Как уберечь свои деньги.

Мошенники обзванивают наших земляков, представляясь службой безопасности известных банков. Они сообщают, что произошла утечка личных данных из-за якобы мошеннических атак, либо кто-то по доверенности пытался оформить на имя предполагаемого потерпевшего кредит.

Свою потенциальную жертву они запугивают, говоря, что от его или ее имени были поданы заявки в различные банки на оформление кредитов, и чтобы отменить их, необходимо удаленно подключить "защиту" - сотрудника технического отдела банка. Рассмотрим данную схему подробнее.

Злоумышленники, к примеру, просят клиента перейти в «PlayMarket» или «AppStore» и в поисковике набрать слово "поддержка". "Появится красное приложение с белым ромбиком, называется «AnyDesk» (либо приложение с синим квадратиком «RustDesk»), нажимаете на него и устанавливаете. Это наше официальное приложение по борьбе с мошенничеством", - говорят мошенники:

«AnyDesk» **«RustDesk»**

Если выполнить все инструкции мошенников-социальных инженеров и после установки вышеуказанных приложений сообщить код, который Вам придет в установленном приложении, либо ввести в нем код, который Вам сообщат мошенники, то шанс остаться без средств на банковских счетах и с "чужими" кредитами возрастает многократно, потому что киберпреступники с помощью приложения «AnyDesk»(«RustDesk») могут удаленно подключиться к любым устройствам и получить полный доступ к онлайн-банкингу и вообще к мобильному устройству.

"Как правило, преступники будут звонить и сообщать об обнаруженной ими проблеме с компьютером или интернетом, возможно мессенджером, после чего предлагать свою помощь. Они скорее всего будут заявлять, что работают на широко известную компанию, например «Viber», или даже на ваш банк.

Никогда не верьте этим людям, если вы не ожидали звонка!

Не верьте в предложенную "помощь", о которой вы не просили!

Ни один банк или компания не будут просить вас по телефону скачать программное обеспечение.

Если кто-то, удаленно подключившись к вашему устройству, просит предоставить имя пользователя для банковской учетной записи или показать личные пароли, он наверняка является мошенником. Не следуйте их инструкциям! Даже если они говорят, что все сведения, которые они Вам сообщили являются банковской тайной, и за ее разглашение третьим лицам (даже сотрудникам милиции), Вы будете привлечены к уголовной ответственности, не верьте им. Если вы чувствуете дискомфорт или опасность:
прервите телефонный звонок, просто положив трубку!".

Многие думают, что стоит прервать сессию удаленного доступа, просто выключив устройство, и тогда мошенники не смогут получить доступ к онлайн-банкингу. Однако киберпреступники за считанные секунды могут считать все данные с телефона пользователя и перенести их на свое устройство. Также мошенники с помощью программ удаленного доступа могут завладеть другой важной информацией: паролями в аккаунты пользователя, в электронную почту, контактами и прочее. Или же они могут "внедрить" в гаджет своей жертвы шпионские программы, которые будут передавать им важные сведения, включая SMS-коды и коды в Push-уведомлениях.

Вернуть деньги, украденные с помощью социальной инженерии, сложно, но попытаться стоит. Так, если вы стали жертвой мошенников, то обязательно:

- удалите приложение AnyDesk или его аналоги со своего гаджета. Поскольку вы сами не сможете обнаружить в своем устройстве шпионские приложения, то лучше покажите его проверенному IT-специалисту, либо сотруднику милиции;
- обратитесь в банк, в котором вы обслуживаетесь, сообщите о случае мошенничества и попросите заблокировать платежные средства, к которым злоумышленники могли получить доступ;
- позвоните по телефону **141** и выясните, не оформляли ли на Ваше имя заявки на оформление кредитов в банках, функционирующих на территории Республики Беларусь, при необходимости, заблокируйте свою учетную запись в данном сервисе;
- обратитесь с заявлением в милицию.

Соблюдайте простые правила безопасности, чтобы не потерять свои персональные данные:

Правило №1. Никогда не предоставляйте незнакомым лицам доступ к своим устройствам и не скачивайте никакие приложения на свой гаджет;

Правило №2. Никогда не делитесь ни с кем паролями к онлайн-банкингу или другой персональной и платежной информацией.