Õngitsuslehed kasutasid ära Smart-ID kasutajate tähelepanematuse ja tegid nende nimel uue Smart-ID

7 aastat tagasi - 14.05.2019 Autor: AM

Riigi Infosüsteemide Ameti aprilli ülevaates olukorrast küberruumis räägitakse sellest, kuidas õngitsusleheküljega peteti kasutajatelt välja Smart-ID loomiseks vajalikud andmed ja loodi pahaaimamatute kasutajate nimel uus Smart-ID, millega sai muuhulgas ka internetipanka sisse logida.

Järgneb lõik RIA aprilli ülevaatest.

Aprillis saadi teada intsidentidest, kus õngitsussõnumeid ja õngitsuslehti ära kasutades üritati luua ohvrite nimel uut Smart-ID kontot, mis teadaolevalt mitmel korral ka õnnestus. Kasutajatele saadeti mobiiltelefoni tuntud panga nimelt sõnum, mis suunas näiliselt panga sisselogimisleheküljele. Seal suunati ohver õngitsuslehele Mobiil-ID-ga sisse logima. Kui ohver sisestas oma kasutajatunnuse ja isikukoodi ja PIN 1, alustasid kurjategijad samal ajal taustal hoopis uue Smart-ID konto loomist.

Ohvri tähelepanu hajutades suunati teda tegema järgmisi vajalikke samme, et Smart-ID konto loomine taustal lõpetada. Niimoodi said kurjategijad luua uue Smart-ID konto ja logida ohvri andmetega sisse teenustesse, mis Smart-ID sisselogimist pakuvad, sealhulgas pankadesse. Teadaolevalt on üksikuid ohvreid, kes on kannatanud ka rahalist kahju.

Sisuliselt kasutavad kurjategijad ära olukorda, kus kasutaja ei pööra tähelepanu kontrollkoodidele ja teenusepakkujate nimedele ning sisestab oma PIN-koodid harjumusest. Smart-ID teenusepakkuja SK ID Solutions tegutseb taoliste petuskeemide vältimise nimel ja töötab välja lisameetmeid kasutajate teavituseks.

- Uudised
- Turvalisus

Pilt

