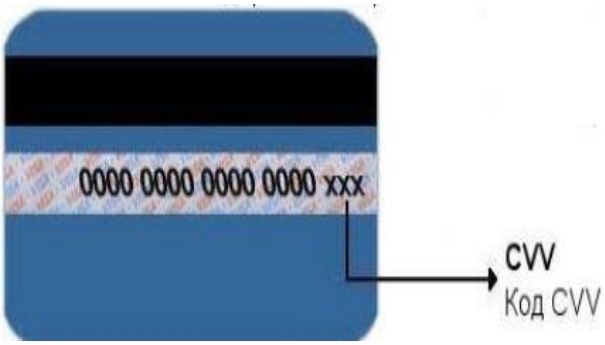
Банктык карт аркылуу интернет операцияларын жүргүзүүдө (сатып алуулар) айрыкча көңүл бурулууга тийиш болгон коопсуздук чаралары



• Интернет, телефон/факс, почта аркылуу товарлар/кызмат көрсөтүүлөр үчүн нак эмес төлөө учурунда кардарлардан CVV2 (үч сандан турган коопсуздук коду) көрсөтүү талап кылынышы ыктымал. Ал карттын арткы бетинде жайгашкан (кол коюу үчүн каралган тилкедеги акыркы үч сан же оң жактагы атайы тилкеде жайгаштырылышы мүмкүн) жана кардарды кошумча текшерүүдөн өткөрүү үчүн кызмат кылат.

• Интернет, телефон/факс, почта аркылуу товарлар/кызмат көрсөтүүлөр үчүн нак эмес төлөө учурунда кардарлардан CVV2 (үч сандан турган коопсуздук коду) көрсөтүү талап кылынышы ыктымал. Ал карттын арткы бетинде жайгашкан (кол коюу үчүн каралган тилкедеги акыркы үч сан же оң жактагы атайы тилкеде жайгаштырылышы мүмкүн) жана кардарды кошумча текшерүүдөн өткөрүү үчүн кызмат кылат.

• Интернет дүкөндөрүндө операцияны ишке ашырууда ошол дүкөн кардарга тиешелүү маалыматтардын купуялуулугунун сакталышы жана коргоого алынышы боюнча ачык милдеттенмени алгандыгын, төлөм системасында сертификациялангандыгын жана сайтында ага байланышуу үчүн маалыматтар бардыгын контролдоп, сайтта көрсөтүлгөн дарегинин жана телефон номерлеринин так экендигине толук ынанып алуу зарыл. Талап кылынган маалыматтар HTTPS-протоколун колдонуу менен коргоого алынган каналдар аркылуу өткөрүлүүгө тийиш.

• Web-сайт алдамчылар тарабынан купуя маалыматтарды алуу максатында да колдонулуп (товарлар/кызмат көрсөтүүлөргө буюрутма берүүдө кардарларга электрондук форманы толтуруп, анда ПИН-кодду кошо алганда, банк эсептеринин, карт реквизиттерин көрсөтүү талап кылынышы мүмкүн), кеңири белгилүү Интернет – дүкөндүн окшош сайттары, «бир күндүк дүкөн" сайттары, деги эле жок уюмдардын атынан иш алып барган сайттар сыяктуу маалымат алууда алдамчыларга жол ачкан ыкмалар кездешип жаткандыгына айрыкча көңүл бурууну өтүнөбүз.

• Интернет түйүнү аркылуу операция жүргүзүүдө жана карт боюнча маалыматтарды сунуштоодо этият болууга чакырабыз.

• «SMS билдирүү» кызмат көрсөтүүсүнө милдеттүү түрдө туташууну сунуштайбыз. Анткени, өзүнөр ишке ашырбаган операция тууралуу SMS-билдирүү алган шартта картка дароо бөгөт койдуруу талап кылынат. Кардар Интернет операцияларын кошо алганда, карт реквизиттерин пайдалануу менен ишке ашырылган бардык операциялар, ошондой эле кардар эсебинен алынган бардык суммалар үчүн өзү жооп берет. Алдамчылыкка жол ачкан сайттар аркылуу ишке ашырылган транзакциялар үчүн Банк жоопкерчиликтүү эмес.

Зарылчылык келип чыккан учурларда **0(312) 61 00 61** телефон номери боюнча банктын колл-борборуна, ошондой эле “Банктар аралык процессинг борбору” ЖАКка **0(312) 66 43 25, 66 50 83** телефондору жана **fraud@bakai.kg** электрондук дарегине кайрылып, картка дароо бөгөт койдуруу зарыл экендигин эскертебиз.