Зачем мошенники звонят и сбрасывают

В итоги 2020-го проскользнул грустный рекорд: Сбер насчитал

3,7 миллиона обращений клиентов о телефонном мошенничестве. По сравнению с

2019годом этот показатель вырос вдвое, а по сравнению с 2017-м — в 30 раз.

Сейчас жулики звонят россиянам в среднем до 100 тысяч раз в сутки.

Потенциальные жертвы к этому уже привыкли, а некоторые ещё и

стали пользоваться специальными приложениями, которые определяют

подозрительные

номера.

Поэтому мошенники используют новую уловку: теперь они иногда

набирают номер и сразу же сбрасывают свой звонок. То есть до того как

кто-нибудь поднимет трубку, а может, и раньше, чем даже оператор соединит с

абонентом.

Так жулики пытаются перехитрить антиспам-приложения. Такие

системы анализируют только входящие звонки, а исходящие — нет, потому что

никто

не рассчитывал, что люди сами начнут звонить мошенникам.

А беспокойство и желание сделать это при виде пропущенного

вызова или сообщении о «недозвоне» появляется у многих.

Но именно на ответный звонок и рассчитывают жулики —

приложение ничего не заподозрит, а мошенник запоёт свою обычную песню:

скорее

всего, представится сотрудником банка и будет либо уговаривать перевести

деньги, либо выманивать конфиденциальные данные.

По статистике, большинство звонков с незнакомых номеров —

это спам. Да вы, наверное, это и сами уже давно заметили.

Поэтому для защиты от новой уловки мошенников полезно стать

чуточку более чёрствым и помнить о старом-добром принципе: кому надо, тот

перезвонит. Или, в крайнем случае, хотя бы напишет сообщение.

Как мошенники спекулируют на вакцине от коронавируса

У опытных жуликов намётан глаз на новости — они следят за

повесткой и включают в свои схемы важные для нас темы. Сейчас одна из таких

—

прививки от COVID-19. Всё больше людей получает фейковые электронные письма

от

имени известных компаний с информацией о лекарствах или предложениями о

продаже

препарата. И судя по всему, это только начало.

Чаще всего схема киберпреступников проста — они

распространяют вирусы в письмах под видом буклетов о вакцине. Если

получатель

откроет приложенный файл или пройдёт по ссылке из письма, вредонос попадёт

на

гаджет. Затем программа зашифрует все данные на устройстве или настроит

удалённый доступ, а мошенник-оператор скопирует то, что ему нужно.

Другой старый как мир трюк — убедить человека оставить

данные о своей банковской карте на сайте мошенников. Потенциальной жертве

приходит письмо, в котором её просят заполнить анкету на получение вакцины.

На сайте с анкетой человека, скорее всего, попросят

«верифицироваться» — отправить один-два рубля с карты по реквизитам, чтобы

подтвердить уникальность заявителя. Вы наверняка догадались, что будет, если

ввести данные карты на местной страничке «оплаты».

Чтобы защититься, нужно быть особенно внимательными и

осторожными с письмами насчёт вакцинации. И конечно, помнить о базовых

правилах:

• стоит насторожиться, если в «официальном» письме от

компании есть орфографические ошибки;

• также обращайте внимание на то, оставили ли отправители

контакты для обратной связи, и если нет, будьте осторожны;

• подозрения должна вызвать и тема письма, если там хотя бы

одна русская буква заменена на английскую;

• если письмо приходит с адреса, который только похож на

официальный, а не полностью совпадает с ним, это мошенничество.

Но главное — не открывайте

вложения и не переходите по ссылкам из подозрительных писем, даже если вы

очень-очень ждёте вакцину. Её в любом случае должно хватить на всех.