MasterCard Worldwide ieteikumi datorkrāpniecības mēģinājumu novēršanai

Sakarā ar pikšķerēšanas (*phishing*) skaita pieaugumu, kuru mērķis ir lietotāju konfidenciālas informācijas iegūšana (lietotājvārds, parole), aicinām iepazīties ar MasterCard Worldwide izstrādātiem ieteikumiem datorkrāpniecības mēģinājumu novēršanai.

Lai izsargātos no pikšķerētājiem un datu izmānīšanas, lūdzu ievērojiet šos ieteikumus:

- **neatklājiet nevienam savu konfidenciālo (aizsargājamo) informāciju. Banka vai MasterCard nekad no klientiem nepieprasa konfidenciālo informāciju (kartes numuru, PIN kodu, 3D Secure Code, CVV), izmantojot elektronisko pastu**;
- nekad neklikšķiniet uz internetvietņu saitēm nepazīstama sūtītāja e-pasta vēstulē, jo sūtītājs, iespējams, ir atdarinājis vietni (izveidojis viltoto vietnes versiju). Apmeklējiet Bankas vietni, pieslēdzieties internetbankai vai sazinieties ar Bankas darbinieku (piezvaniet darbiniekam);
- neatvērt un nelejupielādēt aizdomīgus e-pastam pievienotus dokumentus;
- periodiski mainiet paroles;
- ja esat saņēmis e-pasta vēstuli, kurā jūs mudina sniegt lietotāja personīgos datus (kartes datus), lūdzu nekavējoties dariet šo faktu zināmu Bankai;
- atcerieties, ka pikšķerētāju vēstulēs bieži vien ir gramatiskās un ortogrāfiskās kļūdas, un vēstulēs tiek lūgts sniegt informāciju par jūsu kontu (jūsu kartes datus). Tas skaidri liecina par krāpšanas mēģinājumu. Pikšķerētāji norāda interneta adreses, kuras ir garākas nekā parastās, norāda vietrāžus, kas ietver zīmi @, un adresēs ir drukas kļūdas. Šīs ir kopīgas pazīmes, kas ir raksturīgas pikšķerētāju vēstulēm jeb surogātpastam. Tā kā pikšķerēšanas mērķis ir lietotāju konfidenciālas informācijas izzagšana, pikšķerētāji ir viltīgi un prot maskēt pašu izliktās lamatas;
- atveriet tikai no zināmiem un uzticamiem sūtītājiem saņemtu e-pasta ziņojumu pielikumus;
- nekavējoties sazinieties ar Banku, tiklīdz jums rodas aizdomas, ka jūsu kartes datiem ir nesankcionēti piekļuvusi neautorizēta persona;

Parasti pikšķerētāji izveido viltus internetvietni klienta iemānīšanai. Lietotāju aicina to apmeklēt, tādējādi panākot, ka lietotājs ievada konfidenciālo informāciju (lietotājvārdu un paroli). Lietotājus viltotajā internetvietnē ievilina ar masveida sūtītām e-pasta vēstulēm it kā no labi pazīstamiem un uzticamiem zīmoliem, vai arī no reālas finanšu iestādes (bankas). Krāpnieki var izmantot arī sociālos tīklus, lai nozagtu piekrāptā lietotāja identitātes datus. Lietotājs tiek pamudināts noklikšķināt uz pievienotās saites un nokļūt attiecīgajā vietnē. Kad jūs būsiet nokļuvis viltotajā internetvietnē, krāpnieki mudinās ievadīt jūsu konfidenciālo informāciju (lietotājvārdu un paroli). Pikšķerētāji pielieto psiholoģiskos paņēmienus un daudzveidīgas taktikas, lai izkrāptu lietotāja personīgos datus un piekļūtu bankas kontiem.