БАРАБИНСКАЯ МЕЖРАЙОННАЯ ПРОКУРАТУРА

**Памятка гражданам как не стать жертвой мошенничества с банковскими картами**

Существенным фактором, оказывающим влияние на криминогенную обстановку, продолжает оставаться рост ИТ-преступлений, или преступлений, связанных с использованием информационных технологий. Основную часть преступлений в ИТ-сфере составляют мошенничества, в том числе с банковскими картами.

По причине специфики механизма совершения, данные преступления относятся к категории трудно раскрываемых.  Потерпевшим может стать любой человек, имеющий банковский счет, привязанный к банковской карте и потерявший бдительность или внимательность, а преступное деяние может совершить любое лицо, имеющее необходимые навыки работы. Мошенники втираются в доверие к простодушным гражданам, представляются сотрудниками банков или правоохранительных органов, обещают лёгкую прибыль, получают необходимые сведения, после чего совершают хищение денежных средств со счета потерпевшего.

Не смотря на то, что в средствах массовой информации постоянно размещаются сведения о способах совершения мошеннических действий, случаи обмана доверчивых граждан продолжают иметь место. Тем не менее, защититься от подобного обмана вполне реально, проявляя бдительность и адекватно оценивая ситуацию.

Общими признаками, которые должны как минимум насторожить и заставить внимательнее проанализировать полученный звонок или сообщение, являются:

- неизвестный, скрытый, незнакомый номер, с которого происходит звонок или прислано сообщение;

- особая манера общения, так как главное оружие телефонных мошенников – внезапность. Часто нагнетают обстановку обилием в лексиконе слов «срочно», «быстро», «немедленно, «потом объясню», «нужно быстрее». Их целью является застать человека врасплох, не дать времени на обдумывание, не позволить сомневаться. Во время звонка мошенник, ведет себя всегда уверенно, может давить, настаивать или, наоборот, любым способом пытаться расположить к себе абонента, чтобы выманить информацию;

- следующее отличие в том, что нет четких, прямых ответов на ваши вопросы;

- внимание должно активизироваться при поступлении просьбы или даже требования сообщить какую-то секретную персональную информацию или личные данные (номер и ПИН-код банковской карты, персональные сведения, пароли на сайте и пр.);

- осторожность необходимо проявить при получении известия о победе в конкурсе (тем более, если никогда и нигде не участвовали), призы, выгодные предложения, подарки, за которые нужно «доплатить» «внести залог» или еще каким-либо образом перечислить денежную сумму – это один из многих признаков телефонного мошенничества.

Наиболее распространёнными видами мошенничеств являются:

**«Объявления…»**

Приобретая и размещая товары и услуги через сайты бесплатных объявлений:

- не вносите какие-либо предоплаты за товар, чтобы для Вас его зарезервировали и не продали другому лицу, за возможное трудоустройство, а также в качестве аванса за сдачу жилья в наем;

- оплачивайте товар только при личной встрече и после его проверки;

- никому и никогда не сообщайте свои персональные данные банковской карты;

- обязательно проверяйте всю информацию, полученную посредством сети Интернет.

Заподозрить мошенника можно, если:

- потенциальный покупатель звонит из другого региона;

- человек соглашается купить товар не глядя;

- покупатель не соглашается на другие оплаты, кроме электронного платежа;

- покупатель не готов встречаться лично, не говорит адрес доставки товара и прочие данные;

- продавец предлагает вам копии своих документов (паспорт, водительское удостоверение, ИНН) в качестве подтверждения его личности, а в некоторых случаях предлагают оставить оригинал документа. Предоставление копий и оригиналов документов не дают никаких гарантий и к тому же они могут оказаться поддельными.

При заказе через сайт билетов, выбирайте авиа и ж/д компании, положительно зарекомендовавшие себя на рынке. Не переводите деньги за билеты на электронные кошельки или зарубежные сайты. При возникновении подозрений, обратитесь к представителю компании. Никогда не пользуйтесь услугами не проверенных и неизвестных сайтов по продаже билетов.

**«Подозрительные смс…»**

Никогда не переводите никому никаких денег. Отправитель может сам легко вернуть свои деньги. В случае, если вам на телефон приходит сообщение на подобие: «на ваш счет зачислено 30 000 рублей. С уважением, Ваш банк», а через несколько минут перезванивают и говорят, что ошиблись и случайно зачислили на вашу карту деньги, просят вернуть их обратно.

