МОШЕННИКИ В СЕТИ

Интернет стал местом, где многие проводят большую часть своей жизни. Помимо общения, интернет дает очень много возможностей: совершение покупок, платежи за различные услуги, использование государственных порталов для общений граждан.

В последние годы появилось много мошенников, которые выманивают у людей деньги, пользуясь их неграмотностью, да и просто невнимательностью при работе в интернете.

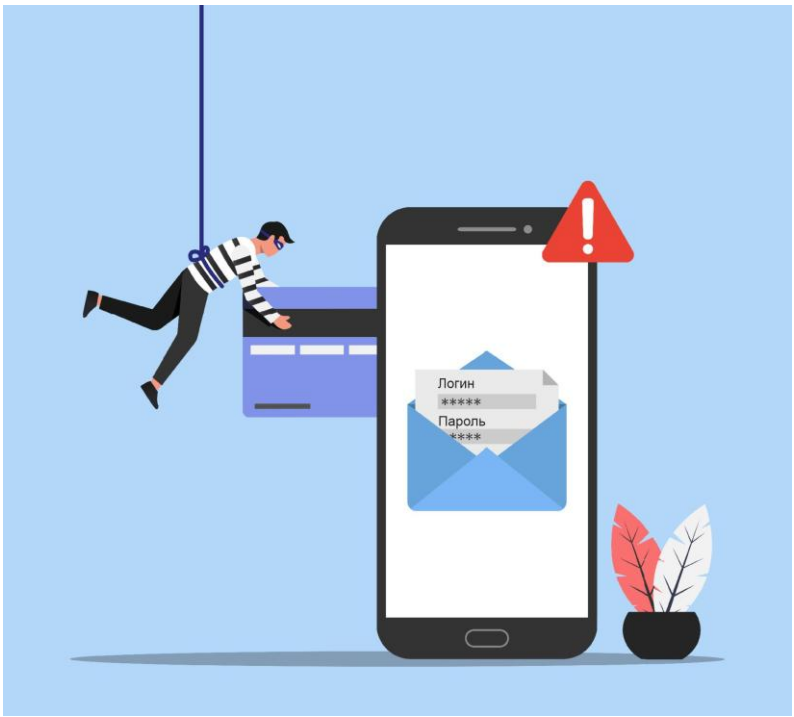
Самый распростарнеенный вид интернет-мошенничества, про вы уже наверняка слышали не один раз, это фишинг – кража любых персональных данных, от которых преступники могут получить выгоду. Это серии и номера паспортов, реквизиты банковских карт и счетов, пароли для выхода в электронную почту, платежную систему и аккуанты в социальных сетях. Персональную информацию мошенники используют для получения доступа к личным кабинетам, к которым привязаны банковские карты, что позволяет похищать с их счетов денежные средства.

Никогда, ни при каких обстоятельствах не сообщайте никому реквизиты пластиковых карт, ваших или ротительстких. Особенно защищенными должны быть PIN-коды и CVV-коды, написанные на обороте карты. Обратите внимание, что личную информацию можно вводить только при безопасном соодинении. Всегда смотрите в адресную строку – адрес веб-сайта должен начинаться с «fttps://», а в интерфейсе браузера должна появиться иконка замка.

Есть очень хорошая фраза: «Если что-то звучить слишком хорошо и заманчиво, что бы быть правдой, скорее всего это неправда». Все мы получаем письма по электронной почте с обещанием чего-нибудь бесплатного или легкого, например, легкой высокооплачиваемой работы, мобильного телефона или билетов на концерт. Это трюки, призванные заставить вас передать личные сведения, не покупайтесь на них.

Есть еще одно правило, которое следует помнить: «Посмотрите в обе стороны, прежде чем переходить улицу». Воспринимайте ее не только в буквальном, но и в переносном смысле. Например, прежде чем скачать приложение или воспользоваться сайтом, посмотрите его рейтинг, почитай отзывы: убедись, что не навредит твоему устройству. Принцип «подумай», прежде чем сделать» будет актуален всегда.

И последнее. Сейчас для разблокировки смартфоном очень популярны отпечаток пальца и разблокировки по лицу. Это очень удобно и стильно, но если вы храните большой объем личной, важной, конфедициальной информации в телефоне – используйте пароль из 4 цифр. Он гораздо надежнее и безопаснее новых способов разблокировки, хоть и не столь быстр и удобен.



Подводя итог всему сказанному, будьте бдительны и внимательны в сети интернет точно так же, как и в реальной жизни. Для наглядности приведены новые типы мошенничеств и наглого обмана граждан, которые появились в последние два года:

1. Мошеннические телеграмм-каналы.

Предлагают вносить финансовые средства на расчетный счет и делать ставки в букмекерских конторах, не зареегстрированый на территории Российской Федерации и действующих без лицензий. Такие каналы часто

продвигают блогеры, получая за рекламу значительные суммы денег, при этом рядовые пользователи становиться жертвами обмана.

2. Предложения по изготовлению поддельных сертификатов о вакцинации или ПЦР-тестов в сети Интернет.

Думаю, не важно напоминать вам, что покупка и реализация таких вещей находится вне закона. Приобретая такой «сертификат» вы не только подвергаете опасности свое здоровье и жизнь окружающих, но и становитесь потенциальным соучастников преступления.

3. Суперприбыльные инвестиции.

Предложения о вложении в ценные бумаги банков или телекоммуникационных компаний. Такие инвестпроекты «гарантируют» безусловный возврат вложенного капитала и высокие прибыли, вместе с тем капиталом в последующем не возвращается.

4. Интернет-магазины с необоснованно низкими ценами.

Мошенники создают сайт интернет-магазина и активно запускают рекламный трафик, чтобы высвечиваться на первых страницах в поисковых системах. За товар требуется полная предоплата, а доставка осуществляется исключительно курьерской службой, самовывоз не предусмотрен. После перевода денежных средств покупателем, продавец перестает выходить на связь и удаляет сайт интернет-магазина.

Осторожно! Телефонные мошенники!

Осторожно! Телефонные мошенники!