Администрация Усть-Катавского городского округа Челябинской области

РАСПОРЯЖЕНИЕ

От 28.10.2024г. № 127-р

О профилактике мошенничества в администрации Усть-Катавского городского округа и подведомственных учреждениях

В связи с ростом преступных посягательств в отношении работников администрации Усть-Катавского городского округа и подведомственных ей учреждений, совершенных мошенническим путем с применением информационно-телекоммуникационных технологий (ИТТ), в целях повышения бдительности работников и их защищенности от негативных последствий в случаях преступных посягательств, руководствуясь Уставом Усть-Катавского городского округа,

1. Заместителям главы Усть-Катавского городского округа (С.В. Харитонову, А.П.Логиновой, Д.Н. Дьячковскому, Я.В. Гриновскому), руководителям структурных подразделений администрации Усть-Катавского городского округа (Е.В. Ивановой, О.А. Никулиной, И.В. Зуевой), управляющему делами администрации Усть-Катавского городского округа Т.В. Мировчиковой):

1.1. Ознакомится с профилактическими материалами по предупреждению и пресечению имущественных преступлений, совершаемых злоумышленниками с использованием ИТТ, представленными ОМВД России по Усть-Катавскому городскому округу.

1.2. Организовать ознакомление подчиненных работников под подпись с вышеуказанными профилактическими материалами, направив листы ознакомления работников в общий отдел администрации Усть-Катавского городского округа.

Срок исполнения: до 08.11.2024г.

2. Начальнику общего отдела администрации Усть-Катавского городского округа (О.Л. Толоконниковой) разместить профилактические материалы на официальном сайте администрации Усть-Катавского городского округа www.ukgo.su.

3. Настоящее распоряжение вступает в силу с момента подписания.

4. Организацию исполнения данного решения возложить на первого заместителя главы Усть-Катавского городского округа по вопросам социально-культурной политики, охране здоровья населения С.В. Харитонова.

5. Контроль за исполнением настоящего распоряжения оставляю за собой.

Исполняющий обязанности главы
Усть-Катавского городского округа С.В. Харитонов

Справка по IT-мошенничеству.

1) **Мошенники предоставляются работодателями:**

Злоумышленники рассылают по электронной почте, через СМС или мессенджеры сообщения с привлекательными условиями работы: высокой оплатой труда, неполным рабочим днем, легкими задачами. Зачастую это работа на маркетплейсах (продажа товаров и услуг через интернет). Для уточное деталей человеку предлагают перейти по ссылке, которая ведет в популярные мессенджеры.

Что предпринять?

Не доверяйте рассылкам с предложением о работе, тем более ели вас заставляют оплатить какие-либо услуги, товары, зарезервировать вакансию и провести другие платежи. Такие предложения «гарантированной работы»-популярный прием мошенников. Кроме того, при получении таких предложений о работе не сообщайте свои паспортные данные и финансовые сведения (данные карты и её владельца, трехзначный код с обратной стороны карты или СМС-код).

2) **Лжесотрудники Банка России:**

Банк России отмечает очередную волну широкого распространения мошеннической схемы, при которой злоумышленники предоставляются сотрудниками Центрального банка. Вначале мошенники звонят человеку и сообщают о сомнительных операциях, якобы совершаемых по счету или карте, после направляют ему в мессенджер или на электронную почту поддельное удостоверение сотрудника Банка России с логотипом и печатью. Такие документы могут содержать фамилии реальных работников-эти сведения злоумышленники могут брать с сайта регулятора. Высылая фальшивое удостоверение, они надеются убедить человека в правдоподобности своих недобросовестных действий, чтобы в дальнейшим лишить его денег или оформить на него кредит.

Что предпринять?

Банк России напоминает, что не работает с физическими лицами как с клиентами, не ведет их счета, не звонит им, а его сотрудники не направляют никому копии своих документов. При поступлении телефонного звонка от мошенника немедленно прервите разговор и по возможности заблокируйте его номер. При возникновении любых сомнений относительно сохранности денег на вашем банковском счете самостоятельно позвоните в свой банк по номеру, указанному на его официальном сайте или на оборотной стороне банковской карты.

3) **Представляются сотрудниками операторов мобильной связи:**

Злоумышленники звонят гражданам под видом сотрудников службы поддержки оператора сотовой связи и сообщают, что номер абонента скоро перестанет действовать. Чтобы избежать отключения номера, человеку предлагают набрать на мобильном телефоне определенную комбинацию цифр. Однако в результате абонент подключает

переадресацию звонков и текстовых сообщений, в том числе с СМС-кодами от банка, на номера мошенников. Это позволяет им получить доступ к дистанционному управлению банковским счетом и похитить деньги.

Что предпринять?

При поступлении такого телефонного звонка прервите разговор. Если вы продолжили общение и вам во время разговора пришел СМС-код от личного кабинета, никому не сообщайте его. Если возникли вопросы, самостоятельно позвоните в службу поддержки мобильного оператора по номеру, который указан на его официальном сайте.

4) **Предлагают перевести деньги на «специальный счет Центрального банка»:**

В последнее время злоумышленники часто звонят человеку с сообщением о том, что неизвестные лица пытаются похитить деньги с его счета и для сохранности средства нужно перевести на специальный (безопасный) счет в Центробанке.

Что предпринять?

Банк России не работает с физическими лицами как с клиентами, не ведет их счета и не совершает звонков гражданам. При поступлении такого телефонного звонка немедленно прервите разговор.

5) **Убеждают оформить кредит:**

Человеку звонят якобы сотрудник бюро кредитных историй и утверждает, что на него или его близких родственников мошенники пытаются оформит кредит. Через некоторое время ему снова звонят и уже могут представляться сотрудниками службы безопасности банка, правоохранительных органов или Банка России. Звонящий подтверждает, что на имя гражданина или его близких неизвестные лица действительно оформляют кредит и, чтобы предотвратить его незаконное оформление, необходимо как можно скорее оформить «встречный» кредит самостоятельно онлайн или в офисе банка. Сумма кредита должна совпадать с той суммой, которую оформляют неизвестные лица по его паспортным данным.

Что предпринять?

При поступлении такого телефонного звонка немедленно прервите разговор. Ни сотрудники банков, ни бюро кредитных историй не информируют граждан об изменениях в кредитной истории по телефону. Сообщить по телефону или каким-либо другим способам о попытке оформления кредита могут, как правило, только мошенники.