

ການປ້ອງກັນຄວາມປອດໄພ ແລະ ຄວາມສ່ຽງໃນເວລານໍາໃຊ້ LAOVIETBANK MOBILE BANKING

I. ສິ່ງທີ່ບໍ່ຄວນປະຕິບັດ

1. ບໍ່ຄວນ ບອກຊື່, ລະຫັດເຂົ້າລະບົບ, ລະຫັດ OTP ໃຫ້ກັບຜູ້ອື່ນຮັບຮູ້ບໍ່ວ່າຈະໃນກໍລະນີໃດ, ຮູບແບບໃດ, ນັບທັງຜະນິກງານທະນາຄານ ຫຼື ມີຜະນິກງານໂທຫາແລະອ້າງວ່າເປັນຜະນິກງານຊ່ວຍເຫຼືອລູກຄ້າຂອງທະນາຄານລາວຫວຽດ.
2. ບໍ່ຄວນສະໜອງບັນດາຂໍ້ມູນສ່ວນໂຕທີ່ຝົວຜັນເຖິງບັນຊີ ແລະ ບໍລິການທະນາ ຄານເອເລັກໂຕຼນິກ ເຊັ່ນ: ຊື່ ແລະ ນາມສະກຸນຂອງລູກຄ້າ, ບັດປະຈຳຕົວ, ໜັງສືເດີນທາງ, ເລກບັນຊີ, ທີ່ຢູ່ອີເມວ, ເບີໂທລະສັບທີ່ລົງທະບຽນນໍາໃຊ້ບໍລິການ, ເນື້ອໃນຂໍ້ຄວາມໃຫ້ກັບຜູ້ອື່ນຮັບຮູ້ **ນອກຈາກ** ລູກຄ້າໄດ້ໂທຫາເບີໂທຊ່ວຍເຫຼືອຂອງທະນາຄານລາວຫວຽດ ເພື່ອຂໍຄວາມຊ່ວຍເຫຼືອໃນການນໍາໃຊ້ບໍລິການ.
3. ບໍ່ຄວນເຂົ້າໃຊ້ບັນດາ web ທີ່ບໍ່ໜ້າເຊື່ອຖື, ບໍ່ປ້ອນຂໍ້ມູນສ່ວນໂຕ ແລະ ຂໍ້ມູນບໍລິການທະນາຄານເອເລັກໂຕຼນິກເຂົ້າໄປບໍ່ວ່າຈະເປັນໜ້າເວບໄດ ຫຼື Application ທີ່ບໍ່ທັນເປັນທາງການຂອງທະນາຄານລາວຫວຽດ.
4. ບໍ່ຄວນ ຕັ້ງຄ່າລະຫັດເຂົ້າໃຊ້ Internet Banking ແລະ ບັນດາບໍລິການທະນາຄານແບບອອນລາຍໃນບັນດາອຸປະກອນນໍາໃຊ້ສ່ວນລວມ (ມີຫລາຍຄົນເຂົ້າໃຊ້), ໃນຄອມພິວເຕີສາທາລະນະ.

II. ສິ່ງທີ່ຄວນປະຕິບັດ

1. ລະມັດລະວັງໃນການເຂົ້າໃຊ້ໜ້າເວບປອມ, ລູກຄ້າຕ້ອງຮັບປະກັນເຂົ້າຖືກຕ້ອງຕາມທີ່ຢູ່ໜ້າເວບຂອງທະນາຄານລາວຫວຽດດ້ວຍວິທີຝົມເນື້ອໃນໂດຍກົງ www.LAOVIETBANK.com.la ຫຼື ebank.LAOVIETBANK.com.la ໃນທີ່ຢູ່ຂອງເວບບຣາວເຊີ. ຫຼັງຈາກນັ້ນ, ລູກຄ້າສາມາດເຂົ້າໃຊ້ບໍລິການທະນາຄານແບບອອນລາຍ, ເປີດໃຊ້ຂໍ້ມູນ ຫຼື ດາວໂຫລດ ບັນດາການນໍາໃຊ້ທີ່ເກີດຂຶ້ນໃນບັນດາໜ້າເວບນີ້. ລູກຄ້າບໍລິການເຂົ້າໃຊ້ໜ້າເວບບໍລິການທະນາຄານແບບອອນລາຍໃນບັນດາເສັ້ນທາງເຊື່ອມຕໍ່/ທີ່ຢູ່ທີ່ມີຢູ່ໃນ email ຫຼື ບັນດາໜ້າເວບ web ທີ່ບໍ່ແມ່ນຂອງທະນາຄານລາວຫວຽດ.
2. ເມື່ອລູກຄ້າເຮັດໂທລະສັບເສຍ, ປ່ຽນ sim ໂທລະສັບໃຫ້ແກ່ຜູ້ອື່ນ ຫຼື ໄດ້ຮັບຮູ້ວ່າມີລາຍການທີ່ຜິດປົກກະຕິທີ່ກ່ຽວຂ້ອງກັບບັນຊີ **ຈິ່ງແຈ້ງໄປຫາທະນາຄານທັນທີ** ຕາມໜຶ່ງໃນເບີໂທລະສັບ (856-21) 251-418 ຕໍ່ 800; 02052220222 ຫຼື ບັນດາຈຸດບໍລິການທະນາຄານລາວຫວຽດ ທີ່ໃກ້ທີ່ສຸດເພື່ອປ່ຽນຂໍ້ມູນຫຼືຢຸດ ບໍລິການທີ່ລູກຄ້າໄດ້ລົງທະບຽນກັບ ທະນາຄານທີ່ກ່ຽວຂ້ອງກັບເບີໂທລະສັບໄວ້ຊົ່ວຄາວ.

