācijas iegūšanai.

Arī Tu vari būt mērķis, jo Tavs darbs un Tev pieejamā informācija ir interesanta izlūkdienestiem. Nenovērtē sevi par zemu!

Mērķtiecīgi izstrādāti un īpaši pieskaņoti kiberuzbrukumi var tikt vērsti gan pret Tavas iestādes, gan Tavām personīgajām mobilajām iekārtām un datoriem. Mērķis – piekļūt informācijai, kas tiek apstrādāta datoros, e-pastu sarakstē, tālruņos un planšetēs. Kad piekļuve šīm ierīcēm ir iegūta, tā tiek uzturēta ilgstoši un nemanāmi.

Lai atlasītu potenciāli interesējošās personas un detalizēti tās analizētu, ārvalstu izlūkdienesti izmanto sociālos tīklus. Tur savāktā informācija tiek izmantota, lai izstrādātu tālākas darbības – kontaktētos ar Tevi klātienē vai uzsāktu saziņu internetā.

MOBILĀS IEKĀRTAS

Mobilās iekārtas – tālruņi, planšetes, portatīvie datori, viedpulksteņi u.c. viedierīces – var Tevi izsekot, noklausīties un filmēt, tās ir atslēgas uz Tavu dzīvi. Neņem līdzi mobilās iekārtas, kad risini sensitīvus, privātus vai profesionālus jautājumus.

Pilnībā drošu mobilo iekārtu nav. Jebkura ražotāja iekārtās un lietotnēs ir drošības nepilnības, ko spēj izmantot ārvalstu izlūkdienesti. Izvērtē, kādas lietotnes Tev tiešām ir nepieciešamas un kādām iekārtas funkcijām tās prasa piekļuvi. Piemēram, ja telefona lukturīša aplikācija prasa piekļuvi kontaktu sarakstam, neizmanto to.

Saglabā piesardzību un neizpaud sensitīvu informāciju, lietojot WhatsApp, Viber, Signal, Telegram u.c. saziņas aplikācijas, jo neviena no tām nav pilnībā droša.

Izslēdz bezvadu savienojumu (mobilo datu, Wi-Fi, bluetooth u.tml.) un atrašanās vietas noteikšanas funkcijas (GPS), kad Tev tās nav nepieciešamas.

Neizmanto Wi-Fi publiskās vietās – viesnīcās, lidostās, kafejnīcās u.c. Ārvalstu izlūkdienesti var izmantot šo platformu, lai iegūtu kontroli pār Tavu mobilo iekārtu, kas tiks saglabāta arī pēc tam, kad konkrēto Wi-Fi vairs nelietosi.

Regulāri veic mobilo iekārtu un lietotņu atjaunināšanu. Mobilajās iekārtās aktivizē funkciju ierīces satura šifrēšanai.

Izvērtē situāciju, vai atstāt savas mobilās iekārtas bez pieskatīšanas. Esi īpaši piesardzīgs, apmeklējot valstis, kas nav NATO un ES dalībnieces.

SOCIĀLIE TĪKLI

Nebūtisku sīkumu nav! Iedziļinies visos drošības un privātuma iestatījumos, pārdomā, cik plašam personu lokam ļauj sekot līdzi Tavām aktivitātēm sociālajos tīklos.

Izvērtē, kādu informāciju iekļaut sadaļā "Par mani". Ziņas par dzīvesvietu, darbavietu, ģimenes stāvokli, absolvētajām mācību iestādēm u.tml. var izmantot ārvalstu izlūkdienesti, lai veiktu personas padziļinātu izpēti.

Domā par privātumu un reputāciju pirms publicē, komentē, izsaki patiku, apstiprini draudzību.

Pilnīgi privātu aktivitāšu sociālajos tīklos nav. Rēķinies, ka profils var tikt "uzlauzts" un informācija publicēta.

Ārvalstu izlūkdienesti sociālajos tīklos veido viltus profilus un var uzdoties par Tev zināmiem cilvēkiem, lai iekļūtu Tavu draugu lokā.