Предложите звонящему, обратиться в свой банк и решить вопрос самостоятельно, так как отправитель может сам очень легко вернуть свои деньги через банк.

**«Звонок из банка…»**

Настоящий сотрудник банка никогда не будет спрашивать у вас сведения о ПИН-коде, номере карты и ваши анкетные данные. Все эти сведения сотрудник банка видит на экране своего монитора, так как ранее Вы сами их предоставили при личном посещении отделения банка. Спрашивать эти сведения повторно, тем более по телефону, сотрудникам банка запрещено, а другим лицам, не являющимся сотрудниками банка, эти сведения не должны быть известны. В случае, если же какая-либо проблема действительно возникнет, настоящим сотрудником банка вам будет рекомендовано обратиться в ближайшее отделения банка лично, для решения всех вопросов. Если у вас возникли сомнения, задайте ему простые вопросы. Например, спросите у звонящего, какой у вас остаток на карте. Настоящий сотрудник банка увидит эти сведения у себя на экране, мошенник же не сможет ответить на этот вопрос и постарается убедить вас, что у него нет доступа к этой информации.

**«Социальные работники …»**

Незнакомец представляется соцработником и сообщает о надбавке к пенсии, перерасчете квартплаты, премии ветеранам, срочном обмене денег на дому, якобы «только для пенсионеров». Не верьте,  это мошенник!

Без официального объявления в нашей стране не может проводиться никакой «срочный обмен денег»!

**«ВКонтакте» (взлом страниц)**

Со страницы друзей, знакомых, родственников начинают приходить сообщения с просьбой одолжить денег на неотложные нужды. Преступники, взломав страницу в социальной сети, не гнушаясь ничем, от имени владельца страницы, сообщают о потере близкого родственника, либо о тяжёлой болезни, которые требуют больших финансовых затрат. Просят перевести денежные средства на счет банковской карты, при этом пользуясь современными технологиями, отправляют фотографию банковской карты с анкетными данными владельца страницы, которую взломали. Перед тем как начать рассылку сообщений, мошенники изучают информацию, имеющуюся на взломанной странице в социальной сети, изучают круг общения, просматривают фотографии «друзей». Данной информацией они пользуются при рассылке сообщений, чтобы их просьба выглядела более убедительно и правдоподобно.

Как реагировать на попытки обмана.

- получая тревожные звонки или сообщения, главное – постараться успокоиться и не принимать решения сразу. Лучше сразу сказать звонящему, что вам необходимо время, чтобы все обдумать, не принимайте поспешных решений, о которых вы потом будете жалеть;

- никогда и никому ни при каких обстоятельствах не сообщайте свои персональные данные или конфиденциальную информацию, например, ПИН-код банковской карты, номер счета, логин и пароль от страниц в социальных сетях, на интернет-сайтах и т.д.;

- задавайте вопросы. Если звонящий представляется как сотрудник полиции, банка, доктор поликлиники, страховой агент, первое, что нужно сделать, попытаться узнать как можно больше информации о собеседнике. Простые вопросы, например, фамилия и должность звонящего, из какого отделения полиции, банка или страхового агентства звонят, контактные данные руководителя организации, как найти официальный сайт и прочее, настоящего сотрудника не смутят, а мошенников заставят занервничать и сделать ошибку в алгоритме действий по обработке клиента;

- прежде чем реагировать на сообщения или звонки от «родственников», либо «друзей», нужно дозвониться человеку, от имени которого пришло сообщение, или кому-то из его близких, с которыми он в настоящее время может находиться;

- не поленитесь поискать в сети Интернет информацию о конкурсах и розыгрышах, участвовать, в которых призывают при помощи СМС-рассылки. Нередко обманутые участники подобных предложений оставляют на форумах предостерегающие отзывы;

- не спешите переводить или отдавать деньги. Требование внести денежную сумму, например, в качестве залога при розыгрыше призов или пополнить «контрольный» счет банка должно сразу насторожить.

Помните, сохраняя бдительность, Вы можете обезопасить себя и своих близких от противоправных действий, убережёте своё личное имущество от преступных посягательств. Все необходимые Вам справочные номера телефонов организаций и служб храните на видном месте. Очень часто жертвами мошенников становятся пожилые люди и дети, как наиболее доверчивая категория граждан. Поделитесь этой информацией со своими родственниками, предостерегите их, чтобы они не стали очередными жертвами мошенников.

Заместитель Барабинского межрайонного прокурора

Маморцев И.В.