Городской округ Ханты-Мансийск
Ханты-Мансийского автономного округа – Югры
Администрация города Ханты-Мансийска

ЗАМЕСТИТЕЛЬ ГЛАВЫ ГОРОДА

Дзержинского ул., д.6, г.Ханты-Мансийск,
Ханты-Мансийский автономный округ – Югра,
Тюменская область, Россия, 628012
Тел/факс 8(3467)33-23-80
E-mail: pr@admhmansy.ru
ОКПО 02067681, ОГРН 1028600511488,
ИНН/КПП 8601003378/860101001

Руководителям предприятий, организаций
и учреждений осуществляющих
деятельность на территории
муниципального образования
город Ханты-Мансийск

09-Исх-1143
05.08.2024

Уважаемые руководители!

Информирую Вас, что на территории автономного округа продолжается широкомасштабная кампания по информированию жителей Югры о способах и схемах мошеннических действий, а также о способах их распознавания и защиты от действий преступников.

Несмотря на принимаемые меры, в настоящее время на территории города Ханты-Мансийска, не удается стабилизировать ситуацию и добиться снижения числа регистрируемых IT-преступлений.

В общем числе преступлений данной категории продолжают регистрироваться IT-преступления, совершенные в отношении работников и служащих учреждений, организаций и предприятий, осуществляющих свою деятельность на территории муниципального образования город Ханты-Мансийск.

С учетом изложенного предлагаю: организовать индивидуальное доведение до работников Вашего предприятия (организации, учреждения) актуальной информации о способах совершения мошенничеств и способах защиты от них;

Тематические фото, аудио и видеоматериалы, можно скачать по ссылке: **clck.ru/34u8ax.**

Приложение: на 6 листах, экз. ед.

Заместитель
Главы города

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 4FB87C304FE6A1F8FEDCACAF02ECCA58
Владелец: Боровской Геннадий Викторович
Действителен с 19.12.2023 по 13.03.2025

Г.В.Боровской

Исп. Федоров Евгений Юрьевич
Заместитель заведующего отдела по вопросам общественной
безопасности и профилактике правонарушений
Администрации города Ханты-Мансийска,
тел. 8(3467) 35-33-36 доб.2

Приложение к письму
от «____» августа 2024 №_____

**С какими мошенническими схемами
можно столкнуться в 2024 году
(данные МВД России)**

Мошенники стали запугивать россиян просрочкой по ипотеке

Новую схему преступников выявил ВТБ. Мошенники звонят клиентам от лица сотрудников банка и уверяют, что у них якобы возникла просрочка по кредиту. Чтобы ее урегулировать, жертв просят назвать номер СНИЛС и смс-код.

С этой информацией преступники могут получить доступ к "Госуслугам", а также зайти в онлайн-банк, чтобы украсть деньги или оформить кредит.

Вам пришла посылка из-за границы!

- говорит вам по телефону некто, представившись сотрудником "Почты России". И тут же сообщает, что нужно оплатить таможенный сбор.

Для того, чтобы отказаться от посылки, которую человек не заказывал, мошенники просят назвать код из sms. По их словам, это нужно, чтобы якобы подписать официальный отказ в базах почты.

Целью такой мошеннической схемы может быть получение доступа:

1. к банковскому мобильному приложению с тем, чтобы впоследствии украсть деньги со счета или взять кредит

2. к аккаунту на Госуслугах, где можно собрать персональные данные гражданина и использовать их для будущих схем "развода".

В преддверии периода подачи документов в вузы аферисты обманывают абитуриентов и их родителей.

Они создают фейковые сайты, страницы в соцсетях, где среди прочего предлагают «купить» бюджетное место в учебном заведении.

Мошенники умело убеждают своих потенциальных жертв «гарантиями» прохождения в престижные вузы, а также заманивают относительно привлекательной стоимостью «бюджетных» мест — в некоторых регионах она варьируется в пределах 20 тыс. рублей.

Приняв решение купить место в образовательном учреждении для ребенка, родитель рискует передать свои персональные данные мошенникам или потерять доступ к порталу «Госуслуги» и банковским приложениям. Это, в

свою очередь, приведет к дополнительным финансовым потерям и прочим проблемам.

Очередной вид мошенничества на маркетплейсах.

Аферисты взламывают личные кабинеты пользователей, оформляют заказы у фейковых продавцов и списывают таким образом средства с привязанных к чужим профилям банковских карт.

Не используйте однотипные пароли для разных сайтов и регулярно меняйте их.

Если есть возможность, можно подключить двухфакторную идентификацию. Тогда для входа в личный кабинет нужно будет вводить не только пароль, но и код, например, из SMS.

