**2023 11 13**

**Ar teisingai siunčiate failus internetu? Kelios klaidos gali perduoti jautrią informaciją sukčiams tiesiai į rankas**

**Didelės apimties nuotraukos, vaizdo įrašai, nuomos sutartys, dokumentų kopijos, bankų išrašai – tai tik keli failų pavyzdžiai, kuriuos, tikėtina, esate bent kartą siuntę ar gavę per failų dalijimosi platformą. Akivaizdu, kad šių failų nenorėtumėte į rankas atiduoti kibernetiniams sukčiams, bet, pasak Manto Užupio, „Tele2“ IT saugumo eksperto, apsisaugoti pavyksta ne visiems. Nesaugiomis failų dalijimosi svetainėmis ar programomis pasitikintys žmonės rizikuoja prarasti jautrius duomenis, bet būdų apsisaugoti yra.**

**Kodėl svarbu apsaugoti failus?**

„Patogus dalijimasis failais internete tapo neatsiejama kasdienio gyvenimo dalimi. Tiek darbiniams projektams, tiek tarpusavio dalijimuisi svarbiais dokumentais, ar nuotraukų siuntimui – efektyvaus ir saugaus dalijimosi failais poreikis yra ypač svarbus. Tačiau kartu su tokių failų dalijimosi platformų patogumu ateina ir tam tikros rizikos, todėl kibernetinių grėsmių amžiuje tapo itin svarbu užtikrinti savo skaitmeninio turto saugumą“, – sako Mantas Užupis, „Tele2” IT saugumo ekspertas.

Pasak jo, užtikrinti saugų failų dalijimąsi internete svarbu dėl kelių priežasčių. Pirmiausia, tokiu būdu apsaugoma jautri informacija. „Daugelyje failų, kuriais dalijamės internete, yra jautrios ir asmeninės informacijos – nuo finansinių įrašų iki konfidencialių darbo dokumentų. Šių failų saugumas yra labai svarbus, kad būtų išvengta neteisėtos prieigos ir galimo piktnaudžiavimo duomenimis“, – teigia M. Užupis.

Be to, apsaugoti siunčiamus failus būtina ir norint išsaugoti privatumą. Dalijimasis failais internete susijęs su duomenų patikėjimu trečiųjų šalių platformoms, kurios kontroliuoja, kas turi prieigą prie failų, todėl reikėtų naudotis tik patikimais kanalais.

„Failų, įvairių dokumentų saugumas ypač svarbus ir verslui, kuris neretai remiasi į bendradarbiavimą, tad žmonės nuolat keičiasi įvairiais duomenimis. Tad saugumas yra svarbus norint išsaugoti konfidencialias komercines paslaptis ar intelektinę nuosavybę“, – sako ekspertas.

**Dažnai sutinkamos grėsmės**

Egzistuoja keli būdai, kaip naudojantis nesaugiomis failų dalijimosi platformomis programišiai gali pavogti jautrius naudotojų duomenis ar užkrėsti įrenginius. Dažnai pasitaikanti priemonė – kenkėjiška programinė įranga (angl. „malware“) ir virusai, kai užkrėstose svetainėse galima parsisiųsti paslėptų kenkėjiškų programų arba virusų, kurie gali užkrėsti įrenginius ir pakenkti saugumui.

Pasitaiko ir vadinamosios *fišingo* (angl. „phishing“) atakos. Pavyzdžiui, naudojant apgaulingas dalijimosi failais nuorodas arba el. laiškus gali būti bandoma apgaule išgauti konfidencialią informaciją, pavyzdžiui, įvairių paskyrų naudotojo vardus ir slaptažodžius.

**Taisyklės, kurias reikėtų žinoti**

Vis dėlto, naudotis skaitmeninio bendradarbiavimo privalumais galima ir nepažeidžiant savo ar organizacijos privatumo bei duomenų vientisumo. M. Užupis dalijasi keliais saugiais dalijimosi failais internete būdais ir taisyklėmis.

**Debesų saugyklos paslaugos**. Aukštam saugumui užtikrinti galima naudoti patikrintas debesų saugyklų paslaugas. Tokiu būdu jūsų failus pasiekti galės tik tie žmonės, su kuriais dalijatės debesijos prieiga. Tarp tokių platformų – „Google Drive“, „Dropbox“ ir „Microsoft OneDrive“.

**Slaptažodžių apsauga**. Prieš dalydamiesi failais, apsaugokite juos stipriais slaptažodžiais. Tai suteikia papildomą apsaugos lygį, todėl prie bendrinamo turinio galės prieiti tik teisingą slaptažodį turintys asmenys.

**VPN**. Dar vienas būdas apsaugoti failus – naudotis VPN (virtualus privatus tinklas) paslauga. Ši paslauga sukuria saugų ir šifruotą ryšį, ypač naudingą naudojantis viešaisiais „Wi-Fi“ tinklais.

**Failų šifravimo įrankiai**. Apsvarstykite galimybę naudoti failų šifravimo įrankius, kurie užšifruoja failus prieš juos bendrinant. Taip užtikrinama, kad net ir įvykus neteisėtai prieigai, be iššifravimo rakto turinio nebus galima perskaityti.

**Papildoma įrenginių apsauga**. Pasirūpinkite papildoma įrenginių apsauga, užkertančia kelią programišių pastangoms. Pavyzdžiui, „Tele2“ tinklo lygmeniu įdiegta interneto apsauga automatiškai aptinka kenkėjiškus puslapius ir akimirksniu užblokuoja prieigą prie jų. Apie bandymus įsilaužti klientai yra informuojami SMS žinute ar el. laiškais. Šią paslaugą užsisakyti galima operatoriaus savitarnos svetainėje.

**Daugiau informacijos:**

*Asta Buitkutė*

„Tele2“ atstovė ryšiams su visuomene

**M** +370 668 00467

**@** asta.buitkute@tele2.com