**Мошенники придумывают новые способы обмана**

Банк России фиксирует новые мошеннические схемы для хищения денег с банковских счетов. При этом преступники активно используют тему коронавирусной инфекции. Мошенники обзванивают граждан, обещая отсрочки по выплате кредитов, разного рода компенсации, пособия, возврат денег за авиационные билеты, услуги по медицинской диагностике нового вируса и многое другое.

Под тем или иным предлогом, используя методы социальной инженерии, преступники вынуждают людей сообщить данные карты или самостоятельно перевести деньги на счет мошенников, установить приложение, которое позволяет злоумышленникам удаленно управлять смартфоном или компьютером жертвы. В сети появляются фирмы-однодневки, которые обещают решить любые вопросы с прощением банковских кредитов, а также предлагают продажу поддельных справок и больничных листов с отметкой о коронавирусе.

Мошенники могут позвонить, представившись, например, сотрудниками авиакомпании, и попросить сообщить данные банковской карты, якобы для возврата платы за отмененный рейс. Действительно, плата за "сгоревшие" авиабилеты должна быть возвращена гражданам, именно на знание об этом и рассчитывают мошенники. Однако для официального возврата средств вовсе не нужно никому сообщать данные карты или счета: деньги вернутся на карту, с которой вы платили. Особенно должно насторожить предложение сообщить три цифры с обратной стороны карты. Всегда внимательно проверяйте ссылку, по которой собираетесь кликнуть: не перепутаны ли буквы в названии сайта. Если с написанием что-то не так, это верный признак, что мошенники подсовывают вам поддельную страницу.

Для того чтобы выманить у граждан данные банковских карт и убедить человека открыть вложение или перейти по ссылкам на зараженные сайты, мошенники часто подделывают бренд и фирменный стиль авторитетных организаций (Министерства здравоохранения, Роспотребнадзора, Банка России, Всемирной организации здравоохранения и других). У владимирцев есть риск попасть на фишинговые сайты, предлагающие популярные медицинские товары: маски или другие защитные средства. Всегда проверяйте адресную строку сайта, если перед адресом вы не видите префикс https (где «s» означает secure — безопасное) и знак закрытого замочка, то лучше этот сайт покинуть и совершенно точно не оставлять здесь свои данные. Приобретая товары в незнакомом вам прежде интернет-магазине, проверьте прежде добросовестность продавца по отзывам, которые легко найти в интернете. Как правило, недобросовестные торговцы уже успели где-то "оставить след".

Сейчас в особой группе риска перед атаками мошенников - пенсионеры. Злоумышленники под видом волонтёров пытаются разузнать, где пожилые люди хранят деньги. Они предлагают свои услуги и просят внести скромную предоплату. Или же просто спрашивают данные карты, на которую как бы необходимо перевести деньги от имени какой-нибудь несуществующей госпрограммы по поддержке пенсионеров на самоизоляции. Появилась еще новая схема — «спасение» сбережений пенсионеров от девальвации рубля. Мошенники звонят под видом сотрудников банка и обманом выуживают у пожилых клиентов конфиденциальные данные для доступа к их картам и онлайн-банку.

"В сегодняшней ситуации нужно обязательно перепроверять любую информацию, особенно ту, которую сообщают вам незнакомые люди. Стоит насторожиться, если вам звонят с предложением льгот и каких-либо компенсаций от государственных программ, при этом требуя ваших незамедлительных действий. Например, продиктовать данные своей банковской карты, или пароли из СМС-сообщений. Обязательно прерывайте такой разговор и перезвоните в организацию, от имени которой был совершен звонок, самостоятельно, - подчеркивает эксперт Отделения Владимир Банка России Евгений Гаврилюк. – Стоит иметь в виду, что тема вируса может быть использована злоумышленниками на всем протяжении эпидемии, при этом возможно появление новых приемов введения людей в заблуждение, поэтому будьте особенно внимательны и осторожны».