Интернет банкарство

Приступ вашем интернет банкарском порталу, уколико је то могуће, остварите само са вашег личног рачунара (или другог наменског рачунара) и посредством познатих мрежних окружења, избегавајте јавне рачунара и јавне WiFi мреже. Увек сами унесите адресу којој желите да приступите у веб претраживач, избегавајте приступ сајту преко линкова примљених у електронским порукама.

Бежичне мреже WiFi

Уколико имате бежичне мреже увек их осигурајте веома јаком лозинком и најснажнијим протоколом за аутентификацију који подржавају (погледајте упутство вашег бежичног уређаја или проверите са провајдером интернет услуга).

Не наседајте на понуде које звуче „превише добро“

Нападачи често користе различите методе обмањивања корисника како би их изманипулисали да изврше одговарајуће задатке (инсталације малициозног софтвера, одавање приватних података и сл.), уколико добијете електронску поруку или позив у коме се од вас захтева да одате личне или поверљиве податке добро проверите да ли знате коме их дајете и да ли то стварно желите да урадите.

Обављање трансакција на АТМ апаратима

Приликом уноса вашег пина на банкомату будите дискретни и заклоните тастатуру од погледа, не дозволите непознатој особи да вам асистира приликом трансакције.

Пин је ваш лични идентификациони број који не треба да зна нико осим вас, чак ни банка.

Пин никада немојте носити заједно са картицом.

У случају да АТМ апарат задржи вашу картицу, одмах обавестите банку.

Изгубљену или украдену картицу одмах пријавите вашој банци.

Корисни линкови

http://www.ubs-asb.com/Default.aspx?tabid=9911
http://www.kliknibezbedno.rs
http://www.netpatrola.rs

УБС АСБ
УДРУЖЕЊЕ БАНАКА СРБИЈЕ
ASSOCIATION OF SERBIAN BANKS

Безбедно пословање у дигиталном свету

Шта би све корисник требало да зна о безбедном пословању у дигиталном свету

Како би обезбедили сигурно окружење банке улажу огромне напоре и значајна средства за ову намену. Да би се осигурао читав ланац у банкарском пословању посебан акценат се ставља на крајњег корисника банкарских услуга и његову безбедност. Због тога дајемо кратка упутства за безбедно пословање у дигиталном окружењу.

Одржавајте ваше системе ажурним

Редовно ажурирајте ваше системе са најновијим исправкама са сајтова произвођача (оперативни систем, Office, Adobe, Java и др.).

Нападачи често користе неажурност крајњих корисника и пропусте у дизајну софтера а за које је произвођач већ направио и објавио исправке.

Имајте инсталиран и ажуриран софтвер за детекцију злонамерног кода и заштитни зид

Увек на свим уређајима (рачунар, таблет, мобилни телефон и др.) имајте активиран и ажуриран софтвер за превенцију злонамерног кода (антивирус, антималвер програми). Редовно вршите скенирање вашег уређаја као и скенирање уређаја које прикључујете на уређаје (USB, дискови и др.)

На вашем рачунару укључите заштитни зид (firewall) како би отежали неовлашћен приступ вашем рачунару са мреже.

Легалан софтвер је гарант безбедности система, пиратизоване копије које се могу инсталирати често садрже у себи малициозни код и њихова употреба представља кривично дело.

Редовно правите резервне копије

Учестале су појаве злонамерног софтвера који енкриптује ваше податке и захтева новац за њихово ослобађање (криптомалвер и ransomware).

Отказ хардвера као и разни злонамерни програми такође могу оштетити или уништити ваше податке, прављењем резервне копије обезбеђујете се од оваквих претњи.

Веб сајтови и интернет куповина

Обратите пажњу на тип сајтова које посећујете и на њихов садржај. Никако не инсталирајте додатне програме који вам се нуде уколико нисте у потпуности сигурни да вам је то неопходно. Уколико је потребно да инсталирате неку компоненту најсигурније је да га преузмете са сајта оригиналног произвођача софтвера.

Уколико купујете на интернету најбоље би било да то чините код познатих и реномираних компанија које користе сигурне методе приликом плаћања вашом картицом.

Увек обратите пажњу да ли се приликом слања поверљивих информација налазите на сајту који ваше податке енкриптује, као и на сертификате који су им додељени за ову намену (адресе сајтова који енкриптују садржај почињу са https:// а не са http://).

Електронска пошта

Електронска пошта је широко распрострањен вид комуникације зато је и уобичајени канал дистрибуције злонамерног софтвера.

Код отварања електронских порука будите обазриви приликом преузимања активних садржаја из порука (линкови, додаци и др.) нарочито уколико долазе од непознатих пошиљалаца. Имајте на уму да се нападачи служе различитим техникама којима покушавају да преваре особу којој шаљу поруку (фишинг поруке). Фишинг поруке могу изгледати као да долазе са праве елктронске адресе јер је нападач креирао лажно Од (From) поље. Уколико добијете сумњиву поруку коју нисте очекивали најбоље је да лично контактирате особу која вам је ту поруку посалала и уверите се у њену исправност.

Лични подаци

Велики проценат превара и злоупотреба је као последица компромитовања корисничких креденцијала (лозинка, пин и др.). Имајући ово у виду посебну пажњу обратите на чување оваквих података, немојте их никоме саопштавати и записивати на лако доступним местима. Губитак и злоупотреба личних података могу имати за последицу крађу идентитета која са собом повлачи мноштво других проблема за корисника.