Rekomandime për siguri të Internet bankës së Bankës Komerciale SHA Shkup për parandalimin e keqpërdorimeve dhe malverzimeve të identitetit.

"Zinxhiri është aq i fortë, sa është e fortë edhe hallka e tij më e dobët"

Të nderuar shfrytëzues,

Nevoja për ta vërtetuar identitetin personal është pjesë përbërëse e jetës moderne. Në botë, trendi i veprave kriminele, të cilat në vete ngërthejnë keqpërdorimin e identitet të vjedhur ose joekzistues, është në rritje. Dokumenti sqaron se çka mund të bëni ju me qëllim që të parandaloni tentimin për vjedhje kriminele të identitet tuaj, apo keqpërdorimin e tij dhe mundëson këshilla plotësuese që mund t'ju ndihmojnë në një situatë të imagjinuar, kur ju dyshoni se jeni viktimë e vjedhjes së identitet tuaj.

Në broshurën të cilën mund ta shkarkoni në sajtin e Internet bankës janë shtuar rekomandime për siguri për shfrytëzuesit, të dala nga praktika më e mirë botërore në fushën e sigurisë informative (best security practices).

VËREJTJE: Në rast të çëfarëdolloj veprimi të pazakontë të internet shfrytëzuesit, gjatë shfrytëzimit të Internet bankës së Bankës Komerciale, që mund të jetë pasojë e programeve eventuale të keqpërdorimit të instaluara në kompjuterin tuaj (virus, trojan, spyware...), ju lutemi që sa më shpejt ta kontaktoni Help Desk-un tonë, ta informoni për situatën e krijuar dhe t'i ndjekni këshillat, të cilat do t'i merrni për siguri.

Këshilla për siguri të Internet bankës së Bankës Komerciale SHA Shkup për parandalimin e malverzimeve me keqtrajtimin e identitetit

Përmbajtja

Shfrytëzuesit e Internet bankës dhe roli i tyre në sistemin e sigurisë

Së pari, të sqarojmë se fillimi pionier i punës së Internet bankës së Bankës Komerciale që në vitin 2001, me fillimin e produksionit pilot për pagesa në qarkullimin pagesor në vend, për persona juridikë, në shtator të vitit 2004. Sikurse edhe fillimi masovik i produksionit në 1 tetor 2006, e deri më tash, asnjë shfrytëzues (person juridik apo fizik) i Internet bankës nuk ka paraqitur dhe s'ka qenë viktimë e qasjes së paautorizuar deri tek informatat e llogarive bankare me të cilat disponon (llogaritë personale apo të kompanisë me të cilat disponon) dhe nuk është vërejtur incident i disponimit të mjeteve në llogari përmes Internet bankës.

Në testimet periodike të *ethical hacking* nga ana e kompanive të specializuara të vendit dhe të jashtme në fushën e sigurisë informative, nuk janë vërejtur dobësi, të cilat mund ta rrezikojnë seriozisht sigurinë e Internet bankës si në zgjedhjen dhe miratimin e teknologjive ashtu edhe në proceset dhe aktivitetet e aprovuara të personave të autorizuar për zhvillimin dhe mirëmbajtjen e saj.

Pavarësisht nga të gjitha tentimet e njëpasnjëshme dhe të sinkronizuara në fushën e sigurisë që i bën Ekipi për zhvillim i Internet bankës me Ekipin për siguri informative dhe Përgjegjësin për siguri të sistemit informativ të Bankës si dhe persona të tjerë profesional në kuadër të shërbimeve të bankës, siguria gjithmonë ka qenë çështje e një përzierjeje të përsosur dhe të balancuar në mes të stafit top të trajnuar, të mirëinformuar dhe përdorues të trajnuar, zgjidhjeve dhe aplikimit të teknologjive të besueshme dhe të njohura ndërkombëtarisht, si dhe përdorimin e tyre të përditshëm përmes procedurave të mirëpërcaktuara dhe një morie masash mbrojtëse të njohura nën termin *best security practices*.

