«Мошенники на удаленке»

Несмотря на то, что технологии стали важной частью нашей жизни, и уже невозможно представить без них ни работу, ни отдых, эта среда остаётся для нас достаточно новой, и мы не всегда отдаём себе отчёт в том, какие опасности таит беспечное использование гаджетов и сетей.

В последние годы широкую популярность получили смс-рассылки или электронные письма с сообщениями о выигрыше автомобиля либо других ценных призов. Для получения «выигрыша» злоумышленники обычно просят перевести на электронные счета определенную сумму денег, мотивируя это необходимостью уплаты налогов, таможенных пошлин, транспортных расходов и т.д. После получения денежных средств они перестают выходить на связь либо просят перевести дополнительные суммы на оформление выигрыша.

Оградить себя от подобного рода преступлений предельно просто. Прежде всего необходимо быть благоразумным. Задумайтесь над тем, принимали ли вы участие в розыгрыше призов? Знакома ли вам организация, направившая уведомление о выигрыше? Откуда организаторам акции известны ваши контактные данные? Если вы не можете ответить хотя бы на один из этих вопросов, рекомендуем вам проигнорировать поступившее сообщение.

Любая просьба перевести денежные средства для получения выигрыша должна насторожить вас. Помните, что выигрыш в лотерею влечет за собой налоговые обязательства, но порядок уплаты налогов регламентирован действующим законодательством и не осуществляется посредством перевода денежных средств на электронные счета граждан и организаций или т.н. «электронные кошельки».

Случаи, когда мошенники выходят на прямой контакт с пользователем, относят к фишингу. Основной принцип – притвориться тем, кому человек доверяет, будь то друг, знакомый или сотрудник банка, клиентом которого является пользователь. Мошенники присылают письма по электронной почте, смс и сообщения в мессенджерах и социальных сетях, создают поддельные сайты или просто звонят по телефону. Чтобы не попасться на их уловки, нужно быть достаточно внимательным и бдительным.

Запомните основные признаки фишинга: во-первых, это призыв к действиям, якобы не терпящим отлагательства. Это может быть сообщение об акции, которая вот-вот закончится, компенсации, документы для которой нужно прислать как можно скорее, или об угрозе хищения средств с карты, попытки которого происходят прямо сейчас. Такие известия полностью поглощают наше внимание, и чёткие инструкции от мошенников кажутся нам единственно верным выходом. Но иллюзия быстро рассеивается, когда мы кладём трубку, рассказываем о ситуации близким или, не дай бог, обнаруживаем списание средств со своих счетов.

В случае, если ваш друг в соцсети просит перевести ему деньги, постарайтесь выяснить, что случилось, связавшись с ним напрямую: позвоните или попробуйте

связаться с его близкими. Даже если вам пришло сообщение с убедительной историей о несчастье, болезни или аварии, это может оказаться ложью и попыткой сыграть на желании помочь другу. Стоит отнестись с подозрением и к ситуации, когда знакомые по сети пытаются выведать у вас какую-либо личную информацию. Возможно, учётную запись вашего собеседника взломали и говорите вы сейчас совсем не с ним.

Ну и напоследок напомню, какие данные совершенно точно нельзя сообщать никому: номер карты, срок её действия, секретный код на обратной стороне и код из смс от банка. Передавая эту информацию третьим лицам, вы даёте им возможность совершать любые операции с вашими картами и счетами, в том числе – похитить все деньги.

Не забывайте, что никто лучше вас самих не сможет позаботиться о сохранности той личной информации, которой вы не хотите делиться с общественностью.

Уважаемые граждане!

Соблюдение элементарных правил поможет вам не стать жертвой мошенников и сохранить личное имущество. Потерпевшими от преступных действий злоумышленников становятся не только излишне доверчивые пенсионеры, но и молодые люди. Поэтому стоит как можно чаще напоминать своим родственникам и знакомым о том, как действуют мошенники и объяснять, что ни при каких обстоятельствах не следует перечислять деньги незнакомым людям или сообщать свои персональные данные, логины, пароли и коды банковских карт.

Начальник следственного отделения
МО МВД России «Макарьевский»
майор юстиции Смирнов В.А.