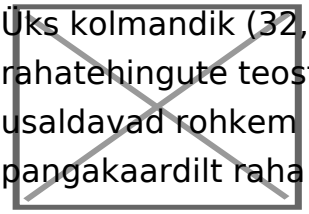
Kaspersky Lab räägib, kuidas muugitakse pangaautomaate ja kuidas pangakaarte kaitsta

11 aastat tagasi - 22.12.2014 Autor: AM



Üks kolmandik (32,7%) Eesti kasutajaid usub, et veebimaksed on turvaline rahatehingute teostamise viis. 24,9% on aga vastupidisel seisukohal: nemad usaldavad rohkem sularaha kasutamist. Samal ajal leiutavad petturid üha uusi pangakaardilt raha varastamise meetodeid.

Kaspersky Labi eksperdid on nende kõige levinumate pangaautomaadi ja maksekaartide lahtimuukimise viisidega kursis.

Eksperdid annavad siin nüüd nõu, kuidas jõuluoste tehes mitte langeda kurjategijate ohvriks.

Varaste seas on üks kõige levinum moodus kiiresti sularahaga rikkaks saada seifi lahtimuukimine või siis kogu pangaautomaadi varastamine. Palju kurvem on pangakliendi jaoks lugu siis, kui tegemist on näiteks nn skimminguga. Sellisel juhul paigaldab kurjategija kaardisisestusavale seadme, mis kopeerib magnetriba andmed ja salvestab PIN-koodi. Seejärel kirjutatakse andmed võltskaardile ja varas suundub pangaautomaadi juurde kontole jäänud raha välja võtma.

Eelmisel aastal paistis üks Brasiilia pettur silma sellega, et paigaldas võltspangaautomaadi pärismasina peale. Pettus tuli ilmsiks siis, kui üks klient soovis kasutada automaati oma konto saldo vaatamiseks. Pangaautomaat väljastas veateate, kliendil tekkis aga kahtlus ja ta kutsus politsei.

Tänapäeval toodetavatele uutele pangaautomaatidele on juba paigaldatud skimminguvastased katikud ja teised kaitsesüsteemid. Kuid tuleks siiski meeles pidada, et esiteks leiavad petturid kergeks rikastumiseks kiiresti uusi lünkasid ning teiseks on pangaautomaat kallis seade, mida pank kasutab paljude aastate jooksul. Seega leidub automaate, mis on toodetud ammustel aegadel, millal skimminguvastaseid meetmeid veel ei kasutatud. Seepärast kontrollige kindlasti, kas klaviatuur, mida näidatakse pangaautomaadi ekraanil, vastab sellele, mida seadme küljes näete. Kahtlase seadme korral helistage kohe panka.

Samuti tuleb meeles pidada, et alati ei pea pettur varguse toimepanemiseks jahile minema. Tihtipeale toimub vargus distantsilt. Selleks kasutatakse

mitmesuguseid meetmeid.

Üks neist on mõnda tuntud portaali imiteeriv koduleht ehk ühepäevaleht. Selline lahendus kogub petturitele andmeid. Ohu vältimiseks kontrollige kodulehe aadressi (ega mõni täht ei ole teises kohas või mõni sümbol välja vahetatud) ning suhtuge tähelepanuga viirusetõrje ja veebilehitseja hoiatustesse.

Teine õngitsemise liik on see, mille puhul pettur palub Teil kas telefoni või e-posti teel mingil ettekäändel teatada kaardi andmed. Tuleb meeles pidada, et isegi pangatöötaja ei küsi kunagi Teie käest PIN-koodi ega CVV/CVV2-koodi. Neid ei pea keegi peale Teie teadma.

Pahavara ja kuritegelike rakendustega võidakse varastada Teie kaardiandmeid ka siis, kui sisestate need veebipoes ostu eest tasudes. Jälgige viirusetõrje soovitusi ja ära unustage värskendamast nii oma viirusetõrjet kui ka selle baase. Samuti võib Teie kaardiandmeid varastada kohviku, hotelli, poe, panga jms töötaja, kui ta viib teenuse eest tasumiseks või muu toimingu sooritamiseks kaardi Teie vaateväljast ära. Jälgige tähelepanelikult, et kõik kaarditoimingud tehtaks Teie silme all.

Pangakaardi turvalisuse suurendamiseks on veel võtteid. Kui Teie pank sellist teenust võimaldab, siis tellige kindlasti SMS-teavitus kõikide oma kaarditoimingute kohta. Aeg-ajalt tuleks vahetada PIN-koodi (aga ei tasu kasutada uueks koodiks oma sünnikuupäeva või telefoninumbri lõppu). Samuti tasub kehtestada tehingulimiit või hoopis langetada see nullini, võttes piirangu maha ainult enne ostu sooritamist või sularaha väljavõtmist. Ning kindlasti säilitage kõikide tehingute kohta maksedokumendid.

Pildil: skimminguseadmed võivad olla väga erinevad. Selline on üks lihtsamatest.

- Uudised
- Turvalisus