Рекомендации
клиентам ООО БАНК «КУРГАН» по безопасности при использовании удаленных каналов обслуживания для осуществления финансовых операций

ООО БАНК «КУРГАН» обращает внимание своих клиентов на возможные риски, связанные с получением несанкционированного доступа к защищаемой информации клиента:

осуществление банковских операций лицами, не обладающими правом их осуществления;

получение доступа к конфиденциальной информации клиента: персональным данным, состоянию счетов и др.;

разглашение конфиденциальной информации клиента;

изменение регистрационных данных клиента;

иные действий, совершенных без воли клиента, и направленных против его интересов.

Никогда не сообщайте посторонним лицам информацию, использование которой может привести к совершению перевода денежных средств без согласия их владельца, например, номер карты, срок ее действия, коды CVV/CVC, ПИН, логин (идентификатор пользователя), пароли, контрольную информацию, предназначенную для доступа и подтверждения операций в удаленных каналах обслуживания и т.д.).

В случае утраты (потери, хищения) устройства, с использованием которого осуществлялись финансовые операции, утраты (потери, хищения) логина и пароля, незамедлительно обратитесь в свой банк для осуществления процедуры по блокировке доступа к сервису или замены пароля.

Принимайте меры по контролю конфигурации устройства, с использованием которого осуществляются финансовые операции:

используйте лицензированное специализированное программное обеспечение (в том числе антивирусное и аналогичное), контролирующее (затрудняющее) внесение изменений в конфигурацию устройства;

периодически контролируйте журналы событий антивирусного и иного специализированного программного обеспечения, системные журналы, перечень установленных программ и запущенных процессов, перечень новых устройств.

Не используйте права администратора, позволяющие вносить изменения в конфигурацию устройства, без необходимости.

Старайтесь исключить возможность бесконтрольного доступа третьих лиц (гостей, коллег, знакомых) к вашему компьютеру или мобильному устройству, с использованием которого осуществляются финансовые операции.

Своевременно осуществляйте обновление операционной системы, а также всего программного обеспечения, повышающего безопасность.

Используйте в работе на устройствах только лицензионное программное обеспечение.

Используйте функцию предварительной авторизации на устройствах и блокировки экрана устройства при отсутствии активности.

Принимайте меры по своевременному обнаружению воздействия вредоносного кода:

используйте на устройстве лицензионные средства антивирусной защиты;

по возможности производите антивирусную проверку любой информации, получаемой из сети Интернет или на съемных носителях.

Не запускайте на своем устройстве программы и не скачивайте файлы, полученные из источников, не заслуживающих доверия.

Избегайте сайтов, которые могут иметь незаконное и/или вредоносное содержание.

В случае обнаружения средствами антивирусной защиты вредоносного кода, приостановите финансовые операции, осуществив выход из сервиса, проконтролируйте отсутствие несанкционированных действий, по возможности проведите дополнительную проверку на предмет устранения проблем, при необходимости обратитесь в свой банк для осуществления процедуры по блокировке доступа к сервису или замены пароля.