МАТЕИАЛЫ
ДЛЯ ОЗНАКОМЛЕНИЯ РАБОТНИКОВ ПРЕДПРИЯТИЙ

Дистанционное мошенничество — это совершение такого вида **мошенничества**, при котором виновный, чаще всего используя компьютерные и телефонные сети, воздействует на сознание потерпевшего путем обмана, склоняет к передаче имущества удаленным образом.

Одним из самых распространенных видов интернет-мошенничества является так называемый**«Фишинг».**Мошенники совершают определенные действия, направленные на получение доступа к денежным средствам на банковской карте потенциальной жертвы, при помощи почтовых рассылок от лица банка, содержащих в себе ссылки на страницы, являющиеся точными копиями официальных сайтов, на которых предлагается ввести данные карты для возможности дальнейшего ее использования.

Еще одним крайне распространенным видом интернет-мошенничества являются **фальшивые интернет-магазины**. Мошенники берут с покупателя предоплату за товар и не выполняют своих обязательств.

Важно отметить, что популярность в поисковике вовсе не гарантия вашей безопасности. На самом деле мошенники активно продвигают свои сайты с использованием вебмаркетинга. И зачастую фальшифкистоят даже выше ссылок на оригинальный сайт и внешне он на первый взгляд ничем не отличается от оригинала. Платежные страницы на таких сайтах только маскируются под оплату товаров и услуг, на самом деле потенциальная жертва переводит деньги на карты мошенников или на номера мобильных телефонов, с которых впоследствии мошенники снимут деньги. Кроме того на поддельных сайтах мошенники собирают реквизиты карт, которые потом используют для несанкционированных операций. После совершения такой оплаты, жертва даже может получить подтверждение по почте, но товаров ни услугдоставлено и оказано не будет.

Как же отличить поддельные сайты от настоящих?

Первое – внимательно изучите адресную строку. Дизайн может полностью копировать оригинальный сайт, но в адресной строке точно будет что-то не так, хотя бы один символ.

Второе – сайт новый и о нем нет никакой информации в интернете.

Третье – тексты на сайте могут содержать ошибки и неработающие ссылки.

Четвертое – дизайн страницы ввода одноразового пароля может отличаться от привычного дизайна вашего банка, а еще название магазина будет написано порски, а не латинскими буквами как обычно в легальных платежных системах.

Пятое – вместо названия магазина на аутентификационной странице символы P2P, PEREVODNAKARTU, или CARD2CARD, то есть информация о переводе средств с карты на карту.

Шестое – сумма на аутентификационной странице банка может быть изменена.

Седьмое – после введения корректных данных сайта для одноразового пароля жертве сообщают, что пароль неверный и просят ввести новый пароль на самом деле, чтобы провести новую операцию.

Заметив любой из этих признаков, звоните по телефону, который указан на вашей карте и пользуйтесь только проверенными интернет-площадками.

Крайне распространенным способом мошенничества является **мошенничество в социальных сетях**. Мошенники взламывают персональную страницу пользователя в социальных сетях или мессенджере и либо всем подряд отправляют сообщения с просьбой помочь и срочно перевести денег, либо анализируют переписку и находят самых близких людей, тех, кто точно не откажет.

После первого перевода мошенники могут связаться с жертвой, сказать, что-то пошло не так, попросить повторить перевод и так пока на карте не закончатся деньги или жертва не догадается об обмане, но выманивать могут не только деньги, но и реквизиты карт якобы для того, чтобы перевести деньги жертве, спросят номер карты, срок действия, трехзначный код безопасности и пароли из смс, однако деньги жертве разумеется не придут, зато с карты средства будут списаны.

Что же делать, если вам пришло сообщение с просьбой о помощи от одного из знакомых или родственников? Необходимо немедленно связаться с ним по телефону, уточнить отправлял ли он это сообщение и не предпринимать ничего, пока он не подтвердит это лично. Тем более ни в коем случае нельзя сообщать реквизиты своей карты (три цифры на оборотной стороне, срок действия, пароль из смс, кроме того нужно позаботиться и о пароле для своего аккаунта в соцсетях и мессенджерах. Он защищает не только вашу безопасность, но и безопасность ваших родных и близких.

