ОСТОРОЖНО! ФИНАНСОВЫЕ КИБЕРМОШЕННИКИ!

Мошенники активно придумывают новые варианты обмана граждан. Рост активности злоумышленников увеличился вовремя пандемии COVID-19. Мошенники устремились в интернет. Но кибермошенников могут интересовать не только деньги – но и ваши личные данные. Более 90% попыток мошенничества основаны на социальной инженерии с применением негативной новостной повестки о пандемии коронавируса и экономической ситуации. Как правило, мошенники быстро реагируют на любые изменения, происходящие в жизни. Они пользуются неосведомленностью людей, паническими настроениями и на этом «зарабатывают».

Новые виды мошенничества, которые нас подстерегают в сети интернет и не только во время пандемии короновирусной инфекции.

1.В связи с возобновлением транспортных связей возросло количество фиктивных ресурсов по онлайн-продаже авиа- и железнодорожных билетов и бронированию отелей. Некоторые сайты выдают себя за уже известные ресурсы по продаже билетов, другие же заманивают различными скидками и бонусами за покупку. Для своей безопасности необходимо проверять в поисковике, когда был создан этот сайт. Если всего пару месяцев, то, скорее всего, это мошенники. Но, конечно, лучше пользоваться услугами проверенных турагентств.

2. Мошенники используют и более насущные проблемы, связанные с поиском заработка. В интернете появилось много объявлений про быстрый доход, при этом сам способ заработка не раскрывается. Обычно после перехода по ссылке запускается вредоносное ПО или мошенники пытаются с помощью опросов выявить необходимую им информацию о данных ваших банковских карт.

3. Таким же способом нас приглашают быстро заработать на форексе или криптовалюте. На самом деле нелегальные форекс-диллеры никаких финансовых услуг не оказывают. Это обычная игра на деньги, в которой шансов на победу нет.

4. Телефонное мошенничество также не сдает своих позиций. Вам поступает звонок от человека, якобы являющегося представителем банка, который сообщает, что кто-то пытается с вашей карты сделать перевод крупной суммы. Чтобы предотвратить несанкционированные действия, предлагается перевести деньги на «безопасный счет». После этого вы своих денег, как правило, больше не видите. Стоит помнить, что ни один банковский работник не будет спрашивать у вас данные вашей карты. Лучше положить трубку и перезвонить в банк для уточнения обстоятельств по официальному номеру, указанному на вашей банковской карте.

5. Мошенники могут представиться соцработниками и предложить помощь в оформлении выплат, чтобы завладеть данными вашей карты.

6. Также появилось большое число подозрительных ресурсов, эксплуатирующих текущую новостную повестку. Например, злоумышленники пытаются продавать средства индивидуальной защиты, в том числе медицинские маски, а также лекарства, помогающие от короновируса. Регистрируют фальшивые интернет-магазины, где по предоплате предлагают приобрести такие товары.

7. Предложения или звонки с информацией о контакте с подтвержденным носителем вируса, с требованием проведения платного анализа на дому. Ни в коем случае не переводите деньги и не предоставляйте свои личные данные случайным людям. Платные лаборатории могут провести анализ на дому только по Вашему запросу, и такие лаборатории имеют лицензию на осуществляемый ими вид деятельности и не являются «безымянными» - всю информацию о них можно узнать на сайтах и в других открытых источниках.

8. Мошенники могут попросить принять участие в благотворительных акциях, например, пожертвовать деньги на помощь пожилым людям или соотечественникам, оставшимся за рубежом, объявить сборы на лечение детей или взрослых, заболевших коронавирусом. Переведенные в таком случае деньги, скорее всего, вернуть не удастся. Следует тщательно проверять такие обращения.

Во всех этих случаях злоумышленники получают от жертвы деньги и затем не выходят на связь!

В основном злоумышленники используют уже известный прием: под видом банковских сотрудников звонят клиентам и пытаются выманить реквизиты карты и СМС-пароли от банка. Поэтому никогда не сообщайте посторонним людям данные своей карты, не вводите ее данные на неизвестных сайтах или пароли из СМС-сообщений, под каким бы предлогом у вас ни пытались бы их узнать.

Бесплатно проверить, не принадлежит ли номер телефона или сайт мошенникам, можно на сайте Сбербанка. Для этого создан раздел «Как обезопасить себя от мошенников». Необходимо ввести в соответствующее поле номер телефона или адрес сайта, после чего сервис выдаст информацию о риске мошенничества, а также соответствующие рекомендации. Здесь же можно передать информацию о звонках мошенников и адресах мошеннических сайтов. Полученные данные Сбербанк будет отправлять в экспертные организации для расследования случаев мошенничества. Все выявленные мошеннические номера телефонов и сайты будут блокироваться.

С целью получения достоверной информации о коронавирусной инфекции и способов борьбы с ней, получения государственной поддержки в период пандемии, доверяйте только официальным сайтам – Роспотребнадзор, Минздрав, ВОЗ, сайты Правительства и портал Государственных услуг. Однако, и в этом случае следует проявлять бдительность, поскольку известны факты, когда мошенники создают вирусные интернет-сайты, распространяющие вредоносное программное обеспечение, для кражи личных данных или данных банковской карты, которые маскируются под официальные порталы реальных организаций.

За консультацией по вопросам защиты прав потребителей Вы можете обратиться в Центр по информированию и консультированию потребителей Адрес: Великий Новгород, ул. Германа, 29а, Телефоны: 8(8162) 77-20-38; 73-06-77 e-mail: zpp.center@yandex.ru страница в «ВК»: https://vk.com/zppnovgorod сайт: https://www.cgevnov.ru