

ГУ МВД России по Пермскому краю

Межмуниципальный отдел Министерства внутренних дел Российской Федерации «Очерский» (Межмуниципальный отдел МВД России «Очерский»)

ул. Советская, 5, Очёр, 617140 тел/факс (34278) 3-17-88

Главе городского округа -главе администрации Очёрского городского округа А.В. Солодникову

Руководителям организаций и предприятий Очёрского городского округа

2508. 20.29	$N_{\underline{0}}$	10/20239
на №	OT	

В связи с увеличением количества обращений граждан Очёрского городского округа в органы внутренних дел по фактам мошеннических действий в сфере информационно — телекоммуникационных технологий, значительными суммами нанесённого ущерба, нарастающей динамикой регистрируемых уголовных дел по статье «Мошенничество» просим провести разъяснительную работу среди персонала с использованием предоставляемой информации.

«Осторожно! Мошенники!»

Схем, по которым злоумышленники регулярно совершают кражи и мошенничества с использованием информационно-телекоммуникационных технологий, достаточно много

Мошенничества от лже-операторов связи. Мошенники обзванивают граждан, представляются операторами связи и сообщают, что их абонентский номер не прошел подтверждение в системе и будет заблокирован. Для того чтобы пройти процедуру подтверждения, необходимо сообщить коды доступа к личному кабинету, которые будут приходить в виде смс-сообщений.

Когда мошенник получит доступ к вашему личному кабинету оператора связи, он автоматически получит полный доступ к другим мобильным приложениям, с помощью которых может похитить ваши личные сбережения и кредитные средства. Необходимо помнить, что абонентский номер — это инструмент аутентификации, с помощью которого вы регистрируетесь на различных ресурсах и управляете своими сбережениями.

Необходимо запомнить, что подтвердить персональные данные оформленного на вас абонентского номера можно в личном кабинете или в офисе оператора связи.

Нельзя никому сообщать коды доступа в личные кабинеты, таким образом. вы обезопасите себя, свои персональные данные и личные сбережения.

Преступники могут позвонить потенциальной жертве под видом сотрудника фонда социального страхования, любых других организаций. Они филигранно выманивают из собеседника персональные данные, коды доступа и

пароли, которыми потом пользуются противоправно. Получают доступ к личным кабинетам порталов и сервисов. Единственное верное решение в такой ситуации – прекратить разговор с преступником.

Еще одна из популярных схем телефонных мошенников — «Ваш родственник попал в беду». Звонок поступает на стационарный телефон. Мошенник представляется либо сотрудником силового ведомства, либо медицинским работником, либо адвокатом. Сообщает, что близкий человек абонента совершил какое-либо противоправное деяние, а для решения проблем немедленно необходимы деньги. Чаще всего на такие уловки попадаются пожилые люди. Отзывчивые пенсионеры отдают неизвестным все свои сбережения.

Чтобы не стать жертвой мошенников, никогда не доверяйте телефонным незнакомцам, кем бы они ни представились, не поддавайтесь панике и никому не передавайте наличные денежные средства и не совершайте онлайн-переводов. В данной ситуации необходимо связаться с близким человеком и рассказать о произошедшем.

В случаях, когда вам звонят, представляясь сотрудником службы безопасности банка, называют ваши персональные данные, сообщают о том, что по вашей карте происходят подозрительные операции и ваша карта заблокирована, просят назвать данные карты, трехзначный код или перевести все денежные средства на безопасный счет, созданный банком. Это мошенники! Не спешите производить действия по инструкции звонящего. Прекратите разговор. Перезвоните в свой банк по номеру телефона, который указан на обратной стороне карты. Убедитесь, что ваши сбережения в порядке.

Когда вам звонят, якобы сотрудники различных правоохранительных органов, называют ваши персональные данные, сообщают о том, что мошенники оформили на ваше имя кредит и в отношении вас по запросу Банка возбудили уголовное дело. Предлагают провести допрос по телефону, за отказ в содействии или разглашении диалога грозят уголовной ответственностью. Просят принять участие в выдуманной операции по изобличению преступников, после поимки которых все затраты будут компенсированы с доплатой. Сообщают о том, что с вашими картами прямо сейчас работают несколько мошенников и нужно срочно выводить деньги на безопасный счет, который сейчас вышлют абоненту. Это мошенники! При поступлении таких звонков сосредоточьтесь, уточните данные должностного лица звонящего, после чего прекратите диалог. Важно помнить, что кем бы ни представился позвонивший вам незнакомец, не следует поддаваться страху. Перезвоните в интересующий вас орган по номерам телефонов указанных только на официальных сайтах структур.

Мошенничества под предлогом взлома личного кабинета в госуслугах. Аферисты для совершения указанного мошенничества часто используют мессенджеры. Потерпевшему поступает звонок и он видит логотип сайта госуслуг. Мошенник сообщает, что личный кабинет гражданина пытаются взломать. Для того, чтобы обезопасить себя, необходимо предоставить доступ в личный кабинет. Как только потерпевший предоставляет доступ, мошенники оформляют на него кредиты в микрофинансовых учреждениях.

Для защиты от указанного мошенничества необходимо запомнить следующие правила:

- Сотрудники госуслуг не осуществляют звонки при подозрительных операциях в личном кабинете. Они его просто его блокируют.
- Сотрудники госуслуг не просят сообщить конфиденциальную информацию о вас и не просят сообщить коды доступа в личный кабинет.

Если все же Вы попались на уловки мошенников, необходимо обратиться в службу поддержки госуслуг для смены пароля для входа в личный кабинет. Далее через портал госуслуг запросить историю кредитования. При получении ответа и обнаружении оформленных кредитов, обратиться в микрокредитные организации для отмены кредитов, сообщить в полицию.

«Уникальная возможность заработка!» С таких объявлений в сети Интернет начинается ещё один вид мошенничества. Многообещающее предложение большой прибыли за короткий срок привлекает многих граждан. Заполнив анкеты, предоставив свои контактные телефоны, получив инструкции. граждане берут кредиты, делают ставки якобы на бирже или букмекерской компании, вносят средства якобы в инвестиционные компании, проводят якобы операции с криптовалютой и ожидают лёгкого приумножения средств, теряя собственные и заёмные деньги.

Сотрудники полиции рекомендуют гражданам настороженно относиться к заманчивым предложениям о крупных заработках в сети Интернет, не переходить по подозрительным ссылкам и не скачивать незнакомых приложений. Проверить инвестиционную площадку на ее подлинность и наличие лицензии на официальном сайте Центрального банка Российской Федерации. Инвестирование — всегда рискованная деятельность.

Будьте бдительны! Не позволяйте себя обмануть!

Начальник

А.В. Мокрушин