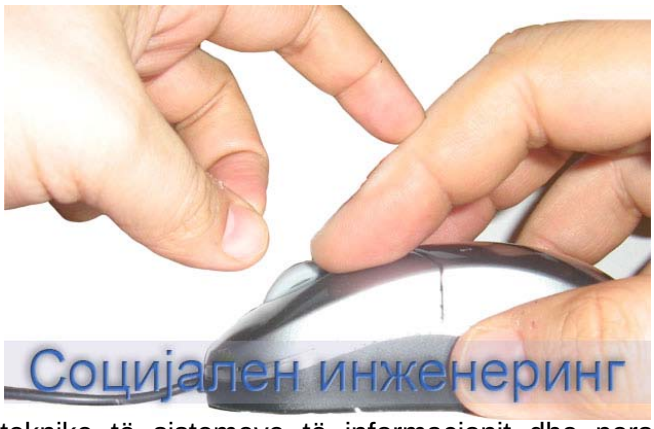
Në mënyrë që tradita e përdorimit të sigurt të Internet bankës të vazhdojë në të ardhmen, ky punim i është dedikuar lidhjes më të rëndësishme në zinxhirin e sistemeve të sigurisë së Internet bankës, pikërisht për mbrojtjen e të cilave është zbatuar: klientët tanë të çmuar pa të cilët sistemi i sigurisë, pavarësisht kontrollit dhe proceseve teknike të zbatuara, mund të vihet në pikëpyetje, nëse të njëjtat nuk kujdesen ndaj kërcënimeve specifike, që për fat të keq, eksitojnë gjatë përdorimit të përditshëm të Internetit.

Vjedhjet e identitetit dhe mashtrimi duke abuzuar me identitetin

Vjedhja e identitetit (Identity theft), është përdorimi dhe abuzimi i identitetit të një personi tjetër, pa dijeninë dhe miratimin e tij/saj. Mashtruesi duhet të ketë qasje në të dhënat tuaja personale apo vjedh dokumentet tuaja të identitetit, në formë të letrës (letërnjoftimin, pasaportën) ose shenjat digjitale për të vërtetuar identitetin tuaj, si emrin e përdoruesit dhe fjalëkalimin, listën ose pajisjen për gjenerimin e kodeve për një përdorim të vetëm, certifikatën tuaj digjitale që është ruajtur në PC, CD ose token të sigurisë, PIN-in për qasje në certifikatën digjitale, etj.

Mashtrimi me anë të abuzimit të identitetit (Identity fraud), përbën përdorimin e paautorizuar ose keqpërdorimin e identitetit të vjedhur në aktivitetet kriminele që ka për qëllim përvetësimin e paligjshëm të mallrave, shërbimeve ose mjeteve financiare.

Bëhuni gjithmonë të kujdesshëm - Inxhinieringu social



Inxhinieringu social është manipulim i sofistikuar ndaj një personi të caktuar nga ana mashtruesit me qëllim që i njëjti nga viktima, në mënyrë të paautorizuar, të nxjerrë informata të ndjeshme ose ta bindë viktimën për të kryer një sërë aktivitetesh të paautorizuara.

Në vend që mashtruesi të përpiqet të gjejë dhe shfrytëzojë dobësitë e mundshme të kontrolleve teknike të sistemeve të informacionit dhe personalisht të futet me anë të aplikimit të teknikave të sofistikuara të piraterisë dhe pajisjeve, i njëjti përpiqet të krijojë marrëdhënie të besimit me viktimën, ku duke krijuar pikëpamje të gabuar për identitetin, viktimën e manipulon në atë mënyrë që i vjedh informatat e ndjeshme, të cilat mund të përdoren në krime të tjera. Zakonisht, mashtruesit prezantohen me identitet falco, duke falsifikuar e-mail adresën e dërguesit dhe duke përdorur logon e kompanisë në emër të së cilës dëshiron të prezantohet, por për qëllime të inxhinierisë sociale mund të përdoren edhe më shumë pajisje konvencionale të komunikimit si telefoni dhe posta.

Rekomandime

Mos i jepni të dhënat tuaja personale ose informacionin financiar (si llogarinë tuaj), personave të panjohur, të cilët ju kontaktojnë nga kompanitë me të cilat asnjëherë nuk keni kontaktuar më parë dhe ju kontaktojmë përmes e-mailit, telefonit ose me shkrim. Përveç kësaj, e njëjta vlen edhe për agjencitë të cilat prezantohen si konsulentë, përmbarues apo agjencitë e marketingut, me kompanitë me të cilat keni krijuar tashmë një marrëdhënie biznesi, të paktën edhe për faktin se nuk ka asnjë garanci në lidhje me identitetin e palës së tretë, e cila kërkon qasje në informatat e ndjeshme.

Keni parasysh faktin se këto kontakte nga një palë e tretë (agjenci), në emër të Bankës janë të pamundura. Sipas Ligjit për mbrojtjen e të dhënave personale dhe rregulloreve të brendshme të Bankës, pa lejen tuaj me shkrim, as informacionin e kontaktit tuaj si telefoni, email-adresa, adresën në shtëpi nuk do t'u zbulohet të palëve të treta (agjencive, kompanive, etj.).

