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 г. Мегиона Ханты-Мансийского автономного округа - Югры, а также для формирования у населения культуры безопасного использования компьютерных технологий, расчетных банковских карт, социальных сетей, разработанные ОУР ОМВД России по г. Мегиону

г. Мегион 2023 год

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

На территории Ханты-Мансийского автономного округа Югры, в том числе на территории г. Мегиона продолжают совершаться противоправные действия, выраженные в совершении хищений денежных средств со счетов банковских карт, 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,

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.

Наиболее часто **МОШННИКИ ИСПОЛЬЗУЮТ АБОНЕНТСКИЕ НОМЕРА НЕСВОЙСТВЕННЫЕ** региону ХМАО-Югры, а именно: абонентские номера, начинающиеся на **+7 495***; +7 499***, 8 800****

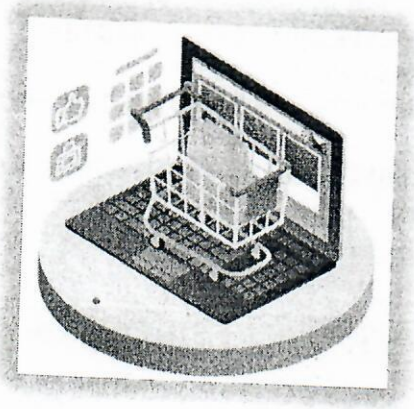
Мошенничества, совершаемые с использованием сети «Интернет»

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!

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!



2. Интернет сайты. НЕ ОСУЩЕСТВЛЯЙТЕ ЗАКАЗ ТОВАРОВ ,ПОКУПКУ БИЛЕТОВ (АВИА и ЖД) 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);

3. Интернет платформы для продажи/покупки товаров. В случае, если Вы осуществляете покупку товаров посредством интернета 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 интернета 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 ВЫИГРАШАХ, НЕОБХОДИМОСТИ ПОЛУЧЕНИЯ КАКИХ-ЛИБО ПОСОБИЙ и иное.

5. **Единый портал государственных услуг Российской Федерации**. Осуществление звонков неизвестных лиц, которые могут представляться сотрудниками службы поддержки портала «Госуслуги», сотрудниками правоохранительных органов или под видом иных должностных лиц с ЦЕЛЬЮ ПОЛУЧЕНИЯ ИМЕЮЩЕЙСЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПОЛЬЗОВАТЕЛЕЙ ПОРТАЛА (паспортные данные, СНИЛС, ИНН, наличие сведений о банковских картах и счетах, номере телефона).

Цель звонка злоумышленника получить в ходе разговора необходимую информацию, а именно код, который будет содержаться в смс-уведомлении, поступившем на абонентский номер пользователя портала (потенциального потерпевшего лица), а также логина и пароля его авторизованной учетной записи.

Необходимые действия: НЕМЕДЛЕННОЕ ПРЕКРАЩЕНИЕ ДИАЛОГА, ПРИ НЕОБХОДИМОСТИ СМЕНИТЬ ПАРОЛЬ УЧЕТНОЙ ЗАПИСИ, ОБРАТИТЬСЯ В МФЦ.

ЗАПРЕЩАЕТСЯ СООБЩАТЬ КОД ИЗ СМС-УВЕДОМЛЕНИЯ, СВЕДЕНИЯ О РЕКВИЗИТАХ БАНКОВСКИХ КАРТ, ИНУЮ КОНФИДЕНЦИАЛЬНУЮ ИЛИ ПЕРСОНАЛЬНУЮ ИНФОРМАЦИЮ.

ВСЕ УКАЗАННЫЕ ДЕЙСТВИЯ СОВЕРШАЮТ МОШЕННИКИ!

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»;
* ПРЕКРАТИТЕ РАЗГОВОР, ЕСЛИ ВАМ ЗВОНИТ НЕИЗВЕСТНОЕ ЛИЦО И ГОВОРИТ С ВАМИ О ФИНАНСАХ, ИМЕЮЩИХСЯ БАНКОВСКИХ КАРТАХ, ФИНАНСОВЫХ ОПЕРАЦИЯХ;
* НЕ ПЕРЕХОДИТЕ ПО ПОДОЗРИТЕЛЬНЫМ СТОРОННИМ 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.

РАССКАЖИТЕ ОБ УГРОЗЕ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ СВОИМ БЛИЗКИМ!

Не верьте, если вам позвонили и сказали, что кто-то из близких попал в неприятную ситуацию. Сейчас очень популярным стал сценарий, согласно которому, на домашний телефон поступает звонок от человека, который сообщает, что ваш родственник попал в ДТП или подрался с кем-то и теперь ему грозит срок. Вам предлагают встретиться в течение нескольких часов и отдать немалую сумму денег, чтобы решить все проблемы.

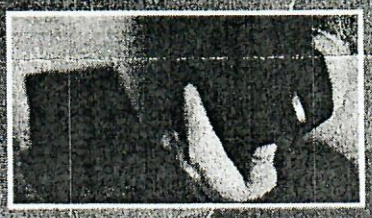
Первым делом постарайтесь любыми возможными способами связаться с родственником, о котором идет речь. Если он не доступен, свяжитесь с кем-нибудь, кто может знать о его местоположении.

