Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS PRIE KRAŠTO APSAUGOS MINISTERIJOS

INFORMACINIS BIULETENIS ELEKTRONINIAI LEIDINIAI

2019 m. rugsėjo 9 d.

Prasidėjus naujiems mokslo metams Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos primena išlikti budriems siunčiantis elektroninius vadovėlius ir knygas. Elektroninės knygos, kaip ir bet kuris kitas elektroninis dokumentas ar laiškas, gali būti su žalingu programiniu kodu, kuris gali užkrėsti kompiuterį ir įgalinti atlikti įvairius kenkėjiškus veiksmus – užšifruoti kompiuterio duomenis, prašyti išpirkos, šantažuoti, rinkti duomenis apie vartotoją, jo prisijungimus prie paskyrų, slaptažodžius. Tokių veiksmų pasekmės gali būti ne tik finansinė žala ar prarasta intelektinė nuosavybė, bet ir prarasti asmeniniai duomenys, nuotraukos ir pan.

Patikimi šaltiniai. Knygas, vadovėlius ir kitus elektroninius leidinius siųskitės tik iš patikimų, visuotinai žinomų šaltinių. Turėkite omenyje, kad ne visi iš pirmo žvilgsnio patikimai atrodantys šaltiniai (pvz. mokyklos interneto svetainė, mokytojo ar bendraklasio siųstas laiškas) yra iš tiesų patikimi, todėl dažniausiai vertėtų imtis papildomų saugumo priemonių, kurias aprašėme žemiau.

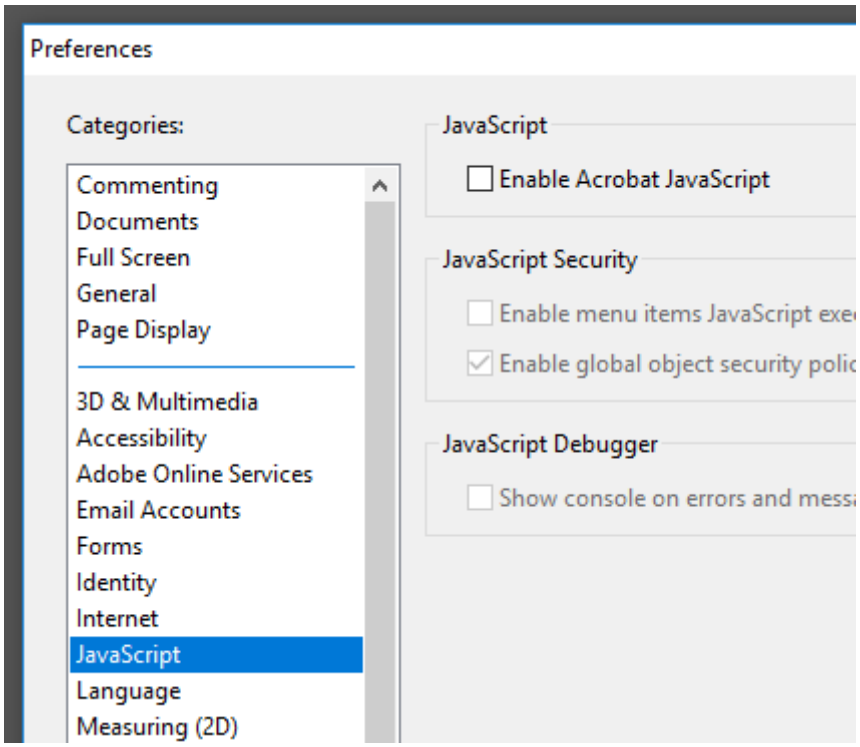
Nežinomi šaltiniai. Jeigu svetainė, iš kurios nusprendėte atsisiųsti elektroninį leidinį, Jums nėra žinoma ar kelia įtarimų, paieškokite apie ją papildomos informacijos – pasinaudokite paieškos sistemomis (pvz. Google) ir paskaitykite rastus atsiliepimus.

Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

Papildomai paieškokite pagal užklausą „virus svetainesadresas.com“ ir pan. Atkreipkite dėmesį, ar sujungimas su svetaine apsaugotas (adresas prasideda https), atkreipkite dėmesį, kokias kitas svetaines reklamuoja, stebėkite, ar nėra nepageidaujamų langų (angl. pop-up).