Довольно часто мошенники выдают себя **за сотрудников банка**. Под предлогом «сбоя в базе данных», «начисления бонусов» или «подключения к социальной программе» злоумышленники просят, а иногда даже требуют сообщить им реквизиты карты, код безопасности и одноразовый пароль. Получив необходимые сведения, мошенники списывают деньги со счета.

ПОМНИТЕ! При звонке клиенту сотрудник банка никогда не просит сообщить ему реквизиты карты и совершать какие-либо операции с картой.

Если вам позвонили из банка, и интересуются вашей платежной картой, разумнее всего прекратить разговор и перезвонить в банк по официальному номеру контактного центра банка (номер телефона службы поддержки клиента указывается на оборотной стороне карты).

Более подробно остановимся на данных, которые могут быть запрошены у жертвы мошенниками.

ПИН-код карты – четырехзначная комбинация цифр, выдаваемая в конверте одновременно с изготовленной банковской картой. Его можно изменить, обратившись в отделение банка или позвонив на горячую линию.

Код безопасности (**CVV**2 или **CVC**2) – комбинация цифр, указанная на оборотной стороне карты, а именно: три крайние правые цифры, указанные после четырех последних цифр номера карты. Проверочный код необходим только для совершения платежей в интернете. При онлайн-оплате он вводится

вместе с номером карты, именем держателя карты и сроком окончания действия карты.

Одноразовый пароль банка для подтверждения оплаты онлайн – комбинация цифр, отправляемых банком в смс-сообщении или push-уведомлении для подтверждения операций с денежными средствами.

Ни в коем случае не сообщайте ПИН-код, код безопасности или одноразовый пароль третьим лицам!

Никто, в том числе сотрудники банка, не вправе требовать от держателя карты сообщить ПИН-код или код безопасности. А одноразовый пароль вводится при совершении онлайн-покупки на странице с защищенным соединением.

Кодовое слово держателя карты – информация, указанная клиентом банка при оформлении карты. Кодовое слово необходимо для идентификации клиента при звонке в контакт-центр банка. Рекомендуется использовать кодовые слова, которые злоумышленникам будет очень сложно узнать. Подумайте о том, что случилось с Вами в детстве или юности, вспомните место действия, объект, человека или событие – пусть оно будет Вашим кодовым словом.

Код клиента банка – комбинация цифр, используемая для сокращения времени на идентификацию клиента при обращении в контакт-центр.

Сообщать кодовое слово или код клиента банка можно только в том случае, если вы обратились в контакт-центр и разговариваете с сотрудником банка.

На территории Ханты-Мансийского автономного округа Югры, в том числе на территории г. Нефтеюганска отмечается рост совершения мошеннических действий в отношении граждан под видом оказания различных услуг, в том числе в банковской сфере, посредством мобильной связи и сети «Интернет». Зачастую потерпевшие от преступных посягательств граждане не осведомлены о вновь появляющихся видах и способах мошенничеств, ввиду чего не способны в полной мере обезопасить себя от таковых посягательств.

С целью предупреждения преступных посягательств в отношении граждан, рассмотрим имеющиеся виды, способы мошеннических действий, а также способы избежать столкновения с мошенником.

Как безопасно пользоваться интернет-банком.

1. Используйте сложный пароль блокировки экрана и качественную антивирусную программу. Не входите в банковские приложения, используя отпечаток пальца или функцию распознавания лица.
2. Ни в коем случае не храните в телефоне логин и пароль от входа в мобильный банкинг.
3. Не храните в телефоне реквизиты карты: номер, срок действия, проверочный код и ПИН-код карты.

4. Избегайте входа в систему мобильного банкинга с чужих устройств.
5. При утрате телефона немедленно обратитесь в банк для блокировки карты и в офис мобильного оператора для блокировки SIM-карты.
6. Не переходите по ссылкам из SMS-сообщений, даже если в сообщении утверждается, что оно из банка.
7. Отключите функцию отображения текста входящих SMS- уведомлений на экране заблокированного телефона.

Как безопасно совершать платежи в интернете?

1. Используйте на устройстве антивирус с активной защитой онлайн-платежей.
2. Совершайте оплату только посредством использования защищенных соединений. Защищенное или зашифрованное подключение можно распознать по значку в виде замочка в начале адресной строки браузера и префиксу https:// (не просто http, а с буквой s на конце) перед адресом сайта.
3. Всегда завершайте сеанс в интернет-банке перед тем, как закроете вкладку браузера. Не проводите финансовые операции с общественного WI-FI в кафе, транспорте или гостиницах.
4. Не сохраняйте свои данные о карте в браузере.

