КАК ЗАЩИТИТЬ СЕБЯ ОТ МАШЕННИКОВ ПРИ ИСПОЛЬЗОВАНИИ БАНКОВСКОЙ КАРТЫ

Год за годом мошенничеств становится больше. Значительно больше. Так, в 2020 году злоумышленники дистанционно похитили у жителей Приангарья свыше **400 миллионов рублей.** Каждое пятое преступление в регионе – совершается при помощи современных технологий. Через интернет, с использованием компьютера или мобильного телефона, с банковских счетов. Каких-то 20 лет назад таких преступлений не существовало вовсе – они появились вместе с доступностью глобальной сети и ростом числа безналичных операций. Каждый день в полицию в нашем регионе поступает от 3 до 15 сообщений о преступлениях подобного рода.

Обмануть могут любого. В год мошенники обманывают несколько тысяч жителей Иркутской области. Возраст пострадавших от 12 до 90 лет. Это люди самого разного социального статуса и рода занятий: пенсионеры и бизнесмены, студенты и их преподаватели, предприниматели и домохозяйки, рабочие и госслужащие... Имеются факты, когда один и тот же человек становился жертвой мошенника трижды.

Злоумышленники готовятся к своим аферам: они могут обратиться к вам по имени и отчеству, назвать ваш возраст или другие данные – это располагает к себе, а в современном мире заполучить такие сведения не сложно. Их речь может имитировать манеру общения тех людей, за кого мошенник себя выдает. В диалоге они создают ситуацию, в которой действовать нужно здесь и сейчас.

Жертвами мошенников становятся не глупые люди, жертвами мошенников становятся люди, подверженные влиянию. А все мы без исключения в той или иной степени подвержены влиянию **и любой из нас потенциально может стать жертвой мошенника.**

Основные намерения мошенника: под любым предлогом уговорить вас перевести ему ваши деньги, либо предоставить ему доступ к сбережениям: картам, счетам, онлайн-кабинету банка и т.д.

Аферисты постоянно совершенствуют способы обмана и придумывают новые. Но наиболее распространенными остаются **три типовых схемы**:

1. Получение предоплаты либо доступа к счету гражданина при купле-продаже товаров (услуг) в сети Интернет;
2. Звонки или СМС-сообщения от «службы безопасности банка»;
3. Сообщения либо звонки о происшествиях с родственниками, плохих медицинских анализах, компенсациях за различные покупки (услуги), дополнительных выплатах, выигрыши в лотерею и т.д.

Как предотвратить:

1. **Не отправлять задаток незнакомым людям.** У вас никогда не будет возможности проверить, существует ли выставленный в интернет-объявлении товар в реальности и насколько честен его продавец. **Покупателям можно сообщать только номер карты или номер телефона** – этого достаточно, чтобы совершить перевод. Все остальные данные нужны только мошенникам.
2. При поступлении подозрительных СМС от имени банка **не перезванивать по указанным в нем номерам**. Если вам позвонили «работники банка» и просят назвать данные вашей карты, совершить действия со счетом, терминалом, в «личном кабинете» на сайте банка, или установить программу на свое устройство – **не продолжайте разговор.** Даже если телефон показывает, что звонок происходит с телефона горячей линии банка - технически замаскировать любой номер для злоумышленников не составляет большого труда. **Повесьте трубку и вручную наберите номер банка, указанную на оборотной стороне карты.**
3. Критически относитесь к сообщениям о любом внезапном выигрыше или якобы положенной выплате. Скорее всего, это «наживка», пообещав которую мошенники постараются заполучить ваши деньги.

Помните, **пока вы ничего не предпринимаете - вы защищены.** Не принимайте поспешных решений. Перед любым действием советуйтесь с близкими для вас людьми – возможно они отговорят вас от рискованного поступка.

Если с вашей банковской карты вдруг списали деньги:

– Как можно скорее позвоните в банк (номер есть на обороте карты), сообщите о мошеннической операции и заблокируйте карту.

– Обратитесь в отделение банка и попросите выписку по счету. Напишите заявление о несогласии с операцией. Сохраните экземпляр заявления с отметкой банка о приеме.

– Обратитесь в правоохранительные органы с заявлением о хищении.

