На территории Оренбургской области участились случаи хищения денежных средств со счетов граждан.
УМВД России по Оренбургской области предупреждает,
будьте бдительны, не дайте себя обмануть!

1. Хищение под предлогом предотвращения несанкционированного списания денежных средств, несанкционированного оформления кредита, блокировки банковской карты, сохранения денежных средств на резервном счёте.

Преступники представляются сотрудниками Центробанка, ФСБ, МВД и вводят жертву в заблуждение, сообщая о подозрительных операциях со счетами либо о попытках оформления кредитов. Злоумышленники могут прислать выписки из банка, удостоверения и другие документы с печатями. В итоге предлагают обналичить со своих счетов имеющиеся сбережения либо в отделении банка подать новую заявку на кредит (для отмены предыдущей), и впоследствии просят перевести денежные средства на «безопасный» счет.

2. Хищение посредством телефонного звонка под видом покупателя либо продавца по размещённому объявлению на торговых площадках сайтов «Авито», «Юла» и т.п.

Преступник вводит жертву в заблуждение поясняя, что в связи с нахождением за пределами Оренбургской области лично передать деньги не может и предлагает осуществить сделку дистанционно. Для этого, как правило, лица переходят для общения в мессенджеры, чаще «WhatsApp», договариваются о получении (отправке) товара с помощью служб доставки (Avito – доставка, CDEK, Boxberry и т.п.), преступники скидывают интернет – ссылку на фишинговые (поддельные) сайты, где жертва вносит реквизиты банковской карты.

3. Хищение посредством телефонного звонка под предлогом выдачи кредитов (займов).

В данной ситуации, до совершения преступления, потерпевший самостоятельно находит предложения в интернет среде о предоставлении кредита, перейдя на фишинговый сайт, оставляет свои контакты. Злоумышленник, под видом работника кредитного учреждения, связывается с жертвой, выманивает реквизиты карты под предлогом оплаты комиссии и распоряжается деньгами через подконтрольные банковские счета.

4. Хищение с использованием «фишинговых сайтов» в сети Интернет.

Как правило это «двойники» сайтов продаж авиабилетов, сайтов интернет - магазинов бытовой техники, электрооборудования и электроинструментов. Различаться такие сайты от настоящих могут в одну букву или цифру. Доменные имена таких сайтов обычно зарегистрированы за пределами РФ.

5. Хищение с использованием сети Интернет в социальных сетях («Одноклассники», «ВКонтакте», «Инстаграм»), в том числе путём взлома страниц.

В этой ситуации прослеживается закономерность: в «Одноклассниках» жертвами становятся лица пожилого возраста, предлогом является мнимая выплата всякого рода компенсаций (НДС, доплаты к пенсии и т.п.). Во «Вконтакте» злоумышленником взламывается страница связей потерпевшего и от их имени путём переписки запрашиваются деньги в долг, с указанием реквизитов банковской карты. В социальной сети «Инстаграм» распространены так называемые интернет – страницы продаж вещей, где под видом сделки преступники завладевают реквизитами банковских карт либо вынуждают внести предоплату за товар и не исполняют своих обязательств.

6. Хищение посредством телефонного звонка, под предлогом освобождения родственника от уголовной ответственности.

7. Схема «руководитель». Жертвам мошенников поступают звонки и сообщения в мессенджерах от лица действующих или бывших руководителей. Далее с потерпевшими связываются сотрудники различных государственных структур и сообщают о попытках хищения денежных средств либо о необходимости оформления кредитов, с целью дальнейшего их перевода на «безопасный» счет.

Весь спектакль с привлечением руководителя нужен злоумышленникам, чтобы вызвать доверие к озвученной информации. Аферисты заранее готовятся к обману и используют утечки баз данных и другие сведения, находящиеся в открытом доступе, с целью реализации персонализированного сценария атаки, вызывая минимум подозрений у жертвы.

8. «Истекает срок действия сим-карты». Жертве мошенников поступает телефонный звонок от имени сотрудника оператора связи, который сообщает об окончании срока действия абонентского договора, и что для его продления необходимо продиктовать код из смс-сообщения,

С помощью кода преступники получают доступ к номеру жертвы, а следовательно, к личному кабинету банковских приложений, Госуслуг и других сервисов. Помните, что договор с оператором связи бессрочный!

9.Хищение денежных средств под предлогом дополнительного заработка в различных маркетплейсах («Озон», «Вайлдберриз», «СберМегаМаркет» и т.д.). *В сети Интернет потерпевшим предлагают заработок в сфере торговли товара и оказания услуг.*

10.Хищение денежных средств под предлогом инвестирования. Часто для обмана мошенники создают сайты, которые сложно отличить от настоящих сайтов брокерских компаний. Прежде всего в таких предложениях должна насторожить высокая доходность.

Первый шаг этой схемы – заставить человека зарегистрироваться на сайт. Второй – пополнить виртуальный счет, то есть перевести деньги. Иногда, чтобы вызвать доверие, жертве действительно поступает на карту небольшая сумма – якобы дивиденды с акций. Если человек пытается вывести вложения или откажется инвестировать больше, мошенники стараются давить сильнее: рисуют перспективы обогащения, предлагают взять кредит и продать имущество ради быстрого заработка.