Насоки за Информативна сигурност во дигиталниот простор

Никогаш не ги откривајте вашите лични/финансиски информации на непознати лица кои остваруваат контакт преку емаил, телефон и писмен допис, исто важи и за компании кои се претставуваат како консултанти, маркетинг агенции па дури и извршители со кои веќе сте поставиле деловен однос бидејќи немате никаква гаранција за идентитетот на лицето кое бара да пристапи до личните податоци.
Согласно Законот за заштита на личните податоци и интерните акти на Банката ниту една ваша контакт информација не смее да биде дадена на трети лица(компании) без ваша писмена согласност.
Врз основа на пропишаната Политика за информативна сигурност на банката и Политиката за утврдување на осетливи информации, службените лица од банката ниту трета страна со која банката има склучено договори за соработка, никогаш не смее да побара да му ги разоткриете следниве податоци за идентификације: вашата лозинка, пинот од дигиталниот сетификат(усб токен) и листа на токен кодови за еднократна употреба (OTP).

Доколку се случи да ве контактира лице (преку било кој комуникациски канал – маил,телефон) и се обидува да ви пружи техничка поддршка за некој проблем што сте го пријавиле и притоа ви бара да ги откриете некои од горенаведените информации веднаш прекинете ја комуникација и пријавете го настанот.
По потреба побарајте привремено блокирање на пристапот до е-банкинг од вашето корисничко име.
По преземањето на претходно наведените заштитни мерки имате право случајот да го пријавите во МВР како и во Дирекцијата за заштита на лични податоци каде што по службена должност ќе се отпочне истрага против евентуалните сторители на делото.

Независно од авторитетот на страната со која во моментот комуницирате и начинот на кој таа комуникација ја воспоставувате (преку било кој комуникациски канал – маил,телефон) не одговарајте и игнорирајте ги барањата за проследување на следните чувствителни информации: PAN - броеви на платежни картички, PIN-от за авторизација на POS или ATM, сигурносниот 3-цифрен/4-цифрен код (CVV/CSC) на позадината на картичката со кој се авторизираат плаќањата за електронската трговија преку Интернет, ЕМБГ или други лични податоци кои се особено чувствителни и за кои Дирекцијата за заштита на лични податоци пропишала посебни стандарди за нивна заштита и евентуална размена.

Линкови
За пристап до електронското банкарство користете ја официјалната веб страна на банката и притоа осигурете се дека користите https протокол кој може да го видите во url лентата во вашиот пребарувач пр. http://www.stbbt.mk
Е-банкинг пристап преку линкови добиени по електронска пошта или изложени на трети сајтови независно дали се работи за Интернет весници, социјални сајтови (Facebook, LinkedIn, Instagram, Twitter итн.), блогови и сл., во основа го носат ризикот да завршите во мрежата на измамниците и да станете жртва на кражба на вашиот дигитален идентитет.