Sipas Politikës për siguri informative të Bankës dhe Udhëzimeve për zbatimin e Politikës për siguri informative, asnjë zyrtar i vetëm i Bankës ose palë e tretë me të cilën Banka ka nënshkruar marrëveshje bashkëpunimi, pa marrë parasysh situatën pse ju ka kontaktuar assnjëherë nuk guxon t'ju pyes që t'i zbuloni karakteristikat e mëposhtme të identifikimit digjital për qasje në shërbimet e Internet bankës:

- fjalëkalimin tuaj përdorues;
- PIN-in për të hyrë në certifikatën tuaj digjitale dhe
- Listën e kodeve prë një përdorim.

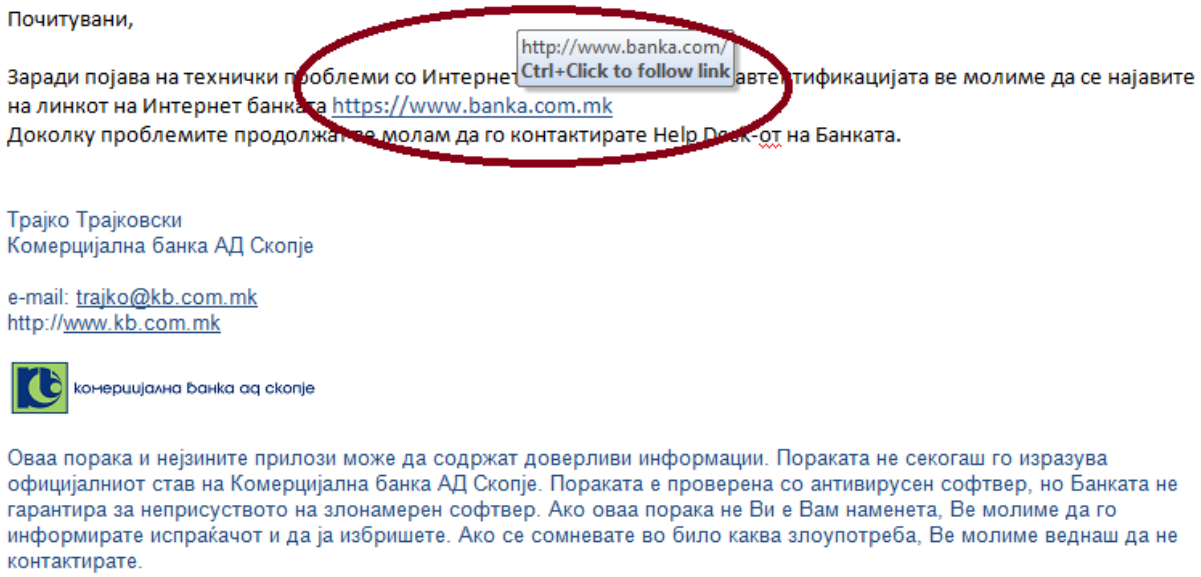
Pa marrë parasysh se personi ju ka kontaktuar me telefon, e-mail ose mundohet t'ju ndihmojë që të mënjanoni ndonjë problem teknik për të cilin ndoshta keni kërkuar ndihmë, nëse incidenti i lartëpërmendur ndodhë, menjëherë ndërpriteni komunikimin dhe informojeni Help Desk-un e Bankës për ngjarjen.

Kini kujdes të mos u zënë – Peshkimi (Phishing)

Phishing**–u** është një mashtrim i paramenduar mirë, ku qëllimi përfundimtar është mbledhja e informatave të ndjeshme digjitale për identifikimin personal si emri i përdoruesit dhe fjalëkalimet, PIN-ët për kartat ose PIN-ët për qasje në certifikatat digjitale, me çka mashtruesi maskohet me qëllim që t'i ngjajë një entiteti të besuar në komunikimin elektronik, ku shfrytëzuesi është i mësuar për të punuar (p.sh. ueb faqja i ngjan Internet bankës së Bankës Komerciale SHA Shkup).

