

Nuo vagystės iš vieno garsiausių pasaulio muziejų Paryžiuje iki vis dar veikiančio telefoninio sukčiavimo – sukčių išradingumui ribų nėra. Europoje jie atranda dar vieną nišą – elektromobilių įkrovimo stoteles. Ekspertai perspėja, į ką atkreipti dėmesį ir kaip į apgavikų rankas neperduoti savo turto.

Mūsų įprastos kasdienybės įpročiai slepia pavojus. Elektromobilio vairuotojas atvyksta prie įkrovimo stotelės, nuskenuoja QR kodą, sumoka ir ramiai laukia, kol automobilis bus įkrautas. Viskas paprasta ir įprasta. Tačiau būtent tuo paprastumu ir naudojasi sukčiai.

Vis daugiau Europos šalių kalba apie plintantį sukčiavimo būdą – klastojamus QR kodus, plačiai naudojamus viešojo įkrovimo tinkluose, kaip vienas iš atsiskaitymo būdų. Ant oficialaus operatoriaus lipduko, vedančio į apmokėjimo puslapį, sukčiai užklįjuoja beveik identišką ar bent jau panašų savo. Nukreipę vairuotoją į netikrą svetainę, jie išvilioja kortelės duomenis, o kai kuriais atvejais pinigai iš karto nukeliauja į sukčių sąskaitas.

„Enefit“ viešojo įkrovimo tinklo plėtros vadovas Tomas Žilionis sako, kad neteisėtai praturtėti siekiančių asmenų išradingumas – ne naujiena ir Lietuvoje. Tikėtina, jog šis sukčiavimo būdas netrukus taps aktualus ir čia, mat dalis operatorių vis dar taiko atsiskaitymą nuskenavus QR kodą.

„Dar visai neseniai kovojome su pasipelnyti karpant elektromobilių įkrovimo laidus nusprendusiais asmenimis. Situacija privertė ieškoti papildomų saugumo priemonių. Dabar Europoje plintantį sukčiavimo būdą įgyvendinti itin paprasta, o žmonės dar nėra įpratę įtariai vertinti QR kodų. Nors kol kas tokių atvejų Lietuvoje nefiksuojame, bet, žinant, kaip greitai sklinda idėjos internete, tai tik laiko klausimas, kada lipdukai su netikrais kodais atsiras ir pas mus“, – sako jis.

Anot jo, nors „Enefit“ tinkle QR kodai, kaip atsiskaitymo būdas, nenaudojami. Net ir netaikant šio atsiskaitymo metodo, sukčiai vis tiek gali testuoti žmonių akylumą, tad kiekvienas QR kodas ant stotelių turėtų kelti įtarimų.

Kaip neapsigauti ir ką daryti, jei patekote į spąstus

Iš pirmo žvilgsnio apgaule pastebėti sunku. Sukčiai stengiasi, kad jų QR kodai atrodytų nepriekaištingai – ta pati spalva, tas pats šriftas, netgi tie patys žodžiai. Vis dėlto tiesa slypi detalėse. Jei kodas atrodo įtartinais, yra užklįjuotas ant kito lipduko ar jo dizainas kiek skiriasi – geriau neskenuokite. Net jei pats QR kodas abejonių nesukėlė, jas gali sukelti puslapis, į kurį būsite nukreipti.

Sukčiavimo metodus analizuojantys specialistai pataria pirmiausia atkreipti dėmesį į svetainės adresą. Oficialūs puslapiai visada turi aiškų, pažįstamą domeną, tvarkingai pateiktą informaciją ir kontaktinius duomenis. Jei adresas trumpintas, svetainė atrodo neįprastai ar joje yra rašybos klaidų – verčiau sustoti ir papildomų veiksmų neatlikti. Tokiu atveju visada galima kreiptis į klientų aptarnavimo centrą ir pasitikslinti.

1. Žilionis rekomenduoja rinktis alternatyvius atsiskaitymo būdus, kurie yra patikimesni ir saugesni.

„Nors atsiskaitymas QR kodu patogus ir paprastas, „Enefit“ tinkle jis nėra naudojamas. Nuolat ieško alternatyvų, kad patirtis įkraunant elektromobilį viešosiose stotelėse būtų kuo sklandesnė, o atsiskaitymo būdai – kuo saugesni, patogesni. Mūsų tinkle klientams siūlome atsiskaityti įvairiais būdais: programėle, RFID kortele, atidėto mokėjimo būdu ar banko kortele, tiesiog prilietus ją prie skaitytuvo“, – pataria T. Žilionis.

Jei vis dėlto patekote į sukčių pinkles ir supratote, kad įvedėte duomenis ne ten, kur reikia – nedelskite. Susisieki su banku, užblokuokite kortelę ir praneškite apie apgaulingą mokėjimą. Apie įvykį praneškite ir policijai bei elektromobilių įkrovimo stotelės operatoriui.

„Stotelių ir mūsų klientų apsaugai skiriame didelį dėmesį. „Enefit“ stotelės visą parą stebimos vaizdo kameromis. Gavę klientų pranešimus apie įtartinus atvejus, juos tikriname nedelsdami, kad išvengtume bet kokių galimų nuostolių“, – sako bendrovės viešojo įkrovimo tinklo plėtros vadovas.

