

СОВЕТЫ ПО БЕЗОПАСНОСТИ

- никогда, никому и ни при каких обстоятельствах не сообщайте реквизиты своих банковских счетов и банковских карт, в том числе лицам, представившимся сотрудниками банка или правоохранительных органов;

- не следует сообщать в телефонных разговорах и при общении в соцсетях полный номер карточки, срок ее действия, код CVC/CVV (находящиеся на обратной стороне карты), логин и пароль к интернет-банкингу, паспортные данные, кодовое слово (цифровой код) из SMS-сообщений;

- в случае поступления звонка «от сотрудника банка» необходимо уточнить его фамилию, номер телефона, после чего завершить разговор и самим позвонить в банк или в круглосуточную службу сервиса, номер которой написан на оборотной стороне платежной карты. Сообщите о случившемся. Скорее всего, никаких несанкционированных операций не было, и никто из банка не звонил;

- в случае поступления звонка «от попавшего в ДТП родственника» либо «сотрудника милиции» необходимо уточнить его фамилию, номер телефона, после чего завершить разговор и самим позвонить данному, либо иному родственнику либо иному другому лицу у которому можно перепроверить информацию. Далее, незамедлительно сообщить о данном факте в милицию и ни в коем случае не передавать никому денежных средств;

- в том случае, если с использованием Вашего счета и правда кто-то будет пытаться совершить несанкционированные операции и банк это заметит, то его сотрудники сперва инициативно заблокируют банковскую платежную карту, затем сообщат Вам причину принятого решения (ничего не уточняя) и пригласят посетить банк с паспортом для получения наличных денежных средств и написания заявления на перевыпуск карты;

- ни в коем случае не предоставляйте доступ к мобильному устройству посторонним лицам! Никогда не устанавливайте по просьбам незнакомых лиц программы удаленного доступа, такие, например, как «AnyDesk», «TeamViewer» и др. Не сообщайте незнакомым лицам сеансовые коды! Через эти приложения мошенники могут получить доступ к мобильному приложению интернет банкинга на Вашем устройстве и совершить хищение денежных средств. Учтите: сотрудники банков никогда не используют для связи с клиентами мессенджеры («Viber», «Telegram», «WhatsApp»);

- в настоящее время просто необходимо наличие второй банковской платежной карты, не привязанной к основному банковскому , счету (например, зарплатному). Этой картой рассчитывайтесь в сети Интернет, заранее пополняя ее на необходимую сумму. В таком случае Вы сможете обезопасить свой основной банковский счет. Многие банки предлагают своим клиентам услугу выпуска «виртуальной карты». Процесс ее открытия не требует посещения клиентом банка и представляет собой достаточно быстрый процесс. В итоге Вы станете обладателем электронного аналога банковской карты, посредством которой сможете рассчитываться за услуги в сети Интернет без риска скомпрометировать основной банковский счет. Просто перед оплатой пополните ее необходимой суммой с основной карты - и никаких проблем!;

- каждый владелец банковских платежных карт может настроить собственный алгоритм безопасности при их использовании. Для обеспечения сохранности денежных средств, размещенных на банковских счетах, каждый держатель карточки посредством систем дистанционного банковского обслуживания может установить индивидуальные ограничения (лимиты/запреты). Среди основных - следующие: подключение технологии 3D-Secure (обязательное подтверждение операций, совершаемых держателями карточек с применением их реквизитов в сети Интернет); установление, банком-эмитентом ограничение на проведение расходных операций (максимальная сумма и количество операций в определенный период времени); возможность самостоятельно устанавливать ограничения (на проведение операций в сети Интернет, на совершение операций в конкретной стране, на совершение отдельных видов операций);

- для доступа к системам дистанционного банковского обслуживания и личным аккаунтам необходимо использовать сложные пароли, исключающие возможность их подбора. Рекомендуется составлять комбинации паролей не менее чем из 12 знаков (цифры, буквы и символы в разном регистре). Создавайте уникальные пароли для каждого сервиса в отдельности. Стоит воздержаться от паролей, составленных из дат рождения, имен, фамилий - то есть тех, которые легко вычислить из общедоступных источников информации (например, тех же социальных сетей). Также следует регулярно менять пароли, чем чаще - тем лучше. Пользуйтесь только проверенным менеджерам паролей!;

- при поступлении в социальных сетях сообщений от лиц, состоящих в категории «друзья», с просьбами о предоставлении реквизитов банковских платежных карточек - не следует сразу же отвечать на подобные сообщения! Нередко такие просьбы рассылаются от имени друзей преступниками, взломавшими аккаунт в социальной сети и получившими доступ к конфиденциальной переписке. Поэтому сначала необходимо связаться с этим человеком (по телефону, лично встретиться) и уточнить, действительно ли он нуждается в помощи;

- в целях защиты устройств необходимо использовать лицензионное программное обеспечение, регулярно обновлять программное обеспечение и операционную систему. Установить антивирусную программу следует не только на персональный компьютер, но и на смартфон, планшет и регулярно обновлять ее.

Обучите своих родных и близких этим простым правилам !