20 Правил безопасного использования банковских карт

1. Обязательно подключите банковскую систему **смс-оповещения** обо всех операциях и/или систему **push-уведомлений** через онлайн- приложение вашего банка. В случае любой информации об операции (даже самой мелкой), которую вы не совершали, которую не инициировали, сообщите в службу поддержки банка по телефону, указанному на карте.
2. **Запишите телефон службы поддержки банка** в записную книжку вашего мобильного телефона, а также на всякий случай

на бумаге и положите в доступное для вас место, а также в кошелёк. В случае пропажи карты это поможет вам незамедлительно заблокировать карту и, тем самым, сохранить свои деньги в безопасности.

3. **Проверяйте состояние счета после любых операций с картой.** Если остаток на счете не совпадает с вашими ожиданиями, внимательно просмотрите все последние смс-сообщения от банка о ваших транзакциях. Вы также можете запросить в банкомате, через мобильный, интернет-банк или в банковском офисе выписку по последним операциям. Проверьте обоснованность всех операций.
4. **Запомните телефоны и электронные адреса банка,** с которых вам поступает информация от банка. В случае получения информации от имени банка с других номеров, не отвечайте на них, обратитесь по известным вам контактам с тем, чтобы поверить, действительно ли к вам обращался банк.
5. Для ограничения недобросовестных звонков используйте сервис вашего банка **по блокированию мошеннических звонков. Внимание,** такой сервис может быть платным.
6. Не стыдитесь **прикрывать** рукой, газетой, сумкой и т. п. руку, которой вы набираете ПИН-код. Дополнительная безопасность не будет лишней. Это подчеркнёт вашу компетентность в вопросах безопасности, что вызовет уважение у близких и коллег.
7. Помните, что **ПИН-код** понадобится только для совершения операций в банкоматах, платежных терминалах и при оплате товаров в магазинах службах сервиса для подтверждения транзакции.

   Передача своего ПИН-кода по запросам в интернете, звонкам незнакомых и даже знакомым людям не допустима. ПИН-код не должны знать и сотрудники вашего банка.
8. **Не оставляйте свою банковскую карту без присмотра** и не позволяйте в магазинах и ресторанах ее уносить. Она всегда должна находиться в зоне полного контроля.
9. Помните, что имя, фамилия, номер карты, срок ее действия, а также номер cvv2/cvc2, который указан на обороте карты, являются важными элементами идентификации владельца. **Не позволяйте чужим людям переписывать** содержащуюся на карте информацию или фотографировать карту.
10. При оформлении карты многие банки предлагают указать **контрольное слово или секретный вопрос,** которое

впоследствии может использоваться сотрудниками банка для подтверждения того, что по телефону с банком общаетесь именно вы. Введение такой системы безопасности разумно. Знание в экстренных ситуациях позволит вам быстрее идентифицировать себя по телефону.

11. При покупках на сайтах и в интернете введите подтверждение в виде **дополнительного уведомления или по смс,** а также **максимальный лимит** по одной транзакции.
12. **Старайтесь не носить с собой банковские карты,** которые вы в настоящее время не используете. Если вы не собираетесь использовать карту, то лучше обратиться в банк с просьбой закрыть счет лишней карты.
13. Если вы часто пользуетесь картой для приобретения товаров и услуг через интернет, рекомендуем в**ыпустить для этих целей дебетовую карту** или кредитную карту с небольшим лимитом.
14. Совершайте покупки в интернете только на хорошо знакомых сайтах, в проверенных интернет-магазинах.
15. Обращайте внимание на **первые буквы в адресе интернет магазина.** Он должен начинаться с названия протокола **htpps.** Если вам предлагают совершить покупку с сайта с протоколом htpp, этот протокол не предназначен для расчетов и хранения персональной информации, поэтому следует отказаться от указанных действий на таких сайтах.
16. **Не стремитесь к бесконечному увеличению лимита** по кредитной карте. Лимит должен соответствовать вашим реальным потребностям. Для дебетовых карт рекомендуем установить лимиты ежедневных операций, которые соответствуют вашим жизненным потребностям.
17. Старайтесь пользоваться банкоматами, расположенными в банках, в солидных торговых центрах, гостиницах, где **обеспечивается контроль за устройством.**
18. **Не пользуйтесь чужими гаджетами и компьютерами** для совершения операций с банковской картой.
19. **Регулярно обновляйте антивирусные программы** на компьютерах, планшетах и смартфонах, через которые вы совершаете операции с банковскими картами.
20. Для лучшей подготовки к возможной экстренной ситуации **проведите необходимую самостоятельную подготовку** с учётом особенностей вашей жизни на реагирование на мошенническую угрозу.