

Schema Nr. 1.

Pareiškėjui gavus nuorodą, susijusią su „Vinted“, „DPD“, „Skelbiu.lt“, „LP Express“ ir kt. internetinėmis platformomis, kuriose prašoma suvesti banko kortelės duomenis (kortelės CCV/CVV numerį, galiojimo datą ir kortelės numerį) ir, atlikus nurodytus veiksmus, sukčiai, neteisėtai įgiję asmens mokėjimo kortelės duomenis, juos neteisėtai panaudoja, atsiskaitydami internetinėse svetainėse už prekes ar paslaugas.

Schema Nr. 2.

Sukčius, paskambinęs pareiškėjui ir prisistatęs banko darbuotoju, siekdamas suklaidinti nukentėjusįjį, nurodo apgaulingą informaciją (pvz. pareiškėjo atžvilgiu daromas nusikaltimas arba būtina atlikti tariamą elektroninės bankininkystės paskyros saugos užtikrinimą ar programinės įrangos atnaujinimą), ir išvilioja elektroninės bankininkystės prisijungimo duomenis, t. y. nukentėjusiojo asmens kodą, prisijungimo prie elektroninės bankininkystės kodus, kuriuos, prisijungęs prie informacinės sistemos, neteisėtai panaudoja inicijuodamas finansines operacijas.

Schema Nr. 3.

Pareiškėjas į mobiliojo ryšio telefoną tariamai iš banko gauna žinutę (pvz. paskyra yra užblokuota arba neteisėtai nuskaityti pinigai), kurioje nurodyta, kad, norint atblokuoti sąskaitą arba blokuoti neteisėtus pinigų pervedimus, būtina paspausti pateiktą nuorodą (pvz. (seb)-accpaslaugos.(com), e-seb-saskaita.(com), (seb).login20.(com), seb.login26.(com), (swed).pagalba-palaikymas.(com) ir kt.).

Paspaudus gautą aktyvią nuorodą, nukentėjusiajam nurodoma suvesti savo elektroninės bankininkystės prisijungimo duomenis (pvz. asmens kodą, banko kliento kodą), juos suvedus, iš nukentėjusiojo banko sąskaitos atliekamos neteisėtos finansinės operacijos. Būkite atidūs, pasidalinkite su draugais!

