ZINOŠS JELGAVNIEKS = PASARGĀTS JELGAVNIEKS

civilā aizsardzība/kiberdrošība/datu aizsardzība

Virtuālo krāpnieku nodarītais kaitējums uzņēmumu un iedzīvotāju finansēm turpina pieaugt. Nezināšanas vai neuzmanības dēļ cilvēki atklāj krāpniekiem savus sensitīvos datus, bankas piekļuves un e-pastu paroles, atļaujot tās izmantot noziedzīgos nodarījumos. Lai pasargātu sevi no iekļūšanas krāpnieciskās shēmās, svarīgi veicināt izpratni par izplatītākajām krāpniecības formām un regulāri atjaunot zināšanas par kiberdrošību. Šoreiz Jelgavas Digitālais centrs apkopojis faktus par vienu no biežāk lietotajiem virtuālās krāpšanas veidiem – pikšķerēšanu, kas sastopama ikviena tālruņa un interneta lietotāja ikdienā.

KAS KOPĪGS MAKŠĶERĒŠANAI UN PIKŠĶERĒŠANAI?

ĀĶIS = VILINOŠS PIEDĀVĀJUMS

Pikšķerēšana mērķis - attālināti izvilināt no cilvēkiem personas datus, internetbanku un e-pastu paroles un lietotāja vārdus, lai izmantotu tos kibernoziegumos.

Visbiežāk izmantotās pikšķerēšanas metodes:

- e-pasta vēstules;
- paziņojumi par viltus loterijām, akcijām un laimestiem;
- tālruņa sarunas un balss ziņas.

Krāpnieku uzbrukuma rezultātā cilvēki:

- zaudē sensitīvus datus, ko krāpnieki var izmantot nelegālos darījumos;
- zaudē finanšu līdzekļus;
- zaudē virtuālo identitāti un drošību;
- var saskarties ar kaitējumu reputācijai.

PIKŠĶERĒŠANAS PAZĪMES

Ko krāpnieki aicina izdarīt pikšķerēšanas e-pastos?

- Atklāt sensitīvu informāciju - paroles, personas datus u.tml.
- Noklikšķināt uz krāpnieciskas interneta saites.
- Atvērt inficētu e-pasta pielikumu, kas satur vīrusu.

Pikšķerēšanas e-pastos krāpnieki visbiežāk informē par:

- problēmām ar e-pastu, internetveikala kontu u.tml.;
- tehniskā atbalsta problēmām;
- romantisku attiecību piedāvājumu, tēlojot attiecības, kas pārtop naudas izspiešanā;
- nepieciešamību sniegt papildu informāciju, lai pabeigtu kādu iesāktu darījumu.

Ko krāpnieki piedāvā upuriem viltus loterijās?

Milzīgas naudas summas, nesamērīgi lielas balvas, piemēram, automašīnas, digitālās ierīces vai citas dārgas preces.

Loteriju pikšķerēšanā krāpnieki visbiežāk:

- jautā personisku un finanšu informāciju;
- pieprasa iemaksāt naudu, lai saņemtu balvu vai palielinātu iespēju laimēt;
- izmanto viltību, lai saņemtu naudu - lūdz iemaksāt valūtas maiņas starpību vai naudas pārskaitījuma nodevu u.tml.;
- aicina kādu laiku paturēt noslēpumā informāciju par laimestu, lai upura līdzcilvēki nepagūtu noreaģēt uz krāpšanas mēģinājumu.

Kā krāpnieki veic tālruņa un balss ziņu pikšķerēšanu?

- Izmanto rūpīgi izstrādātus scenārijus un metodes, lai iegūtu upuru uzticību.
- Krāpnieki pirms zvanīšanas upurim veic izpēti par viņu, lai ar lielāku pārliecību apvārdotu cilvēku.
- Krāpnieki var izlikties par policijas, bankas, kāda pakalpojumu sniedzēja pārstāvi, lai iebiedētu upuri ar finanšu mahinācijām viņa kontā, tā iegūstot informāciju par upura bankas kontu.
- Iedveš steidzamības un baiļu sajūta, izmanto naivumu un nezināšanu.

Kāpēc tālruņa un balss ziņu pikšķerēšanas uzbrukumi bieži ir sekmīgi?

- Viltus zvanus ir grūti atšķirt no īstiem - sarunas ir rūpīgi izplānotas.
- Uzbrucējs pārstāv iestādes, kam cilvēki uzticas - Valsts policija, bankas u.tml.
- Izmanto cilvēku bailes vai personīgās intereses, lai iegūtu sensitīvu informāciju.

NESTEIDZIES, JA SAŅEM AICINĀJUMU RĪKOTIES AR SENSITĪVIEM DATIEM. MIERĪGI APDOMĀ, KAS, KO UN KĀPĒC TEV JAUTĀ. JA TEV VAI TAVIEM LĪDZCILVĒKIEM IR AIZDOMAS, KA KONTAKTĒJIES AR VIRTUĀLO KRĀPNIEKU, ZIŅO 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).

Meklē informāciju www.cert.lv.

Aktivizē CERT.LV izveidoto DNS ugunsmūri savā datorā un viedtālrunī: https://dnsmuris.lv/

SARGĀ TO, KAS PIEDER TEV – NEUZĶERIES UZ KRĀPNIEKU IZMESTĀ ĀĶA!