Peshkimi me ndihmën e mesazheve të dërguara me postë elektronike

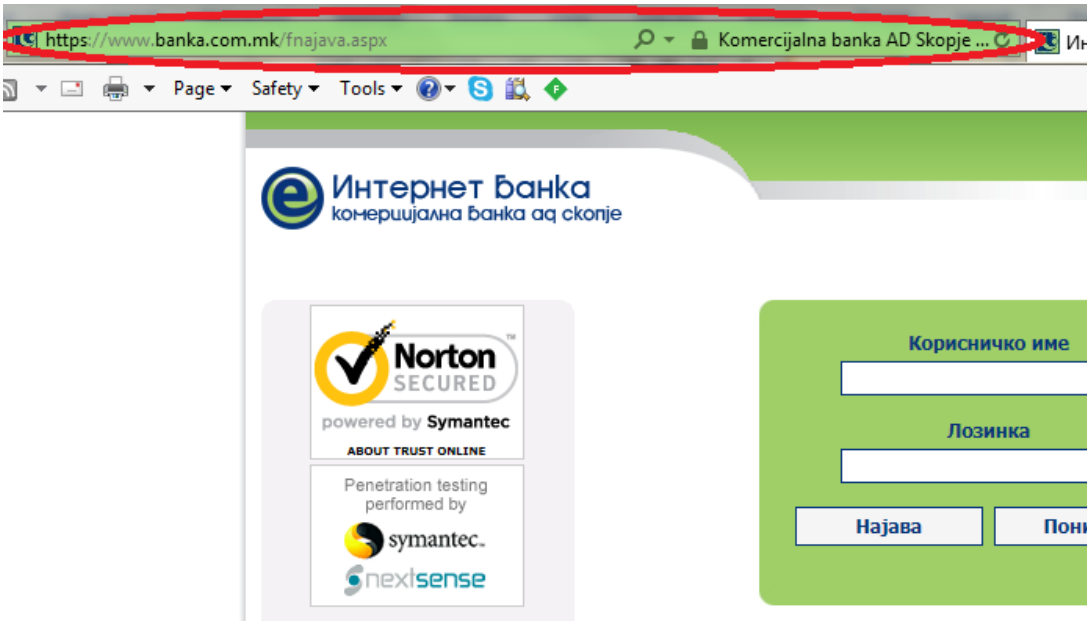
Një përpjekje klasike e mashtrimit, ku kombinohet inxhinieria shoqërore dhe peshkimi si teknikë, është shembulli në vazhdim:

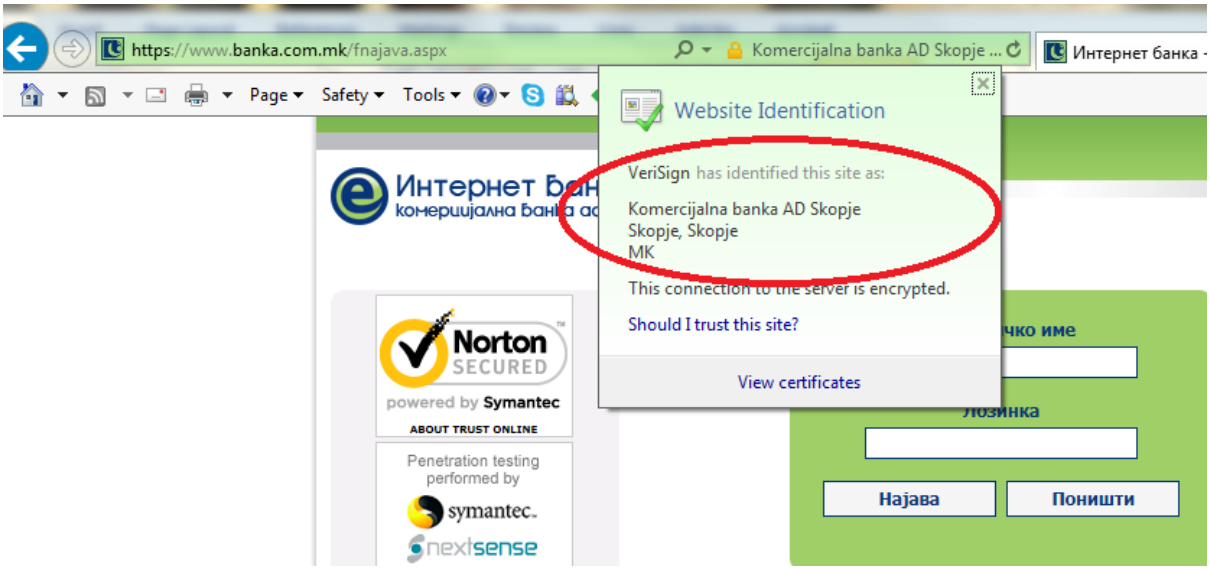


Nëse treguesi i miut është më afër linkut do të vëreni se i njëjti do t'u çojë në një adresë tjetër, ndryshe nga https://www.banka.com.mk (http://www.banka.com). Shpesh, tek adresat e rreme (replica sites), ueb faqet nuk janë të pajisura me një certifikatë të vlefshme serverike dhe përdorin lidhje të zakonshme të pakriptuar http (faqet e kriptuara domosdoshmërisht janë https), por gjithmonë ky është rasti.

