г.п. Белый Яр 2022 год

**РЕКОМЕНДАЦИИ**

**о правилах безопасного использования компьютерных технологий, расчетных банковских карт, социальных сетей.**

Разработанные с целью пресечения преступлений, совершаемых с использованием информационно-телекоммуникационных технологий на территории Сургутского района Ханты-Мансийского автономного округа - Югры, а также для формирования у населения культуры безопасного использования компьютерных технологий, расчетных банковских карт, социальных сетей, разработанные ОМВД России по Сургутскому району

**РЕКОМЕНДАЦИИ**

**о правилах безопасного использования компьютерных технологий, расчетных банковских карт, социальных сетей**

На территории Ханты-Мансийского автономного округа Югры, в том числе на территории Сургутского района 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.

**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 БАНКОСКОЙ КАРТЫ, КАКИЕ-ЛИБО ПОСТУПАЮЩИЕ КОД-ПАРОЛИ, ТРЕТЬИМ ЛИЦАМ!



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

**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»**

**1. 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!

**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 ВЫИГРАШАХ, НЕОБХОДИМОСТИ ПОЛУЧЕНИЯ КАКИХ-ЛИБО ПОСОБИЙ и иное.

**ВСЕ УКАЗАННЫЕ ДЕЙСТВИЯ СОВЕРШАЮТ МОШЕННИКИ!**

**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.



**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).

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!

**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 САЙАХ 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 благонадежности контрагента;

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