Чтобы снизить риск быть обманутым в сети «Интернет», рекомендуем следовать следующим правилам:

1. Не доверяйте непроверенным сайтам знакомств, заработка, азартных игр, лотерей, тотализаторам.

2. Если на сайте нет юридического адреса, контактных телефонов, обратной связи, то не предоставляйте свои персональные данные, банковские сведения.

3. Не направляйте SMS-сообщения на короткие номера, указанные в инструкции по разблокировке и защите от вирусов.

4. Создавайте сложные пароли там, где есть доступ к Вашим данным и денежным средствам, пользуйтесь обновляемой проверенной антивирусной программой.

5. При совершении покупок в сети «Интернет» предварительно ознакомьтесь с информацией о магазине, отзывами о его работе, инструкцией по возврату и обмену товара. Обратите внимание на дату создания сайта по дате регистрации домена.
Проверить данные об организации можно на сайте Федеральной налоговой службы России, используя ИНН и ОГРН. Помимо этого, следует с помощью поиска посмотреть «черный список интернет – магазинов».

6. Будьте аккуратны и внимательны при работе с электронными кошельками и банк-клиентами на сомнительных сайтах, а также при проведении операций на чужих компьютерах.

Прокуратура Кировской области
610000 г. Киров, ул. Володарского, д. 98
«Телефон доверия»: 8(8332) 38-11-53
E-mail: prokuror@oblast.kirov.ru

Общероссийская
общественная организация
АССОЦИАЦИЯ ЮРИСТОВ РОССИИ
Кировское региональное отделение
г. Киров, ул. Дерендяева, 23, к.108
тел./факс (8332) 64-98-11
E-mail:info@alrf43.ru

Прокуратура Кировской области
***
Кировское региональное отделение
Общероссийской общественной
организации
«Ассоциация юристов России»

Будьте бдительны!

Мошенничество в Интернете

Киров
2019

Мошенничество в сети «Интернет»

Жертвами мошенников в сети «Интернет» становятся не только начинающие пользователи, но и юридически грамотные люди.

Основными признаками того, что Вас пытаются обмануть, являются очень заманчивые и привлекательные предложения, такие как: высокий заработок в «Интернете» за час работы, низкие цены в интернет – магазинах.

Должно насторожить любое виртуальное мероприятие, которое требует вложения денежных средств, предоплаты.

При покупке товаров настораживающими факторами являются отсутствие возможности курьерской доставки и самовывоза товара, отсутствие у продавца или магазина «истории», неточности или несоответствия в описании товаров, излишняя назойливость продавца или менеджера.

Распространенные способы мошенничества в сети «Интернет»

Создание лотерей, конкурсов, других мероприятий, где необходима регистрация участников с указанием полных персональных данных, используемых впоследствии для совершения хищения. При этом лотерейные билеты можно купить прямо на сайте. Организаторы создают страницу под видом официальной государственной лотереи или сайт – дублер (клон), где за небольшую плату идет продажа онлайн – билетов.

Сайты знакомств

Здесь более 80% анкет являются фейковыми, от их имени пишут владельцы сайта. Провоцируя воспользоваться платными услугами. Впоследствии отключить платную услугу весьма проблематично. Такие сайты никогда не имеют открытой для посетителей страницы с адресами, контактами, наименованием юридического лица.

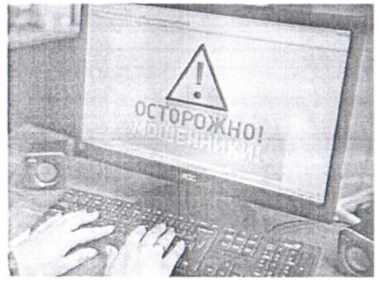
Также достаточно распространены случаи, когда мошенник ведет длительную переписку, в ходе которой поступает просьба о перечислении денежных средств для приобретения авиабилета, на покупку подарка, оплату услуг по доставке товара, в том числе с указанием сайта транспортной компании, о финансовой помощи в сложной ситуации и др.

Предложение заработка в сети «Интернет»

Это сайты о предоставлении рабочих вакансий, когда необходимо внести первоначальное вложение через «Интернет» в обмен на полную инструкцию по заработку.