Viktima që do të klikojë në link, drejtohet në ueb faqen, e cila sipas pamjes ngjan me faqen origjinale të Bankës, por gjithsesi nuk e ka të njëjtin funksion. Nëse pak më mirë i shohim detajet në shiritin e adresës, dallimet mund të shihen:

Internet banka e Bankës Komerciale SHA Shkup (vini re në pjesën e Kyçit ku me klikim paraqitet vërtetimi se jeni të lidhur ueb faqen origjinale)	Kopja e rreme e ueb faqes së Internet bankës që i vjedhin llogaritë e përdoruesve dhe fjalëkalimet (në rastin e Link-ut është ndryshme dhe mundon ikona e Kyçit)





Nëse përdoruesi përpiqet të hyjë dhe e fut llogarinë e përdoruesit dhe fjalëkalimin e saktë në ueb faqen e rreme të Internet bankës, viktima pa mos e ditur, ia përcjell karakteristikat e tij digjitale mashtruesit, i cili më vonë mund t'i përdorë ato në mënyrë që të merr informacionin e ndjeshëm financiar të paautorizuar për përdoruesin.

Peshkimi me ndihmën e shtesave qëllimkëqija të shfletuesit të Internetit (Man in the middle of the browser attack)

Një mënyrë pak më moderne dhe e sofistikuar e "Peshkimit" nënkupton përdorimin e shtesave qëllimkëqija për Internet shfletuesit e përdoruesit (Internet Explorer, Firefox Mozilla, Google Chrome), të cilin shfrytëzuesit më shpesh e instalojnë në kompjuterin e tyre si shtesë e dobishme e shfletuesit të Internetit. Jo rrallë ndodhë që pa dijeninë e shfrytëzuesit, gjatë vizitës të një faqeje të dhënë qëllimkeqe, duke i shfrytëzuar dobësitë interne të sistemit operativ të shfletuesit të internetit, kjo shtesë (**Plug-in**, **Add on**) edhe të instalohet pa njohurinë dhe miratimin e shfrytëzuesit.

Shtesa qëllimkeqe e përgjon rishikimin e faqes së Internetit dhe pasi e zbulon lidhjen HTTPS apo maskimin për të futur emrin e përdoruesit dhe fjalëkalimin në dritaren e formës modulare pop-up, lëshon mesazhin e mëposhtëm:

We do not recognize the computer you are using.

To continue with Online Banking, please provide the information requested below.

Confirm Your Identity

Instructions: Provide your Card Security Code and as much additional security information as you can. Your entries must match the information on the account record and will be used solely to confirm your identity.

Card Number :

[ ]

Card Security Code (required): Turn to the BACK of your card and look in the white panel where you signed your card. Type the last 3 digits of the code.

[ ]

Expiration Date: month/year

[01 \/] / [2010 \/]

ATM PIN:

[ ]

[Continue]

Në sfondin e dritares së posaparaqitur s'është ueb faqja e Internet bankës, por dritarja modulare që nuk është pjesë e së njëjtës. Programi qëllimkeq e shfrytëzon besimin e përdoruesit në faqen e Internet bankës dhe përpiqet të vë në huti se të dhënat që kërkohen në formën e posaparaqitur janë pjesë e së njëjtës.

Sigurisht, në qoftë se e analizojmë përmbajtjen e kësaj forme të inputit, mund të perceptohen më shumë hapa të palogjikshëm që sugjerojnë për tentativë mashtrimi:

1. Mesazhi është i shkruar në gjuhën angleze. Komunikimi zyrtar i Bankës me klientët rezident bëhet në gjuhën maqedonase.

2. Mesazhi insiston në të dhëna të ndjeshme për "gjoja" identifikimin shtesë. Duam të theksojmë se në momentin e dhënë, Banka kryen identifikimikn dyfaktorial për llogarinë tuaj të përdoruesit, fjalëkalimin dhe listën e kodeve për një përdorim apo token dhe PIN-in për qasje në të njëjtin. Këto karakteristika, janë të mjaftueshme që Internet banka t'ju identifikojë. Për më tepër, ***Banka asnjëherë nuk do të kërkojë***

nëpërmjet ueb faqes apo mesazhit të dërguar në postën elektronike që t'i jepni të dhënat e ndjeshme të lartëpërmendura.

