## 1. Мошенничество с QR-кодами.

Мошенники выманивают QR-коды банковских операций, используя их для снятия денег со счетов. Также злоумышленники размещают в общественных местах поддельные QR-коды, которые ведут на фишинговые сайты, где они выманивают персональные данные и информацию о банковских счетах.

Чтобы не стать жертвой мошенников, эксперты рекомендуют использовать только динамические QR-коды, которые создаются специально для конкретной транзакции. При использовании бумажных QR-кодов следует уточнить у кассира или официанта, действителен ли он, и убедиться, что код не наклеен поверх другого.

Фишинговые сайты часто используют незащищенное соединение или поддельные сертификаты безопасности, поэтому перед вводом платежных данных необходимо убедиться в подлинности сайта и наличии безопасного соединения HTTPS.

Злоумышленники также используют чат-боты в популярных мессенджерах, чтобы создать впечатление работы официального автоматизированного сервиса. Они предлагают различные социальные выплаты и льготы, студенческие стипендии и пособия для семей с детьми, выманивая у людей персональные данные и информацию о банковских счетах. Важно помнить, что никакие государственные сайты не требуют предоставления личных данных через QR-коды.

Недавно был выявлен новый вид мошенничества, связанный с арендой самокатов. Человек попытался арендовать самокат и считал QR-код, однако злоумышленники уже подменили код на собственный, и на смартфоне жертвы открылся совершенно другой ресурс. Человек непреднамеренно ввел свои личные данные и заполнил платежные формы, не подозревая о том, что они будут использованы мошенниками в корыстных целях.

Основная проблема, как и в других мошеннических схемах, спешка и невнимательность, которыми пользуются злоумышленники. Чтобы не стать жертвой мошенников, при взаимодействии с QR-кодами необходимо соблюдать базовые правила цифровой гигиены и проявлять бдительность.

## 2. Воровство аккаунтов, путем обхода двухфакторной аутентификации.

Популярность метода двухфакторной аутентификации привела к появлению многочисленных способов взломать или обойти его.

Двухфакторная аутентификация это – это метод идентификации пользователя в каком-либо сервисе (как правило, в Интернете) при помощи запроса аутентификационных данных двух разных типов. На практике это обычно выглядит так:

- Первый тип – логин и пароль.
- Второй тип – специальный код, приходящий по SMS или электронной почте.

Чаще всего в качестве второго фактора используется верификация с помощью одноразовых кодов. Их можно получить различными способами – в виде SMS, голосового сообщения по телефону, письма на почту, сообщения в мессенджере от официального бота сервиса или пуш-уведомления от приложения.

За этими кодами и охотится большинство онлайн мошенников. Например, для перехвата кодов они используют OTP-боты – автоматизированное программное обеспечение, способное выманивать у пользователей одноразовые пароли в схемах с использованием социальной инженерии.

Как выманивают специальный код:

Мошенник заходит в чужой аккаунт (на этом этапе мошенник уже владеет логином и паролем от личного кабинета, а также номером телефона жертвы) и получает запрос на ввод OTP-кода. Жертве на телефон приходит сообщение с одноразовым паролем.

OTP-бот звонит пользователю и с помощью заранее заготовленного скрипта уговаривает ввести полученный код. Жертва набирает код на клавиатуре телефона прямо во время звонка. Код поступает в Телеграм-бот злоумышленника, который таким образом получает доступ к аккаунту жертвы.

Ключевая функция OTP-бота – звонок жертве. Успех мошенников зависит от того, насколько убедителен будет бот: время действия

одноразовых кодов сильно ограничено, и шанс получить действующий код во время телефонного разговора гораздо выше.

Злоумышленники предпринимают максимум усилий, чтобы жертва поверила в легитимность звонка, поэтому некоторые OTP-боты перед набором номера отравляют жертвам СМС-сообщения с предупреждением о предстоящем звонке. Это тонкий психологический прием. Он нацелен на то, чтобы вызвать доверие у пользователя – сначала пообещать что-то и затем сдержать обещание.

Также по телефону могут запросить не только одноразовый пароль, а также и другие данные – например, номер и срок действия банковской карты, ПИН-коды, дату рождения, реквизиты документов и т.п.

В качестве мер безопасности рекомендуем создавать надежные уникальные пароли для всех аккаунтов с помощью менеджера паролей, а также использовать разные пароли для учетных записей. Мошенники не смогут использовать OTP-боты, если не узнают ваш пароль. Если приходит сообщение со ссылкой для ввода любых персональных данных и OTP-кодов, необходимо убедиться в правильности адреса-сайта (подменить пару символов в адресной строке, отправив на похожий фишинговый сайт – любимый трюк мошенников, так что лучше потратить пару секунд и проверить, на легитимном ли сайте вы находитесь и уже после вводить логин, пароль и OTP-код). Не сообщать одноразовые коды третьим лицам и не вводить их на клавиатуре телефона во время звонка. Настоящие сотрудники банка, представители магазинов или сервисов и даже служители закона никогда не будут пытаться узнать ваш одноразовый пароль.

Руководитель Управления А.Ю. Николаев

Демьянов Д.О.
9986738