**Как обезопасить себя от мошенников**

- Никогда и никому, ни при каких обстоятельствах нельзя передавать такие конфиденциальные данные, как логин, пароль или реквизиты вашей банковской карты (секретный код безопасности CVV2, подтверждающий подлинность карты, имя ее владельца, срок действия) и, разумеется, ПИН-код.

- Выучите ПИН-код наизусть или запишите его на листочек, но храните отдельно от карты.

- Не используйте так называемые зарплатные карты для расчетов в магазинах и оплаты интернет-покупок. Деньги с карточного счета лучше переводить на лицевой либо устанавливать суточные лимиты на все виды совершаемых операций.

- Выбирайте банкоматы, расположенные внутри офисов банков или в охраняемых точках, оборудованных системами видеонаблюдения.

- Не пользуйтесь подозрительными моделями банкоматов. Прежде чем вставить карту в терминал, внимательно осмотрите его (нет ли чего-нибудь подозрительного на клавиатуре или в картоприемнике).

- Не стесняйтесь закрывать клавиатуру рукой. При возникновении проблем не пользуйтесь советами "случайных помощников" - сразу звоните в банк и блокируйте карту. Если карта осталась в банкомате и вы не знаете телефон своего банка, позвоните в компанию, осуществляющую техническое обслуживание банкомата. Номер должен быть указан на терминале.

- Если вы потеряли карту или у вас есть основания полагать, что третьи лица узнали ее реквизиты, обратитесь в банк и заблокируйте ее.

- Всегда с подозрением относитесь к сообщениям, в которых вас просят перейти по какой-то ссылке (проверьте, нет ли этой страницы в списке подозрительных). Да и в принципе безопаснее будет вручную ввести ссылку на уже проверенный сайт в строке браузера, чем переходить по ссылке из сообщения.

- Если вас просят заново авторизоваться, обязательно проверяйте адресную строку - на том ли вы сайте находитесь.

- Старайтесь пользоваться последними версиями программного обеспечения, установленными на вашем компьютере или планшете.

- Прежде чем ввести логин и пароль, проверьте, защищено ли соединение. Если перед адресом сайта стоит "https", все в порядке.

- Если сомневаетесь в письме, проверьте его источник.

- Помните, что даже если письмо или сообщение со ссылкой вы получили от лучшего друга, расслабляться нельзя - его тоже могли обмануть. Поэтому ведите себя не менее осторожно, чем при обращении со ссылками, пришедшими из неизвестного источника.

- По возможности не заходите в онлайн-банки и другие подобные сервисы через открытые Wi-Fi-сети в кафе или на улице (за таким Wi-Fi могут стоять мошенники, подменяющие адрес сайта на уровне подключения и перенаправляющие вас на поддельную страницу).

- Заходить в интернет-банк с чужих компьютеров тоже не рекомендуется. Если это все же случилось, по завершении сессии нажмите "Выход" и очистите кэш-память.

- Пользуйтесь антивирусами и своевременно обновляйте их.

- Обнаружив фишинговую операцию, обязательно сообщите о ней в банк (если письмо пришло от имени финансового учреждения) или в службу поддержки социальной сети (если такие ссылки рассылает кто-то из пользователей).

- Без необходимости не вводите никакие свои персональные данные, помимо логина и пароля.

- Придумайте сложный пароль для входа в личный кабинет, а также используйте одноразовые пароли, запрашиваемые банками для подтверждения действий в личном кабинете.

- Не забывайте, что банки не рассылают сообщений о блокировке карт, а в телефонном разговоре не выспрашивают конфиденциальные сведения и коды, связанные с картами клиентов.

- Чтобы уберечь SIM-карту, к которой привязана карта, оперативно уведомляйте банк при получении подозрительных сообщений и ни в коем случае не звоните по указанным в них номерам. Проинформируйте банк, если сменили номер или потеряли SIM-карту. Установите пароль на телефон и не снимайте блок с экрана, если кто-то посторонний наблюдает за вашими действиями. А если SIM-карта оформлена на вас лично, запретите ее замену по доверенности.

- Делая покупки в интернет-магазинах, предварительно узнайте, с кем имеете дело. Попробуйте найти физический адрес продавца (не абонентский ящик) и его телефон. Поищите отзывы в Интернете. Если люди пишут о неприятном опыте с такими магазинами, вам придется решить, стоит ли рисковать.

- Следите за своими банковскими отчетами и отчетами по кредиткам на предмет списаний с вашей карты, которых вы не узнаете или которые подозрительно выглядят. Позвоните своему банку, эмитенту карты или кредитору, если найдете транзакции, которых вы не совершали.

- Если кто-то связывается с вами с предложением малорискованных и высокоприбыльных инвестиций, воздержитесь. Такие мошенники обычно настаивают на немедленном вложении денег, гарантируют высокие прибыли, обещают низкий или вообще отсутствующий финансовый риск или требуют, чтобы вы срочно выслали наличные.

- Если вы собираетесь делать покупку онлайн, лучше совершать ее, используя кредитную карту с высокой степенью защиты.

- Не отвечайте на сообщения с просьбами предоставить личную или финансовую информацию.

- Не верьте сообщениям, которые рекламируют ваши высокие шансы выиграть в иностранную лотерею или сообщают, что вы уже выиграли. Мошенники будут утверждать, что нужно отправить деньги на оплату "налогов", "сборов" или "таможенных платежей", прежде чем выслать вам ваш выигрыш. Если вы отправите деньги, вы их потеряете.

- Имейте в виду: фальшивые письма и фальшивые сайты могут во всем повторять дизайн настоящих (качество подделки зависит от того, насколько хорошо мошенники знают свою работу), но гиперссылки, скорее всего, будут неправильные - или с ошибками, или вообще будут отсылать не туда. По этим признакам можно отличить фишинговое письмо от настоящего.