Rekomandime:

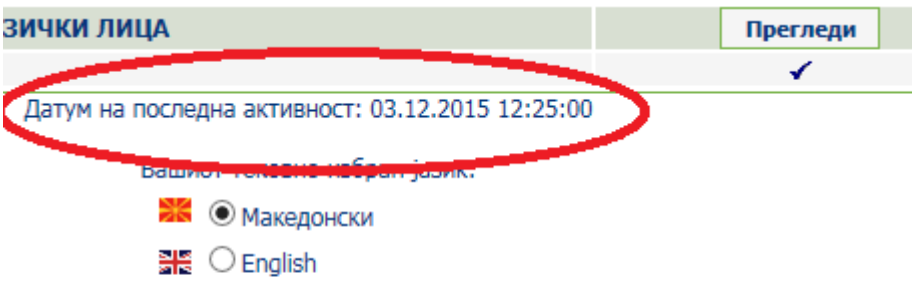
Asnjëherë të mos shfrytëzoni linqe nga faqe të treta për të arritur tek ueb faqja e Internet bankës. Në shfletuesin e Internetit shkruani URL adresën https://www.banka.com.mk dhe nga e njëjta krijoni shkurtesë (shortcuts), apo shtoni atë në ueb faqet tuaja të preferuara (Favorites). Gjatë përdorimit të ardhshëm, klikoni në shkurtesën ose linkun Favorites. Çfarëdo qasje tjetër në ueb faqen e Internet bankës nëpërmjet linqeve të pranuara me e-mail ose nëpërmjet faqeve të treta, pa marrë parasysh se a bëhet fjalë për revista online, mediume sociale (Facebook, MySpace), BLOG dhe të ngjashme, në thelb ato bartin rrezikun për të përfunduar në rrjetin e mashtruesve dhe të bërit një viktimë e vjedhjes së identitetit tuaj digjital.

Pavarësisht autoritetit të faqes që aktualisht komunikoni dhe mënyrës se si e keni krijuar komunikimin (ueb faqja e Internet bankës, mesazhi i dërguar me e-mail, etj.), mos u përgjigjni dhe injoroni kërkesat për të përcjellë informacionin e mëposhtëm të ndjeshëm:

- Numrin e kartave të pagesës
- PIN-in për autorizim në POS apo Bankomat
- Kodin e sigurisë 3- shifror nga ana e pasme e kartës me të cilin autorizohen pagesat për tregti elektronike nëpërmjet Internetit.
- Numrin amë ose të dhënat personale, të cilat janë mjaft të ndjeshme për të cilat Drejtoria për mbrojtjen e të dhënave personale ka përshkruar standardet specifike për mbrojtjen e tyre dhe shkëmbimin e mundshëm.

Veproni shpejt dhe me urtësi - zbulimi dhe procedurat në rast të vjedhjes së identitetit tuaj

Pas çdo logimi të suksesshëm në Internet bankë, vazhdimisht regjistrohet koha e aktivitetit tuaj të fundit. Në anën e profilit tuaj të përdoruesit, mund të shihni dhe krahasoni rezultatet tuaja për qasjen e fundit të autorizuar në Internet bankë:



Në qoftë se hetoni se data dhe koha nuk përshtaten me qasjen tuaj të fundit, menjëherë ndryshojeni fjalëkalimin tuaj dhe paraqiteni rastin në Help Desk-un e Internet bankës, ku në bazë të ditarëve të aktiviteteve do të sqarohen detajet e qasjes eventuale të paautorizuar në financat tuaja.

Rregullisht kontrollojeni ekstraktin tuaj dhe nëse hetoni zëra borxhi në ekstrakt për të cilat jeni i sigurt se nuk i keni autorizuar ju dhe nuk përshtaten me mallrat dhe shërbimet e blera, menjëherë kontaktojeni HelpDesk-un e Bankës dhe kërkoni udhëzime të mëtejshme.

Në rast të humbjes së letrës në të cilën keni regjistruar emrin e përdoruesit apo fjalëkalimin, mundohuni ta kontaktoni Internet bankën dhe menjëherë ndryshojeni fjalëkalimin e përdoruesit. Pas ardhjes së parë, për Bankën dhe identifikim tuaj me kartë identiteti apo pasaportë të vlefshme, do të lëshohet një fjalëkalim i ri, të cilin më pas duhet ta ndryshoni dhe qasja në Internet bankë do t'u mundësohet sërish.

Në kushte të humbjes apo vjedhjes së listës së kodeve apo pajisjes së sigurisë, menjëherë raportojeni çështjen me Help Desk-un dhe kërkoni bllokim të përkohshëm të qasjes në Internet bakë për llogarinë tuaj të përdoruesit.