Publicējot bildes un video, to uzņemšanas vietu norādi tikai tad, ja tas tiešām nepieciešams.

Seko līdzi, ko par Tevi, Tavu ģimeni un darbavietu var uzzināt, pētot radinieku, draugu un kolēģu sociālo tīklu aktivitātes.

DATORA UN INTERNETA LIETOŠANA, INFORMĀCIJAS APSTRĀDE

Klasificētu informāciju apstrādā tikai tam paredzētās informācijas sistēmās.

Rūpīgi izsver sensitīvas informācijas apstrādi internetam pieslēgtās iekārtās un tās pārrunāšanu pa tālruni.

Nelieto privātās iekārtas darba vajadzībām, ja tas nav saskaņots ar Tavas iestādes IT drošības speciālistu. Piemēram, konsultējies, vai drīksti lietot privāto viedtālruni, lai piekļūtu darba e-pastam, vai izmantot privāto datoru profesionālām vajadzībām.

Katrai iekārtai, informācijas sistēmai, e-pastam, sociālajiem tīkliem un internetbankai lieto atšķirīgu paroli, regulāri tās maini un veido pietiekami sarežģītas.

Nelieto svešus datu nesējus (zibatmiņu, datu diskus) pirms Tavas iestādes IT speciālists nav tos pārbaudījis. Pārbaude jāveic arī Taviem datu nesējiem, ja tie tikuši ievietoti svešās iekārtās.

Vienkārši izdzēšot datus no mobilās iekārtas, datora vai datu nesēja, tos ir iespējams atjaunot. Ja gribi būt drošs, ka dati tiek dzēsti neatgriezeniski, konsultējies ar IT drošības speciālistu.

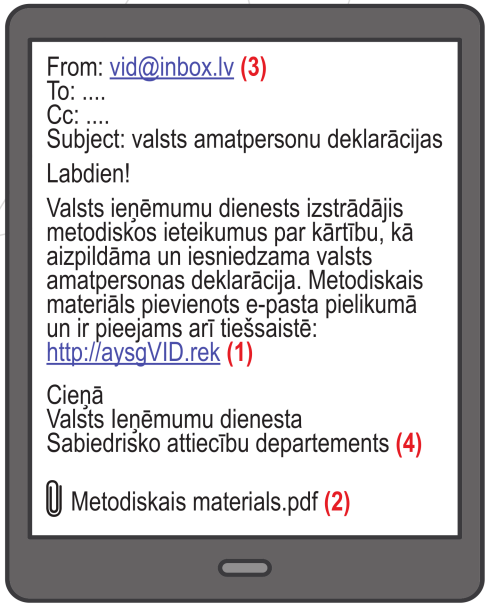
Never vaļā interneta saites, uz kurām norādīta atsauce interneta komentāros. Ārvalstu izlūkdienesti šajās saitēs var iestrādāt vīrusus datora inficēšanai.

E-PASTS

Viltus e-pasta nosūtīšana ir izplatītākais kiberuzbrukumu veids. Vīruss tiek paslēpts e-pastā iestrādātās saitēs **(1)** vai pievienotajos dokumentos **(2)** un bildēs – never tās vaļā, ja šaubies par vēstules īstumu.

E-pasts var tikt maskēts kā Tev pazīstamas personas sūtījums, tas var atsaukties uz pasākumu, ko esi apmeklējis, vēstule var izskatīties kā oficiāls paziņojums no pakalpojumu sniedzēja vai sadarbības partnera.

Pārliecinies, vai Tu pazīsti autoru, kas sūta e-pastu. Vai autors saziņai vienmēr izmanto precīzi šo adresi? **(3)** Vai vēstule ieturēta ierastajā stilā? Piezvani vēstules autoram **(4)**, lai tas apstiprina vēstules īstumu, vai arī konsultējies ar savas iestādes IT speciālistu.



Jebkuru neskaidrību un šaubu gadījumā konsultējies ar savas iestādes IT drošības speciālistu!

Satversmes aizsardzības birojs:
www.sab.gov.lv
tālrunis: (+371) 67025404
e-pasts: info@sab.gov.lv