

Предновогодний обман: на какие уловки идут мошенники перед праздником

Последние предпраздничные дни – это не только время интенсивной работы магазинов и салонов красоты, но и период, когда активизируются мошенники. Криминальная активность особенно возрастает в виртуальном пространстве. Преступники пользуются тем, что люди готовы потратить больше, чем обычно и при этом менее критично настроены.

Первый способ, который используют мошенники, - **рассылка вредоносных ссылок** под видом новогодних поздравлений. Если перейти по ссылке, указанной в письме или загрузить приложенный файл, можно вместо приятных праздничных слов получить неприятную дыру в бюджете: вирусы, зашитые внутри, либо взломают данные различных соцсетей, электронной почты и т.д., либо даже получают доступ к банковскому счету.

Активно внедряются преступники и в такое направление, как **интернет-торговля**. Все больше людей предпочитают не толкаться в очередях, выбирать из 5-6 товаров на полке, мучиться с доставкой домой, а приобретать все, от подарков до блюд на новогодний стол дистанционно. «Если вы собираетесь совершить покупку в интернете, убедитесь, что сайт, на котором вы делаете заказ, действительно принадлежит этому магазину, а платежный сервис должен использовать зашифрованный канал связи. Его легко определить по специальному символу, замочку, и буквам перед адресом – https», - рассказывает управляющий Отделением Рязань ГУ Банка России по ЦФО Сергей Кузнецов. По данным «Лаборатории Касперского», только за 3 месяца этого года зафиксировано 94 млн попыток завладеть данными держателей карт. Также следует помнить, что данные карты (номер, срок действия, а особенно трехзначный код CVC, который располагается на обратной стороне) сообщать нельзя. Это актуально и в том случае, если второй участник сделки – частное лицо, а не магазин.

Не забывают мошенники и про веру людей в чудо, которая особенно усиливается перед Новым годом. Они рассылают сообщения или звонят с «радостной новостью»: якобы человек **стал победителем в розыгрыше**. Для того, чтобы забрать приз, нужно сделать лишь ... Далее вариантов может быть несколько (перезвонить, а номер в итоге будет платным, оплатить налог, зарегистрироваться на сайте, опять же за деньги), исход же один – потеря времени и средств.

Недавняя схема обмана: **маскировка под борьбу с мошенничеством**. Владельцу карты звонят и говорят, что карта заблокирована, апеллируют к законодательству. Чтобы вновь проводить операции, клиент должен сообщить код, который пришлют в СМС. Хотя в действительности банки никогда не требуют такую информацию или данные по картам.

«Мошенники изобретают все новые способы, как присвоить себе чужие деньги. Перед Новым годом, в предпраздничной суете, не следует забывать об основах грамотного финансового поведения и внимательности. Тогда вы не сделаете подарка преступнику и сохраните свои средства», - напоминает управляющий Отделением Рязань ГУ Банка России по ЦФО Сергей Кузнецов.