Не верьте, если вам позвонили и сказали, что кто-то из близких попал в неприятную ситуацию. Сейчас очень популярным стал сценарий, согласно которому, на домашний телефон поступает звонок от человека, который сообщает, что ваш родственник попал в ДТП или подрался с кем-то и теперь ему грозит срок. Вам предлагают встретиться в течение нескольких часов и отдать немалую сумму денег, чтобы решить все проблемы.

Первым делом постарайтесь любыми возможными способами связаться с родственником, о котором идет речь. Если он не доступен, свяжитесь с кем-нибудь, кто может знать о его местоположении.

ТЕЛЕФОННЫЕ МОШЕННИЧЕСТВА

МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ СОТОВОЙ СВЯЗИ СОВЕРШАЮТСЯ В ОСНОВНОМ, ПУТЕМ СООБЩЕНИЯ ГРАЖДАНАМ ЗАВЕДОМО ЛОЖНОЙ ИНФОРМАЦИИ:



Вам сообщают, что кто-то из близких попал в ДТП, больницу, совершил преступление, и ему срочно нужны деньги, после чего просят передать их лично или куда-либо перевести.

Поступает звонок или СМС от якобы сотрудника службы безопасности банка. Вам сообщают о блокировке карт, аресте счетов, незаконном списании средств с вашей карты и т.п., после чего просят сообщить им реквизиты карты и ваши персональные данные.

Вы получаете СМС или звонящий сам сообщает, что вы стали обладателем приза или победителем конкурса, далее следует просьба перечислить ему деньги под благовидным предлогом, как гарантию того, что награда попадет именно к Вам.

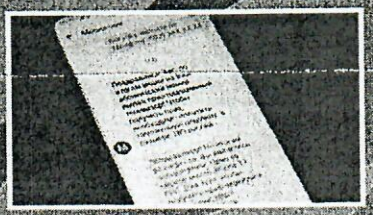
ЧТО ДЕЛАТЬ, ЧТОБЫ УБЕРЕЧЬ СВОИ ДЕНЬГИ

Позвоните своему близкому человеку, в больницу, в органы внутренних дел и проверьте информацию

Никогда не передавайте и не переводите деньги незнакомым людям

КИБЕРМОШЕННИЧЕСТВО

ВИРУСНОЕ ЗАРАЖЕНИЕ ПК ИЛИ СМАРТФОНА ДЛЯ ПОЛУЧЕНИЯ ДОСТУПА К ДАННЫМ СИСТЕМ ОНЛАЙН БАНКИНГА И ПОХИЩЕНИЯ ДЕНЕГ С ВАШЕГО СЧЕТА:



На Ваш смартфон или компьютер поступает сообщение, либо письмо с любой информацией, которая способна Вас заинтересовать, при этом в данном сообщении содержится ссылка, по которой необходимо перейти.

Вы сами устанавливаете на свой смартфон или компьютер нелицензионное программное обеспечение. При этом не обращаете внимание, что предоставляете этой программе доступ к сети интернет, отправке СМС и т.п.

Вы теряете свой мобильный телефон с подключенной услугой «Мобильный банк».

ЧТО ДЕЛАТЬ, ЧТОБЫ УБЕРЕЧЬ СВОИ ДЕНЬГИ

Не переходите по ссылкам и не устанавливайте приложения/обновления, пришедшие по СМС, ММС, электронной почте, мессенжерам, в том числе от имени банка

В случае потери мобильного телефона с подключенной услугой «Мобильный банк», следует срочно обратится в контактный центр банка для блокировки услуги.

МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ

МОШЕННИЧЕСТВА ПРИ ПОКУПКАХ ИЛИ ПРОДАЖАХ ЧЕРЕЗ СЕТЬ ИНТЕРНЕТ (ОНЛАЙН МАГАЗИНЫ, СОЦ. СЕТИ, РЕСУРСЫ ОБЪЯВЛЕНИЙ).

Мошенники создают сайты-клоны торговых площадок с отличной репутацией (копируют интерфейс оригинального сайта), с небольшим отличием в доменном имени сайта. Вы отдаете деньги мошенникам, думая что покупаете товар.

Мошенники создают собственные интернет-магазины, как правило с товарами по цене существенно ниже среднерыночной, либо с большими скидками.

Вы размещаете в сети интернет объявление о продаже какого-либо товара. Вам звонит мошенник и сообщает о своем намерении купить ваш товар, при этом просит сообщить данные вашей банковской карты для перевода на нее денежных средств.

ЧТО ДЕЛАТЬ, ЧТОБЫ УБЕРЕЧЬ СВОИ ДЕНЬГИ

Проверьте правильно ли Вы написали доменное имя сайта. Зайдите в раздел сайта, где размещены контактные данные сайта. Если указан лишь адрес электронной почты или телефон, воздержитесь от покупки. Проверьте дату регистрации сайта, если продавец работает недавно, лучше найти альтернативу.

Никому не сообщайте данные своей банковской карты.