**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 Нефтеюганского 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 Нефтеюганскому району.

г. Нефтеюганск 2022 год

**РЕКОМЕНДАЦИИ**

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

На территории Ханты-Мансийского автономного округа Югры, в том числе на территории Нефтеюганского 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):**



**2. 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!

**1. 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!

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

**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.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!**