Mokami leidiniai prieinami nemokamai. Venkite mokamų knygų, kurios svetainėse pateikiamos atsisiuntimui neatlygintinai. Viskas turi savo kainą - taip dažniausiai viliojami naivūs lankytojai, siekiant užvaldyti jų kompiuterinius resursus ar duomenis. Ypatingai didelės nuolaidos ar neįprasti pasiūlymai – dar vienas pavojaus ženklas, todėl visą informaciją vertinkite kritiškai.

Išjunkite JavaScript. „Adobe Reader“ ir kitos PDF tipo bylų skaitymo taikomosios programos turi savyje integruotą JavaScript funkcionalumo palaikymą, kurio pagalba galima išnaudoti įvairius sistemų pažeidžiamumus arba apgauti vartotoją atlikti žalingus sistemai veiksmus, todėl šią funkciją galima tiesiog išjungti. „Adobe Reader“ programoje tai padaryti galima keliaujant į **Edit** > **Prefences** > **JavaScript** ir nuimant paukštelį nuo „Enable Acrobat JavaScript“ (Pav. 1).



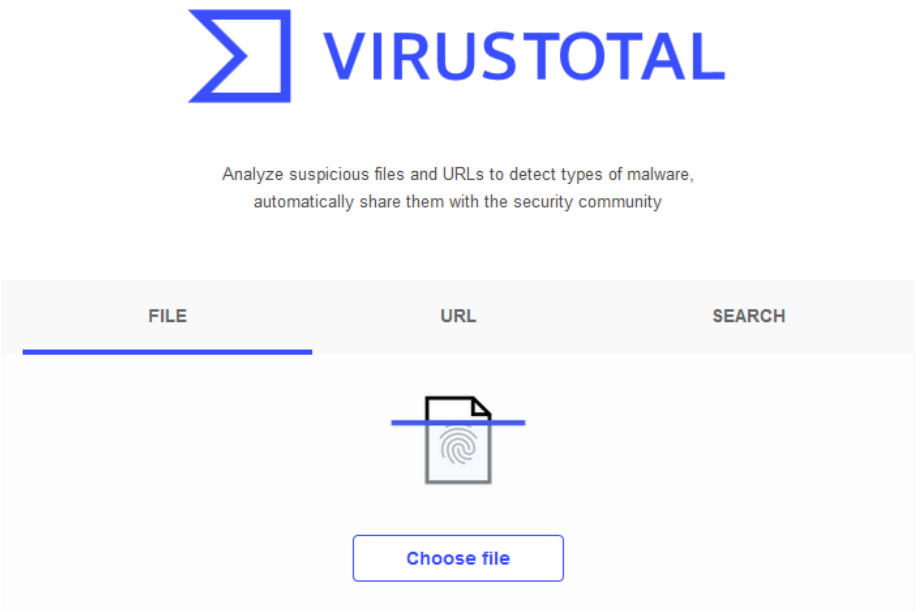
Pav. 1. JavaScript funkcionalumo išjungimas „Adobe Reader“ programoje

Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

Atnaujinimai. Reguliariai atnaujinkite savo prietaisų operacines sistemas ir taikomąsias programas, skirtas skaityti elektroninius leidinius (pvz. „Adobe Reader“). Tik naujausios programų versijos padės išvengti daugumos žinomų pažeidžiamumų ir geriau apsisaugoti nuo kibernetinių grėsmių.

Antivirusinė. Antivirusinė programa – tai dar vienas žingsnis jūsų saugumo užtikrinimui. Nepamirškite, kad ši programa taip pat turi būti nuolat atnaujinama, kad atpažintų naujausias kenkimo kodų versijas, o tam geriausiai tinka automatinio atnaujinimo nustatymas.

„VirusTotal“. Tai interneto svetainė, kuri leidžia labai paprastai ir greitai pasitikrinti įtartinas bylas. „VirusTotal“ naudojasi net kelių dešimčių antivirusinių programų kenkimo kodų duomenų bazėmis, todėl gali būti itin efektyvi, jeigu naudojate ne tokią pažangią arba rečiau atsinaujinančią antivirusinę sistemą.



Pav. 2. www.virustotal.com

Kopijos kopijos kopijos. Susikurti atsargines duomenų kopijas – tai dažniausias patarimas, tinkantis bet kokiais kibernetinių grėsmių atvejais. Laikykite šias kopijas atskiruose įrenginiuose – pavyzdžiui išoriniame diske ar debesinėje duomenų saugykloje. Duomenų kopijos neapsaugos nuo virusų, bet duomenų praradimo atveju (kuomet duomenys užšifruojami ar sunaikinami), juos galima bus atstatyti ar atgauti.

Pagrindinis dalykas – nuolatos būti atidiems ir kritiškai vertinti informaciją.