Në të gjitha rastet e përmendura më sipër, veçanërisht është thelbësore që gjërat të kryhen në mënyrën si vijon:

- Kontaktojeni Help Desk-un e Bankës dhe sipas nevojës kërkoni bllokim të përkohshëm të qasjes në Internet bankë për llogarinë tuaj të përdoruesit.
- Përveç kësaj, pas marrjes së masave të lartpërmendura, keni të drejtë që precedentin ta raportoni në Ministrinë e Brendshme dhe në Drejtorinë për mbrojtjen e të dhënave personale, e cila zyrtarisht do të fillojë një hetim kundër kryerësve të mundshëm të krimit.

Dobësitë e sigurisë dhe rekomandimet për shmangie

- Në qoftë se jeni i/e kyçur në Internet bankë, asnjëherë mos e lini kompjuterin tuaj hapur dhe pajisjen e sigurisë të futur brenda në USB portin ose në tavolinën tuaj të punës listën e kodeve për një përdorim. Në qoftë se këtë e bëni në një vend që është mjaft i frekuentuar nga persona të tjerë, mashtruesve të mundshëm ua keni lënë të gjitha dyert hapur për qasje në asetet tuaja financiare.
- ✓ Në kushtet kur përkohësisht largoheni nga kompjuteri i juaj, duhet ta mbyllni atë (lock workstation) dhe ta merrni me vete listën e kodeve për një përdorim të vetëm ose pajisjen e sigurisë. Duhet patur parasysh faktin se pajisja e sigurisë vetëm njëherë e kërkon PIN-in për qasje në çelësin tuaj privat dhe i njëjti automatikisht do të çregjistrojë sesionin tuaj pasi të kalojnë 15 – 20 minuta pa aktivitet nëse të njëjtin e nxirrni nga USB porti.

- Asnjëherë mos e shkruani llogarinë tuaj të përdoruesit dhe fjalëkalimin ose PIN-in për qasje në certifikatën digjitale në letër të vendosur në portofolin tuaj ose në listën e emrave të telefonit tuaj celular. Praktika tregon se zakonisht më shumë i humbin ose i vjedhin kuletat dhe telefonat celularë.

✓ Nëse keni frikë se mund ta harroni fjalëkalimin ose PIN-in, atë mund ta ruani në letrën që e mbani të mbyllur në tavolinën ose në shtëpinë tuaj. Përveç kësaj, mundohuni t'i mbani gjërat në vende të ndryshme, me qëllim që në rast të humbjes apo vjedhjes së tyre, të mos i lejoni mashtruesit qasje të paautorizuar.

- Kur ta zgjidhni një fjalëkalim, mos e shfrytëzoni asnjëherë ndonjë nga fjalëkalimet standarde që mund të gjenden në fjalorin e pothuajse çdo mashtruesi (P@ssw0rd, admin, 1234567890, user, operator, Administrator, masterkey, sysadm, manager ….). Duhet shmangur në përbërjen e fjalëkalimit përdorimin e emrave ose datave që lehtë mund të sjellin një lidhje me jetën tuaj private (datëlindja e fëmijëve tuaj, emri i të dashurës suaj, etj.).

✓ Fjalëkalimi, të paktën duhet të ketë 8 karaktere, nga të paktën tre grupe të karaktereve nga këto katër, sipas zgjedhjes suaj të lirë:

  - Shkronja të vogla
  - Shkronja të mëdha
  - Shifra
  - Shenja të veçanta

- Një fjalëkalim nuk preferohet të përdoret më shumë se 90 ditë. Në mënyrë shtesë, mos e ndryshoni fjalëkalimin tuaj më shumë herë radhazi me qëllim që të anashkaloni rregullën, ku sipas së cilës nuk duhet të jetë pjesë e historisë së tri fjalëkalimeve të fundit të përdorura.

✓ Me qëllim që më lehtë ta mbani mend fjalëkalimin, është mirë që të definoni rregullën tuaj, sipas së cilës do të krijoni fjalëkalimet e ardhshme.

- Mos u qasni në Internet bankë nga një kompjuter që është në shfrytëzim publik (p.sh: Internet kafe) apo kompjuter të cilin e mirëmbajnë persona të panjohur. Asnjëherë nuk do të jeni të sigurt se në kompjuterët e lartëpërmendur nuk do të hasni instalime piraterie të aplikacioneve qëllimkeqe (malware), që vjedhin llogaritë e përdoruesve dhe fjalëkalimet pa marrë parasysh se të njëjtit janë marrë për arsye të mosekzistencës apo mbrojtjes së dobët anit-virus, apo të njëjtat janë instaluar me qëllim nga personat që i mirëmbajnë.