Финансовые пирамиды

Внесение денег ради прибыли, которая складывается из взносов последующих участников.



Социальные сети

Происходит «взламывание» анкет в социальных сетях, и от имени «друзей» рассылаются сообщения о необходимости перечислить определенную сумму денег либо произвести голосование в каком-либо проекте.

Блокировка доступа к электронной почте, аккаунтам

В данном случае указывается определенная сумма, которую необходимо внести для того, чтобы была произведена разблокировка. Как правило, после внесения денег разблокировка не происходит, а появляется новая инструкция, которая призывает внести деньги повторно.

Интернет-магазины мошенников с предоплатой за товар

На таких Интернет – площадках товары продаются только по предоплате. Заказчик получает посылку с товаром ненадлежащего качества либо испорченным товаром, посылка может прийти пустой или вообще не направляться покупателю.

Вирусы, блокирующие работу компьютера

Для устранения блокировки мошенники предлагают направить SMS на указанный номер, в результате списываются денежные средства со счета либо с телефона.

Фишинг

Для фишинга мошенники создают копию популярного сайта или приложения и активно её распространяют. Предлоги для перехода по ссылке могут быть самыми разными: от уведомлений о посетителях страницы до угроз распространения личных сведений.

Как поступить правильно, чтобы не стать жертвой телефонных мошенников?

Ни в коем случае не пополняйте счета абонентов, чьи номера телефонов Вам не знакомы. Если все-таки это необходимо, то удостоверьтесь, что номер принадлежит Вашему родственнику или знакомому.

Свяжитесь со своим родственником, о котором шла речь в ходе телефонного разговора, и выясните у него, имели ли место события, о которых Вам сообщалось по телефону. Если не представляется возможным быстро связаться с родственником, необходимо обратиться в органы внутренних дел.

Проверяйте состояние своего лицевого счета телефона, а также подобные данные через оператора.

Если у Вас возникают сомнения по поводу услуг, представляемых оператором сотовой связи, обращайтесь в службу техподдержки.

Обращайте внимание на номер телефона звонившего и ни в коем случае не переводите денежные средства, даже если просят очень настойчиво. Никогда не отправляйте деньги незнакомым лицам на их электронные счета.

Не перечисляйте деньги на электронные кошельки и счета мобильных телефонов людям, которых Вы не знаете.

Не переходите по ссылке, указанной в сообщении.

При общении в социальных сетях не размещайте и не передавайте информацию личного характера, которая может быть использована во вред.

При появлении подозрений, что звонок поступает от мошенника необходимо незамедлительно обратиться с заявлением в ближайшее подразделение органов внутренних дел, прокуратуру либо сообщить об этом по ведомственным «телефонам доверия».

Общероссийская
общественная организация
АССОЦИАЦИЯ ЮРИСТОВ РОССИИ
Кировское региональное отделение
г. Киров, ул. Дерендяева, 23, к.108
тел./факс (8332) 64-98-11
E-mail:info@alrf43.ru

Прокуратура Кировской области
610000 г. Киров, ул. Володарского, д. 98
«Телефон доверия»: 8(8332) 38-11-53
E-mail: prokuror@oblast.kirov.ru

Прокуратура Кировской области

***

Кировское региональное отделение
Общероссийской общественной организации
«Ассоциация юристов России»

Будьте бдительны!

Телефонное мошенничество

Киров

2019

Способы телефонного мошенничества

Первый способ

На сотовый телефон абонента поступает SMS-сообщение с просьбой пополнить телефонный счет отправителя.

При этом в сообщении указывается, что отправитель находится на дороге, где произошло ДТП, либо сломался его автомобиль и ему срочно нужно позвонить, а деньги на телефоне закончились.

Абонента просят положить на счет отправителя небольшую фиксированную сумму денег (как правило, от 100 до 500 рублей) либо «сколько не жалко». Подобные сообщения могут носить анонимный характер, однако во многих случаях они подписаны распространенными именами, например, Саша или Иван.

Второй способ

На телефон абонента поступает звонок, при этом звонящий говорит взволнованным голосом и представляется родственником абонента, как правило, сыном или внуком.

