Профилактика краж и мошеннических действий, совершаемых бесконтактным способом и с использованием информационно-телекоммуникационной сети «Интернет»

Уважаемые коллеги, в целях профилактики краж и мошеннических действий, совершаемых бесконтактным способом и с использованием информационно-телекоммуникационной сети «Интернет» (далее – бесконтактные кражи и мошеннические действия) БПОУ ОО «Медицинский колледж» информирует вас о нижеследующем.

По-прежнему наиболее распространенным способом обмана остается перевод денежных средств на несуществующий «безопасный счет» под предлогом замены счетчиков коммунальных расходов.

Также мошенники выдают себя за сотрудников военкоматов: под предлогом оформления удостоверения гражданина, подлежащего призыву на военную службу, или уточнения данных злоумышленники выманивают у граждан коды авторизации от федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» под видом сообщения мошенникам кода «электронной очереди». Как правило, связь осуществляется в мессенджере WhatsApp. В связи с этим БПОУ ОО «Медицинский колледж» напоминает, что органы государственной власти, включая военкоматы, не используют для связи с гражданами сервисы обмена мгновенными сообщениями.

Аналогичным способом осуществляется обман граждан, которым мошенники звонят от имени «Водоканала» по вопросу выезда специалистов на дом в целях поверки счетчиков воды или выполнения срочных работ: в ходе диалога обсуждаются удобное время, детали визита, поэтому никаких подозрений в обмане не возникает, так как злоумышленники не требуют денежных средств, не просят личных данных и не оказывают давления. Создав полную иллюзию легитимного «рабочего» контакта, мошенники заявляют о необходимости подтверждения оформленной заявки объявлением кода из СМС-сообщения. Следует учитывать, что работники «Водоканала» не запрашивают коды по телефону, а визиты сотрудников осуществляются только по заявке.

Бесконтактные кражи и мошеннические действия осуществляются и через поддельные платежные формы – главными способами обмана в целях хищения платежных реквизитов пользователей выступают: создание фальшивых сайтов известных интернет-магазинов, в том числе в мессенджерах, «сайтов-однодневок», предлагающих товары или услуги по

«невероятно выгодным» ценам, фальшивых страниц системы быстрых платежей, поддельных сайтов для аренды недвижимости.

Одним из возможных способов обмана выступает использование вредоносного программного обеспечения, когда злоумышленники под видом фото или видео направляют ссылку или файл с вредоносной программой (источниками также могут быть нелицензионные игры и программное обеспечение). В зависимости от вида вредоносного программного обеспечения можно лишиться данных, средств или запустить на своем устройстве майнинг криптовалют для мошенников.

Старые схемы с блокировкой устройств Apple путем получения неправомерного доступа к iCloud по-прежнему остаются актуальными: мошенник втирается в доверие к жертве, имеющей устройство Apple. Часто это происходит на сайтах знакомств, в тематических или игровых сообществах в социальных сетях, а также при поиске работы. Под каким-либо предлогом (распечатать билеты, важные документы, установить приложение для работы или недоступную в Российской Федерации игру) жертву уговаривают войти в учетную запись iCloud мошенника на своем устройстве. При получении доступа злоумышленник использует функцию «Найти iPhone» и активационную блокировку, после которой чаще всего следует требование денег под угрозой безвозвратной блокировки или удаления всех данных пользователя с устройства.

Во всех случаях совершения бесконтактных краж и мошеннических действий сообщаем о необходимости:

1) немедленной блокировки банковской карты, в случае оплаты товаров, работ и услуг – отмены транзакции с помощью мобильного приложения, личного кабинета на официальном сайте кредитной организации, через службу поддержки банка по номеру «горячей линии» или в любом его отделении;

2) срочного сообщения о случившемся в банк путем подачи заявления в письменной форме о несогласии с операцией в случае списания денежных средств (в заявлении следует описать ситуацию и попросить разобраться);

3) незамедлительного обращения в любое ближайшее территориальное отделение полиции с заявлением о хищении денежных средств;

4) перевода электронного устройства в авиа-режим или отключения Wi-Fi/мобильных данных при незаконном удаленном доступе мошенника на мобильные устройства.

Напоминаем, что для хищения денежных средств у граждан злоумышленники используют изощренные сценарии обмана, которые

регулярно совершенствуют. При этом схемы бесконтактных краж и мошеннических действий выглядят очень правдоподобно.

Также информируем вас о том, что актуальная информация о новых способах совершения бесконтактных краж и мошеннических действий в отношении граждан размещается в официальном телеграм-канале Управления по организации борьбы с противоправным использованием информационно-телекоммуникационных технологий МВД России «Вестник киберполиции России» (ссылка-приглашение t.me/cyberpolice_rus).

ОБРАЩАЕМ ВАШЕ ВНИМАНИЕ, что на официальном сайте БПОУ ОО «Медицинский колледж», а именно в разделе «Безопасность» (подраздел «Информационная безопасность» и «Противодействие мошенникам») размещены памятки и информационный материал о порядке действий при обнаружении признаков мошенничества, совершаемого с применением информационно- телекоммуникационных технологий.