RIIGI INFOSÜSTEEMI AMET

06. juuni 2023

Õngitsussõnumid ohustavad Eesti inimesi

Olukord

RIA intsidentide käsitlemise osakonna (CERT-EE) eksperdid on tuvastanud viimastel nädalatel iga päev suurusjärgus kümmekond uut õngitsuslehte, mille kaudu petavad kelmid inimestelt pangakaardi andmeid ja PIN-koode välja. RIA-le teadaolevalt on inimesed jäänud ilma kokku tuhandetest eurodest, ühel puhul kaotati korraga üle 2300 euro. RIA küberturbe eksperdid on ilmsiks tulnud õngitsuslehed sulgenud, kuid küberruumi pidev seire näitab, et selliseid lehti luuakse aina juurde.

Kuidas õngitsusi levitatakse?

Kuigi endiselt saadetakse inimestele palju õngitsuskirju, pärinevad käesolevad näited SMS-i teel saadetud õngitsussõnumitest. Üks levinumaid skeeme on kullerfirma teavitus valele aadressile saabunud paki kohta. Vahel väidetakse ka, et paki saajal tuleb saadetise kättesaamiseks tasuda tollimaks ning selleks suunatakse kasutaja õngitsuslehele oma pangakaardiandmeid sisestama. Sarnaseid SMS-ide kaudu saadetavaid õngitsusi levib ka teiste, sh tuntud teenusepakkujate, näiteks pankade ja telekommunikatsioonifirmade nimelt.

Tegu on tõenäoliselt õngitsussõnumiga, kui:

1. Sõnumil on kehv õigekiri ja/või ebaloogiline lausete ülesehitus.
2. Sõnum on saadetud kahtlaselt ja/või välismaa numbrilt.
3. Tavapäraselt teenusepakkuja sõnumi teel kliendi poole ei pöördu.
4. Sõnum sisaldab kahtlast veebilinki, mis sisaldab tihti mingil kujul viidet jäljendatavale organisatsioonile/ettevõttele, kelle klientidelt üritatakse andmeid/raha välja petta (Näide 2).
5. Sõnumi tekst viitab tihti probleemi kiireloomulisusele (Näide 1).

Miks kasutatakse SMSe õngitsemiseks nii ulatuslikult?

SMSide saatmine õngitsemise eesmärgil ei ole tegelikult uudne lähenemisviis. Põhjuseid, miks seda lahendust kasutatakse, on mitu:

1. Sõnumite massiline saatmine on suhteliselt odav.
2. Sõnumi saatjat – nii telefoninumbrit kui ka nime – on selleks loodud tööriistade abil suhteliselt lihtne võltsida, mistõttu ilmuvad õngitsussõnumid ka legitiimse organisatsiooniga peetud vestluse lõime (Näide 1) ja jätavad seeläbi tõesema mulje.
3. Paljud ettevõtted ja finantsasutused kasutavad klientidega suhtlemiseks SMS-e.

Näiteid õngitsussõnumitest

- **Õngitsussõnum ilmub legitiimse sõnumiga samasse lõime**

Alumisel pildil on numbriga 1 tähistatud koht, kus on kas mingi organisatsiooni või inimese nimi või telefoninumber. Konkreetse näite puhul oli seal legitiimse

kommertspanga nimi. Numbriga 2 on tähistatud veebilinki sisaldav õngitsussõnum, mis üritab saajas hirmu tekitada ja suunata teda õngitsuslehele. Numbriga 3 on tähistatud inimese kodupanga legitiimne sõnum, mis ilmus samasse lõime ja hoiatas õngitsussõnumite eest.

Näide 1. Inimesele saabunud õngitsussõnum ülal koos legitiimse sõnumiga all

- **Paki kättesaamiseks on vaja tasuda tollimaks**

All kujutatud pildil on näha õngitsussõnum, mis teatab, et inimesele on saadetud pakk, kuid selle kättesaamiseks on vaja tasuda tollimaks. Millised märgid viitavad selle näite puhul õngitsemisele? Esiteks on sõnum saadetud kahtlaselt välismaiselt telefoninumbrilt, mida kohalikul turul tegutsev ettevõtte ei kasutaks, teiseks sisaldab sõnum kahtlast veebilinki ning kolmandaks on sõnum kirjutatud halvas eesti keeles.

Näide 2. Õngitsussõnum saabunud paki kohta

Kuidas ründajad sinu telefoninumbrit teavad?

Inimestel võib tekkida küsimus, kuidas küberkurjategijad nende telefoninumbreid teavad. RIA toob välja kolm üldist põhjust. Esiteks võivad telefoninumbrid olla kättesaadavad avalikel veebilehtedel (nt ettevõtte koduleht vms). Selliseid avalikult kuvatud numbreid on väga lihtne automaattööriistadega internetist kokku korjata. Teiseks võivad kontaktid pärineda varasematest andmeleketest. Neid andmekogusid müüakse huvitatud osapooltele, kes siis andmeid pahatahtlikel eesmärkidel ära kasutavad. Kolmandaks kasutatakse tööriistu, mis genereerivad huupi numbreid. Tihti on telefoninumbrite ülesehitus mingi kindla loogikaga, mis lihtsustab numbrite huupi tuletamist. Kuna SMS-ide saatmine on suhteliselt odav, saadavadki küberkurjategijad neid massiliselt, lootes, et mõned ikka sihtmärkideni jõuavad.

RIA soovitused

- Ära ava tundmatuid linke ega manuseid.
- Ära jaga mingil juhul enda paroole, PIN-koode ega sisesta enda pangakaardiandmeid kahtlastele veebilehtedele.
- Kahtluse korral helista teenusepakkujale ja küsi üle, kas tegemist on nende saadetud sõnumiga.
- Kasuta CERT-EE rakendust, mis kaitseb nutiseadmeid pahatahtlike veebilinkide ja pahavara eest. Täpsemalt saad selle kohta lugeda siit.
- Tee kahtlasest sõnumist kuvatõmmis ja saada see CERT-EE meiliaadressile cert@cert.ee. Pärast seda võid sõnumi kustutada.
- Loe lisaks RIA blogist, kuidas pahaloomulisi e-kirju ära tunda.

Kui soovid olla kursis Eesti küberruumis toimuvaga, jälgi RIA kuukokkuvõtteid, kvartaliülevaateid ja blogi.