Как обезопасить себя и не стать жертвой мошенников

Чтобы не попасть на уловки мошенников, нужно проявлять бдительность при совершении любых денежных операций с помощью банковских карт и никогда никому не раскрывать данные карты. Сотрудники банка не требуют назвать их или CVV/CVC номер на обороте.

Обезопасить личные финансы позволит соблюдение базовых правил:

1. пользоваться отдельной виртуальной картой для покупок, пополнять ее лучше разово — только при совершении оплаты;
2. создавать сложные и пароли и использовать разные данные для почтовых ящиков, соцсетей, других сайтов, ведь пароль восстановить проще, чем вернуть украденные деньги;
3. не кликать по неизвестным ссылкам, которые приходят по электронной почте, в мессенджерах, социальных сетях, особенно если предлагают что-то бесплатное или на выгодных условиях;
4. не сообщать посторонним личные данные карты и не вводить их на незнакомых сайтах, не указывать коды безопасности из смс-сообщений;
5. критически оценивать любую информацию, сообщения, объявления в интернете, а также не верить на слово внезапным обращениям от друзей и родственников, скорее всего неожиданная просьба о деньгах поступила от мошенника, который взломал аккаунт;
6. использовать в незнакомых местах VPN (Virtual Private Network) анонимный (приватный) доступ в Интернет, чтобы мошенники не могли скачать с устройства личные данные.

Мошенничества, совершаемые с использованием мобильного телефона (звонки):

1. Звонок от сотрудника банка (сотрудника службы безопасности банка, финансового помощника): сотрудники финансово-кредитных организаций НЕ ОСУЩЕСТВЛЯЮТ ЗВОНКИ своим клиентам, а также НЕ ИНТЕРЕСУЮТСЯ ОБ ИМЕЮЩИХСЯ У НИХ БАНКОВСКИХ КАРТАХ, ДЕНЕЖНЫХ СРЕДСТВАХ, НЕ ТРЕБУЮТ НАЗВАТЬ КАКИЕ-ЛИБО РЕКВИЗИТЫ БАНКОВСКОЙ КАРТЫ!

В случае, если Вам поступил звонок от неизвестного лица, которое сообщает Вам о том, что в отношении Вас совершаются мошеннические действия, на Вас оформили кредитное обязательство и иное, НЕМЕДЛЕННО ПРЕКРАТИТЕ РАЗГОВОР, не нужно вести диалог с неизвестным лицом, если у Вас имеются сомнения по поводу сохранности Ваших денежных средств и их безопасности, обратитесь в отделение банка эмитента Вашей банковской карты или же осуществите звонок на горячую линию (абонентский номер указан с обратной стороны Вашей банковской карты) для получения подробной информации. НЕ СООБЩАЙТЕ РЕКВИЗИТЫ СВОЕЙ БАНКОВСКОЙ КАРТЫ, КАКИЕ-ЛИБО ПОСТУПАЮЩИЕ КОД-ПАРОЛИ, ТРЕТЬИМ ЛИЦАМ

2. Звонок от сотрудников полиции, прокуратуры, следственного комитета, МФЦ: указанные сотрудники НИКОГДА НЕ БУДУТ интересоваться Вашими финансами, банковскими картами. Также, сотрудники НЕ ПРОСЯТ ГРАЖДАН ОКАЗАТЬ СОДЕЙСТВИЕ В ПОИМКЕ МОШЕННИКОВ или недобросовестных сотрудников банка. Если Вам позвонили и сообщили, что в отношении Вас совершаются мошеннические действия или Вашими личными данными завладело третье лицо, НЕМЕДЛЕННО ПРЕКРАТИТЕ РАЗГОВОР И ОБРАТИТЕСЬ В ПОЛИЦИЮ для уточнения данной информации.

3. Звонок от незнакомых людей с неизвестных номеров, которые сообщают Вам о том, что Ваш близкий человек попал в беду, совершил преступление, попал в больницу и ему срочно требуется финансовая помощь. НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ! В данной ситуации осуществите звонок своему близкому человеку, о котором, возможно, шла речь, уточните информацию о том, в порядке ли он.

