

## **Берегите свои деньги. Свердловское МВД предупреждает - активизировались кибермошенники**

Современные мошенники сродни клещам. Одни жаждут крови, а другие — чужих денег, причем любым способом. За первые три месяца 2021 года в Свердловской области жертвами различного рода аферистов стали 1644 уральца. Региональный главк МВД призывает граждан быть более бдительными и внимательными. Как сообщил пресс-секретарь ГУ МВД области Валерий Горелых, в сети злоумышленников угодили люди разных профессий и возрастов. Среди них есть доценты, сотрудники правоохранительных органов, финансовых учреждений, геологи, врачи, педагоги, пенсионеры и другие. Что характерно, многие из них знали о существовании мошенников, но те, словно, профессиональные гипнотизеры все равно их обманули.

«Прошу запомнить основные методы, которыми пользуются преступники. Вам могут позвонить и сообщить, что кто-то из родных совершил ДТП. А для того, чтобы избежать тюрьмы, потребуют крупную сумму денег. Свяжитесь с близкими и проверьте насколько эта информация соответствует действительности. Вам могут сказать, что необходимо снять порчу. Старая, но по-прежнему действующая схема обмана. Возможно запугивание взломом вашего банковского счета, проведением «подозрительных операций» с ним, оформлением кредита без ведома владельца счета. Могут попросить продиктовать по телефону реквизиты банковской карты, пин-коды из смс сообщений, CVV коды с обратной стороны карты. Могут напугать «компьютерной атакой» на телефон, предложить установить специальное приложение для защиты. Аферисты могут представляться сотрудниками любых правоохранительных ведомств, могут звонить с подменных телефонных номеров идентичных реальным государственным ведомствам и так далее. Напоминаю, что спецслужбы и банковские операторы никогда не звонят напрямую владельцам счетов. В таких ситуациях необходимо положить трубку и самостоятельно позвонить в банк или полицию. Если этого не сделать, можно легко оказаться в ситуации наподобие той, в какой недавно оказался житель Екатеринбурга, 1983 года рождения. Ему поступил звонок, якобы, от службы безопасности банка о том, что необходимо пройти процедуру переактивации счета из-за угрозы мошенников. Послушавшись советов «доброжелателей», мужчина оформил кредиты на сумму шесть миллионов рублей и лично перевел их аферистам, а когда понял, что его обманули, обратился за помощью в полицию», - рассказал полковник Горелых.

**Не повторяйте чужих ошибок. Посмотрите внимательно видеоролики, направленные на профилактику обмана людей, перешлите ссылки своим друзьям, знакомым и близким, в том числе пожилым людям. Помните, известное выражение: «Предупрежден — значит вооружен».**

# ОСТОРОЖНО: МОШЕННИКИ! НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!



## ИНТЕРНЕТ-МОШЕННИКИ

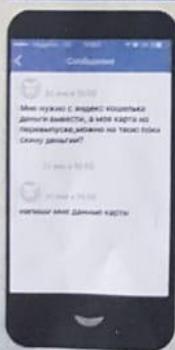
### ОБЪЯВЛЕНИЕ О ПРОДАЖЕ



Мошенники-продавцы просят перечислить деньги за товар, который впоследствии жертва не получает.

### ОБЪЯВЛЕНИЕ О ПОКУПКЕ

Мошенники-покупатели спрашивают реквизиты банковской карты и (или) смс-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.

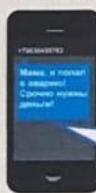


### СООБЩЕНИЯ ОТ ДРУЗЕЙ

Мошенник пользуется чужой страницей в социальной сети в Интернете, и под видом друга (родственника) просит перечислить ему деньги или сообщить данные Вашей карты якобы для перечисления Вам денег под различными предлогами.

## ТЕЛЕФОННЫЕ МОШЕННИКИ

### ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ



Мама, я попал в аварию!

### БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

Сообщение о блокировании банковской карты с номером, по которому нужно позвонить. Цель – узнать личный код банковской карты.



### ПОЛУЧЕНИЕ ВЫИГРЫША (компенсации за потерянный вклад)

Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.п. Жертве можно забрать его, заплатив налог или плату якобы «за сохранность денег».



### ВИРУС В ТЕЛЕФОНЕ

Мошенники запускают вирус в телефон, предлагая пройти по «зараженной ссылке» (в том числе и от имени друзей). С помощью вируса получают доступ к банковской карте, привязанной к телефону. Установите антивирус и не проходите по сомнительным ссылкам.