Будьте бдительны! Мошенники опробовали новые схемы обмана пользователей банков и соцсетей

1. Звонок от "оператора". Мошенники представляются операторами популярных сотовых компаний, их цель - получить паспортные данные жертвы. Если пользователь отказывается предоставить информацию, фейковый оператор угрожает отключением связи. Полученные данные в дальнейшем могут использоваться для получения кредитов.

Сценарий новой схемы опасен своей реалистичностью: жертва верит, что может лишиться связи. Мошенники ссылаются на положения, в соответствии с которыми оператору необходимо проверить личность абонента, и начинают уверенно перечислять все те неудобства, с которыми может столкнуться человек, если сейчас же не предоставит информацию - необходимость личной явки в офис, заполнение документов, ограничение услуг связи или даже блокировка sim-карты.

Самые вероятные риски для жертвы, данными которой завладели, - на ее имя могут оформить микрокредит или фирму-однодневку.

2. Фиш-хейт. Мошенник создает закрытый аккаунт в Instagram. По профилю видно, что аккаунт принадлежит девушке. Для привлечения внимания к своей странице мошенник оставляет оскорбительные комментарии к постам пользователей Instagram. Доверчивые пользователи, заинтересовавшись, кто оставляет им подобные комментарии, пытаются выяснить личность недоброжелателя. Жертвы переходят по ссылке из профиля и вводят свои логин и пароль для аутентификации на подставном сайте, напоминающем популярные социальные сети.

Таким образом, мошенник, используя методы социальной инженерии, получает контроль над аккаунтами невнимательных пользователей социальных сетей.

Ссылка, которую оставляет злоумышленник на своей странице, напоминает уникальный ID пользователя соцсетей. А фишинговый контент доступен только при переходе по ссылке из поддельного профиля мошенника в Instagram.

3. "Банкиры"-сказочники. Мошенники, которые звонят от лица банковских сотрудников, придумали новую легенду для обмана клиентов кредитных организаций. Злоумышленники говорят, что на рассмотрении банка находится заявление о смене номера для получения пуш- и смс-уведомлений по карте. Таким образом они запугивают клиента для дальнейшего выуживания данных по "пластику" (номер, срок действия, имя держателя, CVV-код).

Полученная информация в дальнейшем используется для вывода денег с карты. Опасность заключается в продолжении беседы. Есть риски, что начнется что-то вроде "для отмены заявления назовите свое кодовое слово...".

Поэтому вне зависимости от контекста беседы, если не вы звонили, никаких данных называть нельзя. Если очень хочется, то узнать, по какому добавочному можно связаться с сотрудником для решения вопроса и перезвонить самостоятельно. Нельзя принимать возражения вроде "мы работаем только на исходящих звонках".

В крайнем случае надо не полениться дойти до отделения банка и прояснить ситуацию. Да, неудобно, но когда речь идет о сохранности денег, приоритет лучше отдать безопасности, чем удобству".

Для того чтобы не стать жертвой мошенника, необходимо помнить, что никогда и ни в коем случае нельзя сообщать незнакомым людям, кем бы они ни представлялись, либо вводить на сомнительных ресурсах данные банковской карты, коды из СМС, секретные слова, а также не сообщать другие персональные данные, в том числе логины и пароли

от страниц в соцсетях. Нельзя переводить деньги куда бы то ни было по указанию незнакомых людей. Не стоит вступать в разговор с неизвестными и разглашать персональные данные.

Отделение полиции по Сямженскому району