Мошенничества, совершаемые с использованием сети «Интернет»

Социальные сети. В случае, если Ваш знакомый/близкий человек посредством сообщения в социальной сети просит Вас одолжить ему денежные средства (в долг), осуществите звонок данному человеку посредством сотовой связи и уточните, действительно ли именно Ваш знакомый/близкий человек просит Вас об одолжении. В СЛУЧАЕ, ЕСЛИ УКАЗАННЫЕ ДЕЙСТВИЯ ВАШ знакомый/близкий человек не осуществлял, НЕМЕДЛЕННО ПРЕКРАТИТЕ ДИАЛОГ С МОШЕННИКОМ И ОСУЩЕСТВИТЕ БЛОКИРОКУ КОНТАКТА от которого поступило сообщение с просьбой, так как вышеуказанные действия свидетельствуют о

ВЗЛОМЕ СТРАНИЦЫ в социальной сети Вашего знакомого/близкого человека, ОБЯЗАТЕЛЬНО УВЕДОМИТЕ человека, чья страница была взломана.

НЕ РАЗМЕЩАЙТЕ ЛИЧНЫЕ ДАННЫЕ НА СТРАНИЦАХ СОЦИАЛЬНЫХ СЕТЕЙ, которыми могут воспользоваться МОШЕННИКИ!

Наиболее часто **МОШННИКИ ИСПОЛЬЗУЮТ АБОНЕНТСКИЕ НОМЕРА НЕСВОЙСТВЕННЫЕ** региону ХМАО-Югры, а именно: абонентские номера, начинающиеся на **+7 495***; +7 499***.**

Будьте бдительны к своим финансам и распространению персональных данных!

СТАРАЙТЕСЬ ИЗБЕГАТЬ ПЛАТЕЖЕЙ В СЕТИ ИНТЕРНЕТ ПОСРЕДСТВОМ СВОЕЙ БАНКОВСКОЙ КАРТЫ;

* НЕ ОСУЩЕСТВЛЯЙТЕ ПОКУПКИ В СЕТИ ИНТЕРНЕТ НА ПОДОЗРИТЕЛЬНЫХ И НЕЗНАКОМЫХ САЙТАХ ПО «ПРИВЛЕКАТЕЛЬНЫМ ЦЕНАМ»;

* ПРЕРВИТЕ РАЗГОВОР, ЕСЛИ ВАМ ЗВОНИТ НЕИЗВЕСТНОЕ ЛИЦО И ГОВОРИТ С ВАМИ О ФИНАНСАХ, ИМЕЮЩИХСЯ БАНКОВСКИХ КАРТАХ;

* НЕ ПЕРЕХОДИТЕ ПО ПОДОЗРИТЕЛЬНЫМ ССЫЛКАМ;

* НЕ ПЕРЕЧИСЛЯЙТЕ ДЕНЕЖНЫЕ СРЕДСТВА НА ЭЛЕКТРОННЫЕ КОШЕЛЬКИ, не убедившись в благонадёжности контрагента;

* НЕ СООБЩАЙТЕ НЕЗНАКОМЫМ или МАЛОЗНАКОМЫМ ЛИЦАМ ЛИЧНЫЕ ДАННЫЕ, которые в дальнейшем могут быть использованы Вам во вред

При просмотре социальных сетей НЕ ПЕРЕХОДИТЕ ПО ВСПЛЫВАЮЩИМ ССЫЛКАМ, РЕКЛАМНЫМ ОБЪЯВЛЕНИЯМ, данные ссылки направят Вас на МОШЕННИЧЕСКИЙ САЙТ ДВОЙНИК/ ИНТЕРНЕТ-МАГАЗИН/САЙТ, СОДЕРЖАЩИЙ В СЕБЕ ВИРУСНЫЕ УГРОЗЫ.

При осуществлении заказа в интернет-магазине (страница социальной сети, владелец которой осуществляет продажу товаров), УБЕДИТЕСЬ, ЧТО ВЛАДЕЛЬЦЕМ ДАННОЙ СТРАНИЦЫ ЯВЛЯЕТСЯ НЕ МОШЕННИК! В случае, если у интернет-магазина ОТСУТСТВУЕТ ЮРИДИЧЕСКИЙ АДРЕС, ОТСУТСТВУЕТ ИНФОРМАЦИЯ О ВЛАДЕЛЬЦЕ ДАННОГО ИНТЕРНЕТ-МАГАЗИНА (продавце), а также если ДЛЯ СОВЕРШЕНИЯ ЗАКАЗА НЕОБХОДИМО ВНЕСТИ ПОЛНУЮ ОПЛАТУ ЗА ТОВАР – это свидетельствует о том, что владелец данной страницы интернет-магазина возможно МОШЕННИК!