Звонящий может называть женщину мамой или бабушкой, а мужчину – папой, и сообщает о том, что сбил человека, разбил чужую машину или совершил какое-либо другое преступление. После этого звонящий говорит о том, что в отношении него могут возбудить уголовное дело и, чтобы этого не произошло, необходимы денежные средства, и передает трубку якобы представителю правоохранительных структур.

Второй человек представляется сотрудником правоохранительных органов и уже спокойным голосом сообщает информацию, аналогичную той, которою сообщил первый собеседник. Во избежание уголовного преследования родственнику абонента предлагается собрать сумму денег и либо передать ее некоему человеку при встрече, либо отправить через банк «Блиц»-переводом.

В указанных случаях мошенники называют денежные суммы от нескольких десятков до нескольких сотен тысяч рублей.

Третий способ

Преступники обзванивают абонентов с предложением о какой-либо услуге (в том числе представляясь сотрудниками операторов сотовой связи) или запугивают, угрожают и требуют под любым предлогом перевода денежных средств.

Четвертый способ

На Ваш телефон приходит короткое SMS-сообщение с просьбой внесения, зачисления денежных средств на указанный телефонный номер.

Пятый способ

Вас текстовым сообщением уведомляют о выигрыше подарка или уникального приза, а чтобы получить дополнительную информацию, предлагают отправить смс-сообщение или позвонить по определенному номеру. После Вам могут предложить перевести денежные средства для получения приза.

Шестой способ

Вам на счет вдруг неожиданно начисляется некая сумма денег, о чем иногда может прийти уведомление. После Вам звонят и вежливо извиняются, сообщая о том, что ошиблись. Иногда мошенники не звонят, а присылают сообщение о том, что произведет ошибочный платеж.

Седьмой способ

Вам приходят сообщения и поступают звонки от «оператора сотовой связи». Такие сообщения от псевдооператоров могут приходить в различных вариантах. Например: «Условия Вашего тарифного плана были изменены. Подробности доступны при отправке SMS на номер ***». Номер для отправки, как обещают в сообщении – бесплатный.

Помимо рассылки SMS, бывают и звонки из «технической поддержки оператора». По словам звонящих, у вас проблема с номером телефона, или ваш тарифный план можно поменять на более выгодный. Также могут предлагать принять участие в тестировании новейшей и модной услуги.

Восьмой способ

При покупке в интернет – магазине товаров по суперпривлекательной цене Вам предлагают перечислить предоплату.

Девятый способ

Вы получили SMS-сообщение со ссылкой на скачивание открытки, музыки, картинки и программы.

Банкомат не должен выглядеть подозрительно. Обратите внимание на то, не прикреплены ли к нему какие – либо дополнительные устройства, не имеются ли на экране дополнительные инструкции, надписи и др.

6. Не пользуйтесь советами третьих лиц и не прибегайте к помощи незнакомцев при возникновении проблем в работе с банкоматом. В таком случае необходимо сразу же позвонить в службу поддержки клиентов банка, телефоны которой, как правило, указаны на банкомате.

7. Не передавать карту другим лицам, все операции с картой должны проводиться на Ваших глазах. В торговых точках, ресторанах и кафе все действия с пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты карты и при помощи специальных устройств использовать их в дальнейшем для изготовления подделки.

8. Пользуясь картой в сети «Интернет», внимательно относитесь к своевременному обновлению антивирусной программы. Не совершайте покупки на подозрительных сайтах, обращайте внимание на поддержку сайтами технологии 3D-Secure.

Не держите на карте, которую используете для платежей в сети «Интернет», крупную сумму. Для совершения покупки дистанционно лучше оформить отдельную карту или выпустить «виртуальную карту».

9. Если карта утрачена или есть подозрения, что данные карты стали известны третьему лицу, незамедлительно позвоните в банк и заблокируйте карту. Если Вы подключены к сервису «Мобильный банк», то блокировку можно сделать при помощи направления SMS-уведомления.

10. Не сообщайте данные карты, персональные данные, коды, сведения, содержащиеся в SMS-уведомлениях, посторонним лицам. Не давайте никому доступ к Вашей карте через онлайн-банкинг.

