ZINOŠS JELGAVNIEKS = PASARGĀTS JELGAVNIEKS

civilā aizsardzība/kiberdrošība/datu aizsardzība

Latvijā ikdienu tiek veiktas krāpnieciskas aktivitātes ar mērķi – iegūt bankas kontu, e-pastu un sociālo tīklu piekļuves datus, kā arī izplatīt vīrusus kibertelpā. Lai nekļūtu par virtuālo krāpnieku upuri, ikvienam datoru un mobilo iekārtu lietotājam svarīgi ievērot piesardzību! Jelgavas Digitālais centrs apkopojis izplatītākos krāpšanas veidus un ieteikumus, kā samazināt krāpnieku uzbrukumu riskus.

VIRTUĀLĀS KRĀPŠANAS VEIDI

1.Balss klonēšana - krāpnieki izmanto mākslīgo intelektu, lai precīzi atdarinātu cilvēku balsis. Pazīstama cilvēka balsī (ģimenes locekļa, vadītāja utt.), tiek lūgts veikt steidzamu maksājumu. Šādu zvanu saturam raksturīgs satraukums un prasība rīkoties nekavējoties.

Kā rīkoties?

Vienojies ar ģimenes locekļiem par konkrētu atslēgas vārdu, ko zināt tikai jūs. Aiciniet zvanītāju nosaukt šo vārdu. Ja zvana it kā darba devējs vai sadarbības partneris, pirms veikt naudas pārskaitījumu, pats sazvani konkrēto cilvēku, ieteicams no cita tālruņa numura, un pārliecinies par sarunas satura atbilstību.

2.Pikšķerēšanas kampaņas - tiek izsūtīti krāpnieciski e-pasti un SMS, uzdodoties par banku vai pakalpojuma sniedzēju. Šādu e-pastu mērķis - attālināti izvilināt no cilvēkiem personas datus, internetbanku un e-pastu paroles un lietotāja vārdus, lai izmantotu tos kibernoziegumos. Nereti e-pastam pievienotās saites ved uz it kā bankas vai pakalpojuma sniedzēja tīmekļvietni, kas ir viltota, bet ļoti līdzīga oriģinālam.

Kā rīkoties?

Neklikšķini uz aizdomīgām saitēm e-pastā vai SMS. Ja nepieciešams pārliecināties par e-pastā saņemtā satura atbilstību, atver attiecīgās bankas vai pakalpojumu sniedzēja tīmekļvietni jaunā pārlūka logā vai sazinies ar klientu konsultantu pa tālruni.

3.Viltotas CSDD soda kvītis - tiek sūtīti e-pasti un SMS par it kā piemērotu administratīvo sodu ceļu satiksmē. Šiem e-pastiem un īsziņām ir pievienotas krāpnieciskas saites, ko atverot, tiek prasīts autentificēties ar bankas datiem.

Kā rīkoties?

Atceries - CSDD nesūtīs iedzīvotājiem SMS. E-pasta vēstules parasti satur saites uz e-CSDD platformu, kur it kā ir iespējams iepazīties ar pieņemto lēmumu un veikt naudas soda apmaksu. Oriģinālā saite uz e-CSDD platformu ir ar nosaukumu – e.csdd.lv, taču krāpnieciskā vēstulē norādītās saites ved uz viltus adresēm, piemēram, e.csdd.gov.lv-sdj-753-cfdgs.pw.

4.Tuvojoties Saeimas vēlēšanām, ir sagaidāms, ka krāpnieki var izmantot vēlēšanu tematiku savās shēmās, piemēram, aicinot iedzīvotājus atjaunināt vai pārbaudīt informāciju par deklarēto dzīvesvietu vai balsošanas iecirkni, pieslēdzoties viltotām tīmekļvietnēm. Savukārt vēlēšanu laikā var tikt izsūtītas ziņas par to, ka vēlētāja balss ir anulēta, un nepieciešams pieslēgties kādai tīmekļvietnei, lai to atjaunotu.

Kā rīkoties?

Ja nepieciešams pārliecināties par vēlēšanu iecirkni, pieslēdzies Valsts pārvaldes pakalpojumu portālam Latvija.lv. Never vaļā saites, kas pievienotas e-pastā vai SMS, ļoti iespējams, ka tās ved uz krāpnieku izveidotām tīmekļvietnēm. Atceries - balsošana internetā nav iespējama.

ATCERIES! Ja ir aizdomas, ka esi kontaktā ar virtuālajiem krāpniekiem, paziņo CERT.LV:
-par krāpnieciskiem e-pastiem vai viltus reklāmām sociālajos tīklos raksti: cert@cert.lv;
-krāpnieciskās īsziņas pārsūti uz numuru +371 23230444 (konkrētais tālruņa numurs paredzēts tikai īsziņu pārsūtīšanai nevis sarunām. Izmaksas būs atbilstošas izmantotā operatora tarifiem).
!!!Aktivizē DNS ugunsmūri savā datorā un viedtālrunī: https://dnsmuris.lv/, meklē informāciju cert.lv.

Virtuālie krāpnieki izmanto cilvēku neuzmanību un neziņu, tāpēc, ja šaubies vai saņemtā informācija un piedāvājums ir drošs - atsakies!