3. ລູກຄ້າຄວນຕິດຕັ້ງ, ປັບປຸງບັນດາໂປຣແກຣມຂ້າໄວຣັສເປັນປະຈຳ, ປ້ອງກັນການໂຈມຕີຂໍ້ມູນໃນຄອມພິວເຕີ/ອຸປະກອນເຂົ້າໃຊ້ໃນບັນດາບໍລິການທະນາຄານແບບອອນລາຍແລະອອກຈາກການເຂົ້າໃຊ້ທັນທີຫຼັງຈາກສໍາເລັດລາຍການ.
4. ບໍ່ຂຽນລະຫັດອອກໃສ່ເຈ້ຍ, ບໍ່ຕັ້ງລະຫັດທີ່ເດົາໄດ້ງ່າຍ ເຊັ່ນ: ຊື່, ວັນເດືອນປີເກີດ..., ໝັ້ນປ່ຽນລະຫັດເຂົ້າໃຊ້ບັນດາບໍລິການທະນາຄານແບບອອນລາຍ, email (ຕໍ່າສຸດແມ່ນ 3 ເດືອນ/ຄັ້ງ).
5. ລົງທຳບຽນນຳໃຊ້ບໍລິການຮັບຂໍ້ຄວາມແຈ້ງບັນດາຍອດເງິນໃນບັນຊີ, ລາຍການທຸລະກຳບັດ (LSMS) ເພື່ອເພີ່ມຄວາມປອດໄພແກ່ບັນຊີແລະບັດ.
6. ອ່ານ ແລະ ປະຕິບັດຖືກຕາມບັນດາຂໍ້ກຳນົດກ່ຽວກັບການແນະນຳດ້ານຄວາມປອດໄພຂອງທຸລະກຳເພື່ອຮັບປະກັນໃນການໃຊ້ງານບັນດາບໍລິການ ທະນາຄານແບບອອນລາຍຖືກວິທີ, ປອດໄພ, ເປັນ ຄວາມລັບ
7. ຕິດຕໍ່ ຫາທະນາຄານລາວຫວຽດ ທັນທີ (ຜ່ານໂທລະສັບ, email, facebook) ເພື່ອ ຍິ່ງຍືນຂໍ້ມູນຕົນເມື່ອໄດ້ຮັບໂທລະສັບແຈ້ງໄດ້ຮັບລາງວັນ, ມີລາຍການທີ່ໜ້າສົງໄສຈາກບັນຊີ ຫຼື ເພື່ອຮັບຄວາມຊ່ວຍເຫຼືອເມື່ອ ເກີດບໍ່ສະບາຍໃຈ, ຂ້ອງໃຈທີ່ຕ້ອງການແລກປ່ຽນຂໍ້ມູນກັບທາງທະນາຄານລາວຫວຽດ. ບັນດາຊ່ອງທາງ ຊ່ວຍເຫຼືອ ທີ່ແນ່ນອນຂອງທະນາຄານລາວຫວຽດ:

ຜ່ານບັນດາເບີໂທລະສັບ: (856-21) 251-418 ຕໍ່ 800, 02052220222

ຜ່ານ email: laovietbank247@laovietbank.com.la

III. ລັກສະນະການສໍ້ໂກງ

1. ໄດ້ຮັບສາຍໂທເຂົ້າ, ຂໍ້ຄວາມ, email, ຂໍ້ມູນໃນສັງຄົມອອນລາຍ ແຈ້ງວ່າໄດ້ຖືກລາງວັນ, ລົບກວນໃຫ້ຮັບເງິນຈາກຕ່າງປະເທດໂອນເຂົ້າມາ... ກັບການແນະນຳການຮັບລາງວັນດ້ວຍວິທີຂໍ້ລະຫັດ, ລະຫັດທີ່ໃຊ້ໄດ້ຄັ້ງດຽວ ຫຼື ເອີ້ນວ່າລະຫັດຍິ່ງຍືນທຸລະກຳ (OTP), ຫຼັງຈາກນັ້ນວິສາຊີບຈະນຳໃຊ້ OTP ແລະລະຫັດເພື່ອໂອນເງິນ.
2. ໄດ້ຮັບສາຍໂທເຂົ້າມາ, ຂໍ້ຄວາມ ທີ່ແອບອ້າງວ່າເປັນພະນັກງານ ທະນາຄານ ຫຼື ພະນັກງານກວດສອບໃນນັ້ນມີການຮຽກຮ້ອງໃຫ້ສະໜອງຂໍ້ມູນສ່ວນຕົວແລະບັນຊີທະນາຄານ, ຫຼື ສະໜອງຂໍ້ມູນກ່ຽວ ກັບການຮັບຜິດຊອບ, ຂໍ້ມູນໃດໆ.
3. ໄດ້ຮັບ ສາຍໂທເຂົ້າມາ, ຂໍ້ຄວາມ ທີ່ແອບອ້າງວ່າເປັນໝູ່ເພື່ອນ, ຄົນສະໜິດ, ຍາດຜົນໜ້ອງທີ່ບໍ່ໄດ້ພົບກັນດົນ ທີ່ກຳລັງຫຍຸ້ງຍາກມາຂໍຄວາມຊ່ວຍເຫຼືອດ້ວຍການໃຫ້ຊື້ຊຸດເຕີມເງິນ, ໂອນເງິນເຂົ້າໃນບັນຊີໃຫ້ຕາມແລກ ບັນຊີທີ່ເຂົາໄດ້ເອົາໃຫ້.