Рекомендации по защите информации, информация о возможных рисках несанкционированного доступа к защищаемой информации, а также информация о мерах по предотвращению несанкционированного доступа к защищаемой информации

В целях защиты информации от воздействия программных кодов, приводящего к нарушению штатного функционирования устройств и оборудования, а также в рамках информирования о мерах по предотвращению несанкционированного доступа к защищаемой информации ООО УК «АДЕПТА» (далее – Управляющая компания) ***рекомендует следующее:***

- Всегда используйте актуальное программное обеспечение проверенных производителей для защиты Ваших персональных устройств (PC, планшет, мобильное устройство), от «вирусов» и иных вредоносных программ.
- Используйте на Ваших персональных устройствах только лицензионное ПО, не устанавливайте ПО, полученное из сомнительных источников.
- ***Не открывайте вложения в почтовые письма, полученные от неизвестных Вам отправителей***. Если отправитель Вам известен – в любом случае рекомендуется проверить полученный файл антивирусной системой.
- Не посещайте сайты сомнительного содержания.
- Не проводите конфиденциальные транзакции с использованием недоверенного общедоступного Wi-Fi.
- Оформите отдельную сим-карту для работы с мобильным банком и никому не сообщайте в публичном пространстве этот мобильный номер. Современные устройства связи поддерживают несколько сим-карт одновременно.
- Вы вправе написать заявление в салоне сотовой связи, запрещающее перевыпуск сим-карты без Вашего личного участия. При этом, Вы можете указать строго определенное отделение, в котором можно лично получить сим-карту.
- ***Никогда и никому не сообщайте свои конфиденциальные данные, в том числе, но не ограничиваясь, логины, пароли, коды, ПИН-коды, CVV/ CVC-коды, данные электронной подписи и пр***. Сотрудники финансовых организаций (в т.ч. – Управляющей компании) никогда не требуют указанную информацию.
- Внимательно следите за смс о блокировке сим-карт или перевыпуске.
- В случае сомнений перезванивайте лично в Управляющую компанию или банк по номеру, который указан на официальном сайте или на обратной стороне Вашей банковской карты (для банков). Игнорируйте сообщения о необходимости перезвонить в Управляющую компанию или банк по указанному в сообщении номеру. Так как существуют мошеннические сервисы подмены номеров, звоните в Управляющую компанию или банк самостоятельно.
- ***Не выкладывайте фотографии и сканы Ваших документов в соц.сети и/или иные общедоступные ресурсы*** (например, паспорт, электронные билеты, чеки за оказанные услуги и т.п.): дополнительная информация только помогает мошенникам.
- Будьте особенно бдительны и осторожны, если люди, представляющиеся сотрудниками Управляющей компании, иных финансовых организаций и (или) банков требуют от Вас каких-либо быстрых действий, пытаются напугать, т.к. это распространенные приемы мошенников.
- ***Не передавайте Ваш мобильный телефон и (или) другие устройства третьим лицам***, т.к. они могут установить на него ПО, содержащее вредоносный код, а в случае кражи или утраты злоумышленники могут воспользоваться Вашим устройством для совершения противоправных / мошеннических действий. В связи с этим при утрате, краже мобильного устройства максимально оперативно заблокируйте сим-карту.

Управляющая компания информирует о следующих возможных рисках несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления:

- риски разглашения конфиденциальной информации, персональных данных (например, информации об активах, персональной информации и пр.);
- риски совершения финансовых операций с активами клиента третьими лицами, не обладающими правом их осуществления, а также совершение ими иных действий (например, внесение изменений в регистрационные данные клиента, изменение параметров услуг и пр.);
- риски вредоносного воздействия на устройства и оборудование.

При любом подозрении на мошенничество незамедлительно обратитесь в Управляющую компанию!