УМВД России по Приморскому краю предупреждает: в регионе увеличивается количество случаев телефонного и интернет-мошенничества.

В прошлом году мошенники слили в интернет втрое больше записей с персональными данными, чем годом ранее.

Мошенники получают доступ к онлайн-банкам, а затем увеличивают лимиты перевода средств, чтобы украсть побольше денег. Чтобы заполучить доступ к приложению банка, они звонят и представляются сотрудниками госорганов или кредитных организаций, убеждая жертву, что на нее оформляют кредит. После того, как человек меняет доверенный номер телефона, аферисты получают необходимую информацию. Для защиты рекомендуется проверять историю входов в учетную запись приложения. А при возникновении сомнений блокировать учетную запись или карту. Также следует настроить лимиты перевода средств. Не сообщайте незнакомым людям данные карты, не сообщайте коды, которые приходят в смс, не совершайте манипуляции со своими картами или счетами под диктовку незнакомых лиц.

Еще одна схема аферистов – кража с помощью сервиса снятия наличных через QR-код. Такую функцию предоставляют некоторые банки. Клиент может сгенерировать код в приложении и поднести его к сканеру банкомата, чтобы снять деньги. Для кражи, мошенники звонят под видом сотрудников банка и заявляют, что заметили «несанкционированный запрос на снятие наличных». Для, якобы, отмены операции они просят QR-код, с помощью которого, воруют деньги. Чтобы обезопасить себя, не стоит делиться QR-кодом с другими людьми и хранить его электронное или распечатанное изображение.

Также с обманом можно столкнуться в соцсетях и мессенджерах. Пользователю обещают закрыть ипотеку за три месяца или выйти на стопроцентный доход с помощью криптовалюты. Иногда мошенников могут рекламировать даже каналы с большой аудиторией. Чтобы выглядеть убедительно, аферисты публикуют скриншоты с положительными отзывами или фейковые доказательства высоких доходов. При возникновении сомнений нужно поискать отзывы в интернете о канале или группе в соцсети. Можно попросить у администратора сообщества лицензию или документацию, чтобы подтвердить законность его деятельности. Не стоит сообщать свои данные и авторизироваться с помощью своих аккаунтов в соцсетях и мессенджерах на подозрительных сайтах.

Еще об одном способе нажиться на россиянах с помощью telegram-канала рассказали в Центробанке. Злоумышленники взламывают каналы популярных блогеров и используют в своих целях. Когда автору удается вернуть контроль над ресурсом, мошенники пишут пострадавшим

подписчикам от имени канала AntiSCAM и предлагают вернуть деньги за комиссию. Аферисты придумали, как украсть информацию с помощью маркетплейсов, таких как Wildberries и Ozon. Они просят подтвердить доставку, чтобы получить данные для входа, тогда как маркетплейсы не запрашивают такое подтверждение. Чтобы не стать жертвой, не стоит сообщать коды из СМС, пароли и логины «сотрудникам маркетплейсов». Вместо этого стоит позвонить на официальный телефон поддержки сервиса. Также в качестве дополнительной защиты можно пользоваться приложением.

Если вы попались на такую удочку, то стоит завершить текущие сеансы и зайти на маркетплейс с доверенного устройства, затем нужно поменять пароль от личного кабинета и электронной почты. Также стоит следить за банковскими операциями по карте, которая привязана к сайту. При приобретении товара через сайт объявлений, оплачивайте покупку по факту её получения.

В Амурской области и Санкт-Петербурге пользователи интернета столкнулись с необычным способом кражи данных. Они получили электронные письма с повесткой в военкомат от несуществующего госоргана «Главное управление военного комиссариата МО РФ». При этом в повестке не было указано, кому он адресована. Также к письму был прикреплен файл, в котором якобы был оригинал повестки. Этот документ содержал вирус, крадущий персональные данные.

В любой ситуации сохраняйте бдительность и критическое мышление, не позволяйте мошенникам обманывать вас! Если вам позвонил неизвестный и сообщил, что ваша карта заблокирована, ваш внук попал в беду, вы выиграли машину, предложил приобрести чудодейственные таблетки, представился сотрудником банка, полиции или дальним родственником, прервите разговор и позвоните в полицию по телефонам **02,102.**

Телефон Дежурной части Управления МВД России по Приморскому краю **8 (423) 249-04-91**.

Пресс-служба МО МВД России "Лесозаводский"