Įspėjimas dėl kibernetinių ir informacinių atakų, susijusių su COVID-19

NKSC įspėja, kad piktavaliai elektroninėje erdvėje intensyviai išnaudoja susidariusią ekstremalią situaciją dėl COVID-19 viruso plitimo. Prisidengiant įvairiomis institucijomis ir melaginga informacija, siuntinėjami laiškai su žalingu programiniu kodu, platinamos suklastotos svetainės, socialinės inžinerijos metodais bandoma vartotoją paskatinti įsidiegti kenkėjišką programinę įrangą ir kitais būdais užvaldyti įrenginius bei išgauti konfidencialią informaciją.

Viena iš paskutinių pasauliniu mastu plintančių su COVID-19 susijusių apgavysčių formų yra „Pasaulio sveikatos organizacijos“ imitavimas, siunčiant melagingą informaciją elektroniniu paštu su kenkėjiškomis nuorodomis, patalpintomis laiškuose ar jų prieduose. NKSC atkreipia dėmesį, kad Lietuvos atveju gali būti siekiama suklastoti Lietuvos Respublikos Vyriausybės, Sveikatos apsaugos ministerijos, Nacionalinio visuomenės sveikatos centro, savivaldybių publikuojamą informaciją, kuriami fiktyvūs naujienų tinklalapiai.

NKSC rekomenduoja kritiškai vertinti elektroniniu formatu (elektroniniame pašte, socialiniuose tinkluose, SMS žinutėse) gaunamas nuorodas, susijusias su COVID-19 tematika. Žalingos nuorodos, vedančios į netikrus puslapius ar į naudotojo kompiuterį atsiunčiančios žalingo kodo programinę įrangą, dažnai būna siunčiamos kartu su žinute. Naudojami socialinės inžinerijos metodai: dominuoja skubos, svarbos, krizės ar nelaimės motyvai. Tokie laiškai taip pat dažnai būna siunčiami apsimetant kompetentingomis institucijomis. NKSC atkreipia dėmesį – būtina įvertinti tokių gaunamų laiškų autentiškumą ir turinį, atkreipiant dėmesį į pateiktas nuorodas ir prisegamus priedus.

Įsitikinti siunčiamos nuorodos autentiškumu galite užvedus pelyte ant adreso (nespaudžiant) - nuorodoje neturėtų būti publikuotas kitos svetainės adresas. Atkreipiame dėmesį, kad netikra nuoroda gali būti labai panaši į egzistuojančio ir gerai žinomo tinklapio adresą. Svarbu atkreipti dėmesį ar siunčiama nuoroda turi patikimą SSL/TLS sertifikatą, šifruojantį perduodamus duomenis. Dažniausiai populiariausios naršyklės įspėja jeigu nėra naudojamas sertifikatas ar jis nėra patikimas, tačiau paprasčiausias būdas įsitikinti – prie http trumpinio turi būti raidė „**s**“, pvz.: **https://www.nksc.lt**.

Venkite atskleisti asmeninę informaciją. Niekada elektroniniu paštu, socialiniuose tinkluose, SMS žinutėmis ar skambučiais neatskleiskite savo asmeninės ar finansinės informacijos. Valstybinės institucijos, bankai, sveikatos priežiūros įstaigos, niekada nesikreips su prašymu elektroniniu paštu ar telefonu atskleisti asmeninę informaciją (pvz., asmens kodas, kreditinės ar debetinės kortelės numeris, banko autentifikavimo kodas ir pan.). Gavus panašius prašymus tikslingiausią tokią informaciją perduoti policijai. Kaip atpažinti klastotas nuorodas skaitykite NKSC biuletenyje:

https://www.nksc.lt/doc/biuleteniai/2018-05-15%20phishing%20klastotes%20ir%20duomenu%20vagystes.pdf

Kadangi piktavaliai esamą situaciją naudoja ir melagingai informacijai skleisti, NKSC rekomenduoja remtis tik oficialia Lietuvos valstybės ir patikimų žiniasklaidos priemonių teikiama informacija. Socialiniuose tinkluose platinamos žinutės, prieš jomis pasidalinant, taip pat turėtų būti tikrinamos.

Primename, kad pagrindinis dalykas – nuolatos būti atidiems ir kritiškai vertinti gaunamą informaciją.

Originalus straipsnis

https://www.nksc.lt/naujienos/ispejimas_del_kibernetiniu_ir_informaciniu_ataku_s.html