EUROPOS KIBERNETINIO SAUGUMO MĖNUO

KVIEČIAME DALYVAUTI PROJEKTO VEIKLOSE

SU.ESET.LT

Gerbiami mokytojai ir švietimo specialistai,

ESET Lietuva kviečia minėti Europos kibernetinio saugumo mėnesį ir dalyvauti žinių patikrinimo viktorinoje, kuri vyks interneto svetainėje su.eset.lt

Kviečiame jūsų moksleivius dalyvauti viktorinoje, patikrinti savo žinias ir laimėti puikius prizus!

RENGINIO PARTNERIAI:

EUROPOS KIBERNETINIO SAUGUMO MĖNUO

draugiškas internetas

LANGAS Į ATEITĮ

Tapkite saugesni su ESET ir organizuokite jūsų moksleivių dalyvavimą viktorinoje

Savarankiškai arba drauge su visa klase bei mokytoju priešakyje spręskite **su.eset.lt** svetainėje pateiktas **Kahoot** viktorinas. Rinkite taškus ir nepamirškite pasidalinti savo gautais rezultatais. Viktorinoje galėsite dalyvauti iki kibernetinio saugumo mėnesio pabaigos, o laimėtojus skelbsime jau spalio 29 dieną!

Žaiskite ir laimėkite ESET prizus

SU.ESET.LT

VIKTORINOS TAISYKLĖS

Prisijunkite prie Kahoot žaidimo aplinkos

Prisijunkite prie su.eset.lt puslapyje esančio Kahoot žaidimo lango. Pasirinkite savo norimą slapyvardį ir jį suveskite pradedant žaidimą. Žaidimo metu pasistenkite teisingai atsakyti į kuo daugiau viktorinos klausimų. Taškai skaičiuojami automatiškai, vadovaujantis teisingų atsakymų kiekiu bei sparta. Laimėtojams svarbu nepamiršti išsaugoti savo rezultatus. Tai atlikti galima nufotografuojant įrenginio, kuriame žaidėte Kahoot viktoriną, ekrano langą, kuriame yra matoma žaidėjo užimta pirma, antra arba trečia prizinės vietos.

Kibernetinio saugumo mėnesio metu dalyvaukite dvejose viktorinose

Visi norintys galės dalyvauti dvejose su.eset.lt pateiktose viktorinose. Pirmoji viktorina tema „Sukčiavimas internete“ vyks nuo spalio 11 iki 15 dienos. Antroji viktorina tema „Saugūs slaptažodžiai“ vyks nuo spalio 25 iki 29 dienos. Norint tinkamai pasiruošti viktorinoms, ESET specialistai rekomenduoja peržiūrėti su.eset.lt esančią kibernetinio saugumo naujienų skiltį bei edukacinius vaizdo įrašus, kuriuose rasite daug naudingos informacijos!

Laimėtojus skelbsime Europos kibernetinio saugumo mėnesio pabaigoje.

Pasibaigus kibernetinio saugumo mėnesiui, spalio 29 d. 15 val. su.eset.lt internetinėje svetainėje skelbsime abiejų viktorinų nugalėtojus. Svetainėje skelbsime nugalėtojų slapyvardžius, pateikiant Kahoot laimėtų viktorinų pirmą, antrą ir trečią vietas. Laimėtojams nurodytais kontaktais reikės pateikti išsaugotas ekrano kopijas, kuriose matoma jų laimėta prizinė vieta bei slapyvardis.

ENJOY SAFER TECHNOLOGY™

ESET KIBERNETINIO SAUGUMO PATARIMAI

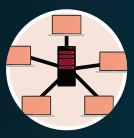
MOKYTOJAMS IR MOKINIAMS

Grėsmių apžvalga

Lietuvoje pastaruoju metu plinta kenkėjiškos programos, nukreiptos į vartotojų asmeninius įrenginius. Plačiau apie kibernetines grėsmes:

Banking Trojans
Kenkėjiška kompiuterinė programa, skirta neteisėtai prieigai prie internetinės bankininkystės operacijų.

Adware
Kompiuteryje rodo nepageidaujamas reklamas, kuriose yra įrašyta kenkėjiškų programų kodų.



Remote connection exploits
Tinklų ir kompiuterių puolimas pasitelkiant kenkėjiškas programas per nuotolinį ryšį.

OS exploits
Išnaudoja programinės įrangos pažeidžiamumus, kad programišiams būtų suteikta prieiga per nuotolinį prisijungimą.

Slaptažodžių politika

Tipiškas interneto vartotojas turi dešimtis internetinių paskyrų. Kiekviena iš šių paskyrų turėtų būti apsaugota tvirtu, unikaliu ir privačiu slaptažodžiu. Patikrinti nutekėjusį slaptažodį galite: https://haveibeenpwned.com

Stiprus slaptažodis turėtų būti:

- Unikalus kiekvienoje naudojamoje paskyroje.
- Žinomas tik paskyros naudotojui.
- Sudarytas iš ne mažiau nei 8 simbolių.
- Sunkiai atspėjamas, nesusijęs su tokia asmenine informacija kaip vardai, šeimos nariai, gyvūnų vardai arba gimimo diena.

