**https://proregion24.by/news/society/kak-v-grodnenskom-rajone-kibermoshenniki-razvodyat-na-dengi/**

**Кибермошенники больше не представляются работниками банков. Теперь они используют новые способы обмана доверчивых граждан. О наиболее популярных «Перспективе» рассказал руководитель группы по противодействию киберпреступности Гродненского РОВД Константин Дедов.**

В последнее время злоумышленники особенно активизировались на популярной торговой интернет-площадке Kufar. С начала года таким образом на их удочку попались уже одиннадцать жителей Гродненского района.

*– Схема такова: предположим, человек решил что-то продать, подал объявление, указав в нем номер своего телефона. Мошенник пишет, как правило, с таких мессенджеров, как Telegram или WhatsApp. Договариваются о сделке. Для того чтобы якобы оплатить покупку, покупатель присылает продавцу ссылку, чтобы ему было проще перевести деньги на карту. Как только человек переходит по ссылке, вводит реквизиты банковской карты для перечисления платы за товар, все средства со счета исчезают, –*рассказывает Константин Валерьевич.

Таким образом люди лишались крупных денежных сумм – от одной до двух тысяч рублей. Но даже не это самое страшное, замечает собеседник. Вдобавок мошенники могут оформить денежный займ на имя владельца карты по программе Трейд-ин. Константин Дедов приводит в пример недавний случай. Жительница Гродненского района хотела продать на Kufar спортивный костюм, но нарвалась на недобросовестного покупателя. Перешла по той самой злополучной ссылке, ввела реквизиты банковской карты и… стала обладательницей кредита на сумму 5 777 рублей.

Вот почему нельзя давать данные даже той карты, на которой нет средств или если ей давно никто не пользуется, предостерегает Константин Дедов. У злоумышленников есть запасной вариант: они пополняют баланс двумя с половиной рублями, разблокируют карту и оформляют через нее денежный займ.

Если раньше самый популярный развод на деньги начинался со звонка псевдосотрудников банка, то сейчас мошенники чаще представляются работниками интернет-магазинов. Они звонят с неприятным известием, мол, на ваше имя оформили покупку в кредит. И предлагают «помощь»: рекомендуют… взять новый кредит, чтобы остановить старый. К сожалению, люди слишком доверчивы и идут на поводу у мошенников.

Осторожность следует проявлять и с интернет-банкингом, советует Константин Дедов. Некоторые и не подозревают, что могут попасть на фейковую страницу, созданную мошенниками. Человек через Google заходит в интернет-банкинг, не обратив внимания, что адрес в строке поиска отличается всего одной буквой. Введя логин и пароль, на экране появляется сообщение: «По техническим причинам сайт временно не работает, зайдите позже». А позже денег на счету уже нет. В Гродненском районе уже зафиксировано четыре подобных случая.

Конечно, обойтись в наше время без интернет-банкинга вряд ли возможно. Но собеседник рекомендует проявлять предельную внимательность и выбирать для использования исключительно мобильное приложение банка.

Киберпреступники постоянно повышают уровень своего профессионализма, не устают изобретать новые способы хищения средств, отмечают в милиции. Кто-то лишается средств, продавая игровой аккаунт в сети. А в конце прошлого года мошенники активизировались в сфере

недвижимости. Публикуют в интернете объявление об аренде квартиры по приятной цене и просят перевести 50 рублей в качестве залога.

*– Сумма на первый взгляд небольшая, но за день набегает до 15 тысяч, –*рассказывает собеседник.

Практика показывает, что на удочку кибермошенников попадаются люди разных профессий и возрастов. И если раньше в зоне риска были пожилые граждане, то сейчас – молодежь и люди среднего возраста, которые чаще пользуются услугами интернет-магазинов, продают товары в интернете. Так как все-таки уберечься от киберпреступников?

*– Советы просты: никому не сообщайте данные своей банковской карты, тем более трехзначный код. Не переходите по сомнительным ссылкам, будьте бдительны при совершении покупок или продаже товара на популярной интернет-площадке Kufar. И помните, что никто, а тем более банковские работники, не может просить у вас назвать реквизиты карты и личные данные. Если подозреваете, что звонят мошенники, игнорируйте их, сразу прекращайте разговор. А то некоторые потом горько вздыхают, мол, со мной так вежливо, убедительно беседовали,*– советует собеседник.

Сотрудники Гродненского РОВД проводят системную целенаправленную профилактическую работу по кибербезопасности. Но граждане, к сожалению, не всегда проявляют бдительность, а потом расплачиваются за чрезмерную доверчивость своими сбережениями.