Ettevaatust - sinu lemmiklooma nutividin võib andmeid lekitada!

6 aastat tagasi Autor: AM

Kaspersky Lab'i uuring näitas, et iga viies (21%) lemmikloomaomanik kasutab mingit nutividinat oma looma eest hoolitsemiseks ja tema jälgimiseks. Need võivad olla veebikaamerad, automaatsöötjad ja -jooturid, elektroonilised mänguasjad või videomängud nutitelefonides ja tahvelarvutites, akvaariumite temperatuuriandurid ja palju muud. Sealjuures tunnistas pool vastajatest, et neil olid nende seadmete tõttu teatud probleemid. 35% vastajatest põhjustas nutividinate kasutamine teatud riske loomade või omanike enda jaoks.

Enamiku juhtumite (34%) puhul seadis elektroonilise seadme vale funktsioneerimine ohtu lemmiklooma tervise. Praktiliselt igal neljandal (23%) juhul oli riski all looma elu, igal viiendal (18%) – tema emotsionaalne seisund. Peale selle lausus kolmandik (31%) vastajaid, et juhtumid nutividinatega põhjustasid stressi neile endile või teistele lähedastele.

Uuringu käigus selgus, et 37% seadmetest, mis on mõeldud lemmikloomade jaoks, omavad ligipääsu internetile ning see teeb nad haavatavateks erinevate küberrünnakute jaoks. Antud hetkel rääkis selliste nutividinate häkkimisest 12% küsitluses osalejatest.

„Tehnoloogiad teevad elu lihtsamaks ja mugavamaks mitte üksnes meie, vaid ka nende jaoks, kelle me kodustasime. Kaasaegsed nutividinad võimaldavad kaitsta lemmikloomi, hoolitseda nende eest, luua neile mugav keskkond. Ent tähtis on mitte unustada, et iga elektrooniline seade peale mugavuse toob endaga kaasa ka teatud riskid: seade võib minna korrast ära või selle saavad häkkida kurjategijad. Sestap enne, kui osta ja hakata kasutama uut seadet lemmiklooma jaoks, tasub mõelda digitaalsest turvalisusest," märkis Denis Makrushin, Kaspersky Lab'i viirusetõrje ekspert.

Viis reeglit koduloomade nutividinate turvamiseks

Tõeliselt mugava ja turvalise digitaalse keskkonna loomiseks lemmikloomadele ja nende omanikele soovitavad Kaspesky Lab'i eksperdid järgida lihtsaid reegleid:

1. enne nutividinate ostmist pöörake tähelepanu nende kaitse tasemele – internetist võib leida informatsiooni avatud ja parandatud turvaaukudest turult saadavates populaarsetes seadmetes;
2. enne seadme kasutamise algust vahetage tootja paigaldatud salasõna kindlama vastu;
3. keelake ligipääsud seadmele lokaalsest võrgust väljaspool (kui teil pole sellist vajadust);
4. lülitage välja kõik võrguteenused nutividinas, mida Te ei kasuta;
5. uuendage regulaarselt seadme tarkvara (ja laadige uuendusi alla üksnes ametlikest allikatest).

- Uudised
- Turvalisus