11. Регулярно меняйте PIN-код Вашей карты. Особенно после заграничных поездок или снятия денег в подозрительных местах.

Только Ваша бдительность и внимательность поможет Вам не стать жертвой преступления!

Прокуратура Кировской области
610000 г. Киров, ул. Володарского, д. 98
«Телефон доверия»: 8(8332) 38-11-53
E-mail: prokuror@oblast.kirov.ru

Общероссийская общественная организация
АССОЦИАЦИЯ ЮРИСТОВ РОССИИ
Кировское региональное отделение
г. Киров, ул. Дерендяева, 23, к.108
тел. факс (8332) 64-98-11 E-mail:info@adr43.ru

Прокуратура Кировской области
***
Кировское региональное отделение
Общероссийской общественной
организации
«Ассоциация юристов России»

Будьте бдительны!

Мошенничество

с кредитными картами

Киров

2019

Банковские пластиковые карты – способ совершения преступления

Банковские пластиковые карты каждый из нас использует в повседневной жизни.

Они упрощают процесс оплаты, а главное – являются дополнительной защитой для денежных средств, ведь украденная карта бесполезна, если не знать PIN-код.

Но безопасность средств, хранимых на банковском счете, зависит в первую очередь от того, соблюдает владелец правила пользования картой или нет.

Небрежное обращение с картой работает на руку мошенникам, которые постоянно изыскивают новые способы обмана владельцев карт.

Самое трудное для мошенников – узнать PIN-код. Для этого могут использоваться различные способы.

В первую очередь, это оглашение сведений о PIN-коде самим держателем карты. Имеется в виду, например, его запись на карте или каком-либо другом носителе (лист бумаги, записная книжка и др.), хранимая вместе с картой.

Также карты могут быть использованы людьми с предварительной осведомленностью о PIN-коде: членами семьи, близкими друзьями, коллегами по работе - то есть теми, кто имеет доступ к хранению карты.

Помимо этого, мошенник может узнать PIN-код держателя банковской карты, подглядывая из-за его плеча, пока тот вводит код в банкомате, либо во время оплаты покупки в магазине.

Последние годы злоумышленники чаще всего звонят гражданам, представляясь сотрудниками банков, называя по имени – отчеству, и просят сообщить данные карт. При этом могут быть использованы программы подмены телефонных номеров, входящий звонок может определяться у клиента как номер банка.

Для совершения мошенничества с кредитными картами могут использоваться фальшивые банкоматы либо переделанные старые банкоматы. Размещаются они в наиболее оживленных местах. После введения карты и PIN-кода на дисплее такого банкомата появляется надпись, что денег в банкомате нет или что банкомат неисправен.

Также преступники могут использовать особые устройства, считывающие информацию с магнитных полос карты (скимминг). Как правило, это специально изготовленные клавиатуры, которыми накрывают существующие.

Нередко мошенники для кражи денег пользуются психологическими приемами для управления действиями человека. Они изображают покупателей автомобилей, земельных участков, животных, мебели, одежды и др. на сайтах бесплатных объявлений или в социальных сетях. При этом они все находятся где-то далеко, но для того чтобы вожделенный товар не приобрел кто-то другой, они готовы перевести часть стоимости или даже полную стоимость немедленно на банковскую карту продавца.

Основные правила безопасности для владельцев пластиковых карт

1. **Никогда и никому не сообщайте PIN-код карты**, не пишите его на карте или другом носителе, не храните его рядом с картой. **Выучите** PIN-код.

2. Для оперативного получения **информации об операциях по расчетному счету** подключите на телефоне услугу «СМС-оповещение».

3. Обратившись в обслуживающий Вас банк, установите лимит (дневной) снятия наличных денежных средств с карты.

4. **Не стесняйтесь закрывать** от посторонних **клавиатуру банкомата** во время ввода PIN-кода.

5. **Снимайте денежные средства и производите операции по карте** в банкоматах, которые расположены в офисах банка, рядом с ними, или находящимися в государственных учреждениях, крупных торговых центрах и т.д.