Также для расчетов в онлайн-магазинах можно завести отдельную карту и каждый раз переводить на нее сумму, необходимую для совершения покупки.

Как понять, что в смартфоне есть шпионское ПО?

Можно выделить несколько основных признаков, которые явно будут указывать на наличие постороннего вмешательства в смартфоне.

Например, телефон начинает жить своей жизнью: на него приходят различные уведомления о действиях, которые пользователь никогда не совершал, а во время разговора по телефону возникают характерные шумы и посторонние звуки.

Помимо этого, устройство может произвольно выключаться или перезагружаться, а также запускать некоторые функции, например микрофон или видеокамеру, открывать и закрывать различные мобильные приложения.

Вредоносное ПО чаще всего осуществляет сбор данных и отправляет их на серверы злоумышленников, что значительно увеличивает трафик и уменьшает скорость интернета.

На наличие вредоносного ПО в смартфоне будет указывать история, которая не отражает реальную пользовательскую активность.

Суть заключается в том, что шпионское программное обеспечение практически всегда будет записывать разговоры человека и сохранять информацию об посещённых сайтах. Поэтому, если в галерее есть множество скриншотов и видеороликов, которые человек не делал, а тем более если на этом контенте присутствует какая-либо личная информация, то велика вероятность, что смартфон был взломан мошенниками.

При обнаружении подобных признаков рекомендуется обратиться к специалистам для проверки гаджета на наличие шпионского и вредоносного ПО.

Телефонные аферисты начали применять в ходе новых атак несуществующую в стране «Единую медицинскую службу» для попыток получить доступ к аккаунтам пользователей на портале «Госуслуги».

В рамках реализации данной схемы злоумышленники на первом этапе звонят потенциальной жертве по телефону, представляются специалистами некой «Единой медицинской службы» и спрашивают человека о том, когда он последний раз проходил флюорографию.

В случае, если потенциальная жертва отвечает, что на процедуре он последний раз был в 2024-м году, мошенники удивляются и заявляют, что в базе данных указан только 2022 г., после чего для уточнения информации у человека просят продиктовать номер СНИЛС.

В том случае, если человек отказывается это сделать, мошенники начинают предлагать обновить данные с помощью портала «Госуслуги», для чего уже требуют предоставить код подтверждения из SMS-сообщения.

В том случае, если пользователь диктует этот код подтверждения злоумышленникам, то с его помощью киберпреступники могут компрометировать личный кабинет человека на портале и использовать этот доступ для проведения других мошеннических атак.

В течение последних нескольких месяцев фиксируется достаточно большое количество звонков телефонных аферистов якобы из ближайших поликлиник и больниц с предложением записаться на флюорографию или другие медицинские исследования. Мошенники в этом случае могут требовать от пользователей продиктовать номер СНИЛС и код из SMS-сообщения.

Ни в коем случае нельзя диктовать какие-либо свои персональные данные и тем более озвучивать коды подтверждения из SMS-сообщений, потому что ни одно российское ведомство и государственные структуры никогда не будут требовать от человека по телефону передать подобную конфиденциальную информацию.

Мошенники предлагают пересчитать пенсию из-за неучтенного трудового стажа.

Вместе с Социальным фондом России (https://t.me/sfr_gov) рассказываем о популярной уловке

Схема выглядит так:

1. Мошенники звонят пожилым людям и представляются работниками Социального фонда России (СФР).
2. Они сообщают, что размер текущей пенсии можно существенно увеличить, так как будто бы обнаружен неучтенный трудовой стаж.

3. Тех, кто поверил в легенду, приглашают якобы на консультацию в Многофункциональный центр или отделение СФР для решения вопроса. Причем мошенники называют настоящие адреса центров, которые находятся в городе, где живет потенциальная жертва. Это окончательно усыпляет бдительность человека.

По сценарию злоумышленников, для записи на прием человек должен сказать данные паспорта, СНИЛС, ИНН и озвучить код из смс. На самом деле эти данные нужны мошенникам для доступа к учетной записи человека на Госуслугах. Заполучив доступ к ней, они могут беспрепятственно оформить на жертву кредиты или займы.

Что делать, если вы или ваши близкие попали в такую ситуацию?

Первым делом прервите разговор. Настоящие сотрудники государственных служб, в том числе Социального фонда России, не звонят по подобным вопросам.

По любым социальным вопросам нужно самостоятельно позвонить в единый контактный-центр СФР по телефону 8-800-10-000-01, либо обратиться в ближайшее отделение фонда.