РАССКАЖИТЕ ОБ УГРОЗЕ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ СВОИМ БЛИЗКИМ!

2. Интернет сайты. НЕ ОСУЩЕСТВЛЯЙТЕ ЗАКАЗ ТОВАРОВ НА САЙТАХ, КОТОРЫМИ РАНЕЕ ВЫ НЕ ПОЛЬЗОВАЛИСЬ. В случае, если всё-таки возникла данная необходимость, прочтите отзывы о данном сайте.

При осуществлении покупок на сайте, который ранее Вы использовали, ОБРАТИТЕ ВНИМАНИЕ НА АДРЕСНУЮ СТРОКУ САЙТА (https://***), в случае, если В АДРЕСЕ САЙТА ПРИСУТСТВУЮТ ЛИШНИЕ СИМВОЛЫ, это свидетельствует о том, что ДАННЫЙ САЙТ ЯВЛЯЕТСЯ ДВОЙНИКОМ оригинального сайта, на котором ранее вы осуществляли покупки.

Пример:

https://www.tutu.ru/ (ОФИЦИАЛЬНЫЙ САЙТ);

https://www.tu-tul.com (САЙТ ДВОЙНИК - мошенник).

3. Интернет платформы для продажи/покупки товаров. В случае, если Вы осуществляете покупку товаров посредством интернет платформ «АВИТО», «ЮЛА» и иных, НЕ ПЕРЕВОДИТЕ АВАНС ПРОДАВЦУ в счет оплаты товара. В СЛУЧАЕ, ЕСЛИ ПРОДАВЕЦ ВАС ТОРОПИТ С ПОКУПКОЙ/ОСУЩЕСТВЛЕНИЕМ ПЛАТЕЖА, это может свидетельствовать о том, что данный продавец – МОШЕННИК! НЕ ПРЕХОДИТЕ ПО ССЫЛКАМ, КОТОРЫЕ НАПРАВЛЯЕТ ВАМ ПРОДАВЕЦ под видом ссылки на переход для оплаты посредством сервиса быстрых платежей.

В случае, если Вы осуществляете продажу товара посредством интернет платформ «АВИТО», «ЮЛА» и иных, НЕ СООБЩАЙТЕ ПОКУПАТЕЛЮ БАНКОВСКИЕ РЕКВИЗИТЫ СВОЕЙ БАНКОВСКОЙ КАРТЫ для оплаты товара. НЕ ПРЕХОДИТЕ ПО ССЫЛКАМ, КОТОРЫЕ НАПРАВЛЯЕТ ВАМ ПОКУПАТЕЛЬ под видом ссылки на переход для оплаты посредством сервиса быстрых платежей.

4. Мессенджеры. В случае, если Вам ПОСТУПИЛО СМС-УВЕДОМЛЕНИЕ в каком-либо МЕССЕНДЖЕРЕ ОТ НЕИЗВЕСТНОГО ОТПРАВИТЕЛЯ, содержащее в себе какую-либо ССЫЛКУ, НЕ ПЕРЕХОДИТЕ ПО УКАЗАННОЙ ССЫЛКЕ, ввиду того, что она может содержать вирусные угрозы (вирусы-мошенники). НЕ РЕАГИРУЙТЕ на поступающие смс-уведомления о ВЫЙГРАШАХ, НЕОБХОДИМОСТИ ПОЛУЧЕНИЯ КАКИХ-ЛИБО ПОСОБИЙ и иное.

ВСЕ УКАЗАННЫЕ ДЕЙСТВИЯ СОВЕРШАЮТ МОШЕННИКИ!

Если все-таки мошенникам удалось совершить преступление, то жертве необходимо обратиться в полицию с заявлением или по телефону 112, сохранить ссылки на сайты, с которых были совершены мошеннические действия, переписку с мошенниками и другие данные, которые могут быть полезны для идентификации мошенников.