✓ Qasjen në Internet bankë bëjeni nga laptopi juaj, kompjuteri të cilin e keni në përdorim në vendin e punës apo nga kompjuteri juaj në punë. Por, nëse jeni qasur në Internet bankë nga një kompjuter i pasigurt dhe i kompromet uar, shfrytëzojeni mundësinë e parë dhe ndryshojeni fjalëkalimin tuaj nga kompjuteri shtëpiak ose laptopi juaj.

- Mos e lini kompjuterin tuaj pa azhurnim të rregullt të antivirusit dhe *firewall* aktiv. Shmangni instalimin e antivirusit nga marka e panjohur për arsye se aplikimet e tilla, zakonisht pas instalimit në mënyrë të gabuar, e paralajmërojë përdoruesin për detektim të rrejshëm dhe kërkojnë pagesë shtesë për mënjanimin e plotë. Ndonjëherë, këto zgjidhje të rreme antivirusi mund të instalojnë aplikacione shtesë

qëllimkëqija (trojan, spyware, key logger dhe të ngjashëm), ose ju drejtojnë në ueb faqe në të cilat bëhet “peshkimi”...

- ✓ Është e këshillueshme të përdorni mbrojtje antivirus nga një prej markave të famshme (Symantec, Nod32, Kaspersky, BitDefender, AVG, Panda, Avast) dhe edicioni të jetë në paketë të plotë të mbrojtur në Internet, ku i njëjti përveç mbrojtjes nga viruset merr mbrojtje edhe nga programe të tjera qëllimkëqija (spyware, adware, trojan), bllokim të JavaScript-ave qëllimkëqija gjatë vizitimit të Internet faqeve, azhurnimit të vazhdueshëm të adresave qëllimkëqija dhe bllokimit të të njëjtave, në dy kahe (outbound dhe inbound), mbrojtje firewall, etj. Ndonjëherë, kombinimi i përshtatshëm i më shumë paketave mbrojtëse softuerike mund të japë nivel më të lartë të sigurisë, por duhet të kihet kujdes të mos e ngadalësoni kompjuterin dhe të mos krijoni konflikt në mes të aplikacioneve.

- Pavarësisht nga sistemi operativ që jeni duke përdorur, sërfimi me Internet shfletues (web browser), gjatë seancës në të cilën jeni regjistruar si një përdorues i privilegjuar (anëtar i grupit Local Administrators në Windows platformë), është i rrezikshëm.
- ✓ Është e nevojshme që në kompjuterin tuaj të krijoni llogari përdoruesi, që nuk i përket asnjë grupi të privilegjuar të përdoruesve dhe të njëjtin ta shfrytëzoni gjatë kohës së sërfimit në Internet, kurse sesionet si përdorues i privilegjuar t’i shfrytëzoni vetëm sipas nevojës kur doni të instaloni ndonjë aplikacion të ri ose të kryeni aktivitete të mirëmbajtjes periodike të kompjuterit tuaj.

- Një nga gjërat më të këqija që mund të bëni është të përdorni një version pirat të sistemit operativ. Përveç se përdorimi i kopjeve të tilla është i paligjshëm dhe i dënueshëm me ligj, një problem tjetër është edhe dukuria shumë e zakonshme që këto kopje të shpërndahen me programe qëllimkëqija paraprakisht të instaluara. Disa nga ato (a.q. Rootkits), shfrytëzojnë teknika të padukshmërisë dhe tejkalimi i thirrjeve të sistemit, në mënyrë, që më vonë ato nuk mund të zbulohen dhe të hiqen nga aplikacionet e antivirusit. Në mënyrë shtesë, softueri piraterik më shpesh përfshin nevojën për ekzekutim të crack-ut (aplikacioni me të cilin nënkuptohet mbrojtje nga shfrytëzimi i palicencuar), me aktivizimin e të cilit gati se çdo herë merrni version të ri të sofistikuar Trojan ose Rootkit. Përveç që rrezikoni vjedhjen e informatave të ndjeshme dhe asgjësimin e dokumenteve tuaja, në të njëjtën kohë rrezikoni që kompjuteri juaj i kompromet uar, pa njohurinë tuaj, të jetë i kontrolluar nga largësia nga struktura të ndryshme kriminale dhe i njëjti të shfrytëzohet për aktivizimin e sulmeve DDoS (Distributed Denial of Service) ndaj ueb faqes së ndonjë kompanie. Në këto raste, IP adresa juaj do të evidentohet si e inkriminuar me çka rrezikoni të jeni i akuzuar për dëmin e shkaktuar eventual.
- ✓ Përdorni softuer të licencuar. Nëse buxheti i juaj financiar nuk ua mundëson një gjë të tillë, atëherë kërkoni alternativë në aplikacionet e ashtuquajtura me kod të hapur (open source).