Никому и никогда не сообщайте личные данные, реквизиты карт, СМС-коды, а также логины и пароли от своих аккаунтов.

Объясните близким старшего возраста, что чаще всего незнакомцы, которые по телефону говорят о деньгах — это мошенники. Все вопросы, связанные с деньгами, лучше обсуждать в спокойной обстановке в семье.

Очередная мошенническая схема

Телефонные аферисты начали обманывать российских граждан с применением новой схемы, в рамках которой злоумышленники предварительно осуществляют сбор целого досье на потенциальную жертву.

В ходе таких атак преступники действуют группой, представляются сначала бывшими коллегами человека, после чего «сотрудниками ФСБ», ищущими «украинский след», и угрожают уголовными делами.

В ходе таких атак злоумышленники сначала представляются во время телефонного звонка или общения в мессенджере бывшим директором потенциальной жертвы. Этот лжедиректор заявляет человеку, что из-за некой утечки данных проводится негласная проверка организации со стороны ФСБ России. Для убедительности злоумышленники присылают фотографии поддельного документа с печатями и подписью действующего генерала ФСБ.

При этом на первом этапе злоумышленники заявляют, что никакие конфиденциальные данные предоставлять не надо, как и переводить деньги, тем самым, не вызывая никаких подозрений.

На втором этапе жертве звонит уже другой злоумышленник, который представляется «следователем ФСБ». Он задаёт человеку вопросы о

предыдущей работе и спрашивает, посещал ли он в последнее время территорию Украины.

После получения всех ответов «следователь» говорит о том, что с банковских счетов бывших сотрудников организации происходят переводы денег в пользу украинских вооружённых сил.

И для того, чтобы человек якобы не попал под уголовное преследование по делу о финансировании террористов и экстремистов, псевдо-сотрудник ФСБ предлагает ему выполнить перевод денег на «безопасный счёт».

При этом мошенник заявляет, что не стоит обращаться в отделение своего банка лично, потому что операция спецслужбы носит исключительно тайный характер.

В том случае, если жертву удаётся обмануть, денежные средства попросту оседают на подставных счетах, откуда они уже уходят на кошельки мошенников.

Мошенники снова обманывают россиян от имени сотрудников сотовых операторов.

На этот раз они сообщают о якобы произошедшем сбое, который привел к тому, что старый тариф был сброшен и более недоступен, а стоимость нового будет выше прежней.

Однако огорчаться не стоит. В ходе беседы аферисты (https://ria.ru/20240702/moshennichestvo-1956769467.html) предлагают абоненту «вернуть» старый тариф. Для этого нужно всего лишь предоставить им доступ к личному кабинету на ресурсе оператора.

Поступать так нельзя, потому что это поможет злоумышленникам завладеть конфиденциальной информацией абонента, чтобы использовать ее в будущем в незаконных целях.

Чтобы обезопасить себя от мошенников необходимо помнить о следующих основных правилах.

– сотрудники любого банка никогда не просят сообщить данные вашей карты (номер карты, срок её действия, секретный код на оборотной стороне карты), так как у них однозначно имеются ваши данные;

– не при каких обстоятельствах не сообщать данные вашей банковской карты, а так же секретный код на оборотной стороне карты;

– хранить пин-код отдельно от карты, ни в коем случае не писать пин-код на самой банковской карте;

– не сообщать пин-код третьим лицам;

– остерегаться «телефонных» мошенников, которые пытаются ввести вас в заблуждение;

– лучше избегать телефонных разговоров с подозрительными людьми, которые представляются сотрудниками банка, не бойтесь прервать разговор, просто кладите трубку;

– внимательно читайте СМС сообщения приходящие от банка;

– никогда и никому не сообщайте пароли, и секретные коды, которые приходят вам в СМС сообщении от банка;

– помните, что только мошенники спрашивают секретные пароли, которые приходят к вам в СМС сообщении от банка;

– сотрудники банка никогда не попросят вас пройти к банкомату;

– если вас попросили пройти с банковской картой к банкомату, то это очевидно мошенники;

– не покупайте в интернет – магазинах товар по явно заниженной стоимости, так как это очевидно мошенники;

– никогда не переводите денежные средства, если об этом вас просит сделать ваш знакомый в социальной сети, возможно мошенники взломали аккаунт, сначала свяжитесь с этим человеком и узнайте действительно ли он просит у вас деньги;

– в сети «Интернет» не переходите по ссылкам на неизвестные сайты;

– действуйте обдуманно, не торопливо, помните, что «Бесплатный сыр только в мышеловке».

Отдел по вопросам общественной безопасности и профилактики правонарушений Администрации города Ханты-Мансийска