Nuotolinis darbas

Asmeninių įrenginių IT saugumo užtikrinimas dabar yra ypač aktualus. ESET kibernetinio saugumo ekspertas Ramūnas Liubertas vaizdo įraše atskleidžia įmonėms būdingas saugumo rizikas bei pandemijos metu atsiradusias kibernetines grėsmes bei sukčiavimo būdus, nukreiptus į vartotojus. Žiūrėkite vaizdo įrašą (QR kodas).

Jungimasis prie organizacijos tinklo

Daugelis organizacijų savo darbuotojams suteikė galimybę dirbti nuotoliniu būdu. ESET specialistai parengė veiksmų seką, padėsiančią tinkamai pasirengti nuotolinio darbo aplinką saugiam Jūsų darbui. Žiūrėkite vaizdo įrašą (QR kodas).

ESET ENJOY SAFER TECHNOLOGY™

ESET KIBERNETINIO SAUGUMO PATARIMAI

MOKYTOJAMS IR MOKINIAMS

Prevencinės priemonės

Jeigu naudojate antivirusinę programą, patikrinkite ar programoje yra įgalintos šios funkcijos:

- E. bankininkystės ir mokėjimų apsauga
- Apsauga nuo sukčiavimo Anti-Phishing
- Privatumo apsauga
- Apsauga nuo brukalo Antispam
- Tinklo apsauga nuo atakų

Plačiau žiūrėkite vaizdo įraše (QR kodas).

Interneto apsauga

Galimybė jungtis prie interneto yra standartinė asmeninių kompiuterių funkcija. Deja, internetas tapo pagrindine kenkėjiško kodo platinimo terpe. Dėl to itin svarbu atidžiai įvertinti savo prieigos prie saityno apsaugos parametrus.

- E. pašto programos apsauga kontroliuoja e. pašto ryšius, priimamus naudojant POP3(S) ir IMAP(S) protokolus.
- Apsauga nuo brukalo filtruoja nepageidaujamus e. laiškus.
- Apsauga nuo sukčiavimo apsimetant leidžia blokuoti žinomas svetaines, kurios platina apgaulingą turinį.

Daiktų internetas

Vis dažniau naudojame išmaniuosius įrenginius - tai kelia grėsmę kibernetiniam saugumui. Išmanieji įrenginiai kasdien perduoda didelius asmeninės informacijos kiekius. Didėjant besidalijamų duomenų kiekiui atsiranda daugiau būdų patekti į privačius tinklus. Jei jūsų naudojamam prietaisui yra būtina prieiga prie interneto, apsvarstykite galimybę sumažinti duomenų, kuriuos perduodate išmaniųjų produktų kūrėjams, kiekį. Be to, naudokite unikalius slaptažodžius arba slaptažodžių frazes. Jei įmanoma, įjunkite dviejų veiksnių autentifikavimą ir nuolat atnaujinkite savo prietaisus bei jų operacines sistemas, naudokite patikimą antivirusinę programą, kad išvengtumėte pažeidžiamumų.

E. pašto apsauga

„Phishing“ – vis dar viena labiausiai paplitusių kibernetinio sukčiavimo formų. Šis terminas, kilęs nuo angliško žodžio „fishing“ (liet. žvejyba), apibūdina melagingų elektroninių laiškų siuntimą siekiant apgauti gavėją. Paprastai tokiuose laiškuose būna pridėtas virusais užkrėstas failas arba į tekstą įterpta nuoroda, vedanti į netikrus tinklalapius. Bet kokiu atveju, „phishing“ atakas privalu mokėti atpažinti, ir laiku į jas sureaguoti.

Dar vienas aptiktas apgaulės būdas - „Spam“ (angl. spam) tipo arba „brukalo laiškai“.
Daugumoje patikimų pašto dėžučių veikia specialūs filtrai, atpažįstantys piktybinius elektroninius laiškus. Dažniausiai tokie laiškai iš karto siunčiami tiesiai į „šlamšto“, „brukalų“ ar tiesiog „spam“ aplanką. Daugelis virusų plinta per nuorodas ar kenkėjiškus failus, kuriuos gauname kaip elektroninio pašto brukalus. Niekuomet nerekomenduojama atidarinėti iš nepažįstamų siuntėjų gautų dokumentų ar spausti ant įtartinų nuorodų. Taip pat atsargiai vertinti ir kitus laiškus iš nežinomų siuntėjų, nuasmenintus laiškus iš įvairių institucijų – įvairūs bankai ir kitos organizacijos, norėdamos pranešti svarbią informaciją, paprastai kreipiasi asmeniškai ir pagrindinius duomenis apie asmenį žino iš anksto.

ESET ENJOY SAFER TECHNOLOGY™