О мошенниках не стоит забывать!

К сожалению, с развитием электронных технологий развивается и кибермошенничество. Злоумышленники находят всё новые способы хищения и обмана доверчивых и простодушных граждан, которые, не опасаясь, называют сведения о себе и своих банковских картах – номера и пин-коды.

Рассмотрим основные уловки кибермошенников, а также рекомендации по противодействию последним:

Просьба о помощи

Достаточно распространенный вид мошенничества. Абоненту приходит SMS с просьбой о помощи. Вариантов таких сообщений достаточно много, но суть у них одна. Например: ***«Мама (папа, сестра, брат и т.д.), пишу с чужого номера. На моем телефоне закончились деньги. Срочно положи столько-то рублей на номер…»*** Могут приходить сообщения о «попадании в аварию», «неприятности с контролерами в общественном транспорте» и т.д.

Для защиты от такого вида мошенничества всегда необходимо уточнить у родных, друзей, знакомых полученную информацию.

При желании перезвонить на номер, с которого пришло подобное SMS, а также стоит обратить на него внимание. Так как это может быть короткий номер или номер иностранного оператора.

Клонирование SIM-карты

Информация с SIM-карты оператора сотовой подвижной электросвязи, которая попала в руки злоумышленника, может быть скопирована (клонирована) в память компьютера, а потом перенесена на «чистую» SIM-карту. После чего она может быть вывезена за границу и активирована в режиме роуминга. Однако счета за оказанные услуги связи будут выставлены владельцу, на которого она зарегистрирована.

Для защиты от подобного вида мошенничества никогда не следует передавать свою SIM-карту третьим лицам, особенно незнакомым. При сдаче телефона или другого устройства связи в ремонт необходимо извлечь SIM-карту.

В случае утери (кражи) телефона (SIM-карты) необходимо незамедлительно обратиться к своему оператору сотовой связи для оказания услуг по ее блокировке. Особенно следует придерживаться данных рекомендаций в случае утери телефона за границей во избежание начисления задолженности на большую сумму (при использовании телефона злоумышленниками), которую придется внести по возвращении в Республику Беларусь. Стоит учитывать и тот факт, что счета за пользование мобильной связью в режиме роуминга выставляются оператором пользователям не сразу, а по прошествии достаточного количества времени.

Ошибочный платеж («Верните деньги!»)

Существует несколько схем такого мошенничества, рассмотрим их подробнее.

SMS может приходить как от оператора сотовой связи (злоумышленник на самом деле пополнил баланс мобильного телефона пользователя), так и с произвольного номера, повторяя «оригинальное» сообщение оператора. Причем в первом случае деньги, как правило, зачисляются на счет абонента, а во втором – нет.

Далее на мобильный номер абонента может поступить звонок с просьбой о возврате денежных средств на определенный номер злоумышленника за ошибочно произведенный платеж. Абонент, подтвердив свое согласие о возврате денежных средств, переводит указанную «ошибочную» сумму на мобильный номер злоумышленника. В первом случае злоумышленник обращается с заявлением к сотовому оператору и повторно переводит со счета абонента-жертвы сумму «ошибочного» платежа. Второй вариант развития событий предполагает, что деньги на счет абонента фактически не поступают, а абонент делится со злоумышленником своими деньгами.

В целях защиты от такого вида мошенничества необходимо помнить, что у всех операторов существует отработанная процедура возврата ошибочно уплаченных средств для пополнения баланса чужого абонентского номера.

В случае возникновения подобной ситуации не стоит переводить денежные средства на незнакомый абонентский номер, а рекомендуется посоветовать звонящему обратиться к оператору сотовой связи в целях урегулирования данного вопроса.

Входящие звонки с неизвестных иностранных номеров

Данный вид мошенничества также основывается на невнимательности абонента.

Например, глубокой ночью абоненту поступает входящий звонок из-за границы, который буквально сразу сбрасывается, а абонент не успевает на него ответить. Абонент, находясь в сонном состоянии, перезванивает на неотвеченный неизвестный иностранный номер, а после установления соединения либо ничего не слышит, либо у него включается автоответчик. При этом со счета абонента списываются денежные средства.

Для защиты от данного вида мошенничества абоненту необходимо проверять номер мобильного оператора, на который он собирается сделать звонок, и без необходимости не перезванивать на незнакомые иностранные номера.

Странные номера входящих вызовов и SMS

Этот вид мошенничества предполагает деятельность злоумышленников, связанную с незаконной терминацией (оригинацией) голосового трафика в обход надлежащих

коммутационных узлов операторов электросвязи, уполномоченных на пропуск международного и (или) межсетевого трафика, и (или) использованием услуги IP-телефонии в нарушение установленного законодательством порядка.

Подобная деятельность влечет негативные экономические последствия как для операторов электросвязи, уполномоченных на пропуск международного и (или) межсетевого трафика, а также на оказание услуг телефонии по IP-протоколу в пределах действия сетей электросвязи Республики Беларусь, так и для абонента, с лицевого счета которого в случае осуществления звонка на подобные номера будут списаны средства как за исходящий вызов.

В целях осуществления противодействия такому виду мошенничества абонент может обратиться к своему оператору сотовой связи и сообщить о подобном факте. Оператор электросвязи, совершив необходимые действия, сможет пресечь на стороне своей сети незаконную деятельность третьих лиц.

Звонки со стороны «службы поддержки» сотового оператора

Злоумышленники представляются сотрудниками технической поддержки оператора и под различными предлогами (несвоевременная оплата счета, технические проблемы, случайная блокировка абонентского номера технической службой, сбой в работе оборудования, перевод оборудования оператора для работы с другими голосовыми кодеками и т.д.) предлагают абоненту либо перевести деньги на указанный ими номер, либо оплатить штраф, либо перезвонить на короткий номер для решения возникшей проблемы или на номер телефона, на котором будет включен автоответчик с «рекомендацией», какие действия предпринять абоненту в дальнейшем.

Чтобы исключить данной вид мошенничества, необходимо помнить, что операторы сотовой связи всегда приглашают абонента в фирменный центр продаж своих услуг в целях решения всех возникших проблемных вопросов.

Выигрыш приза

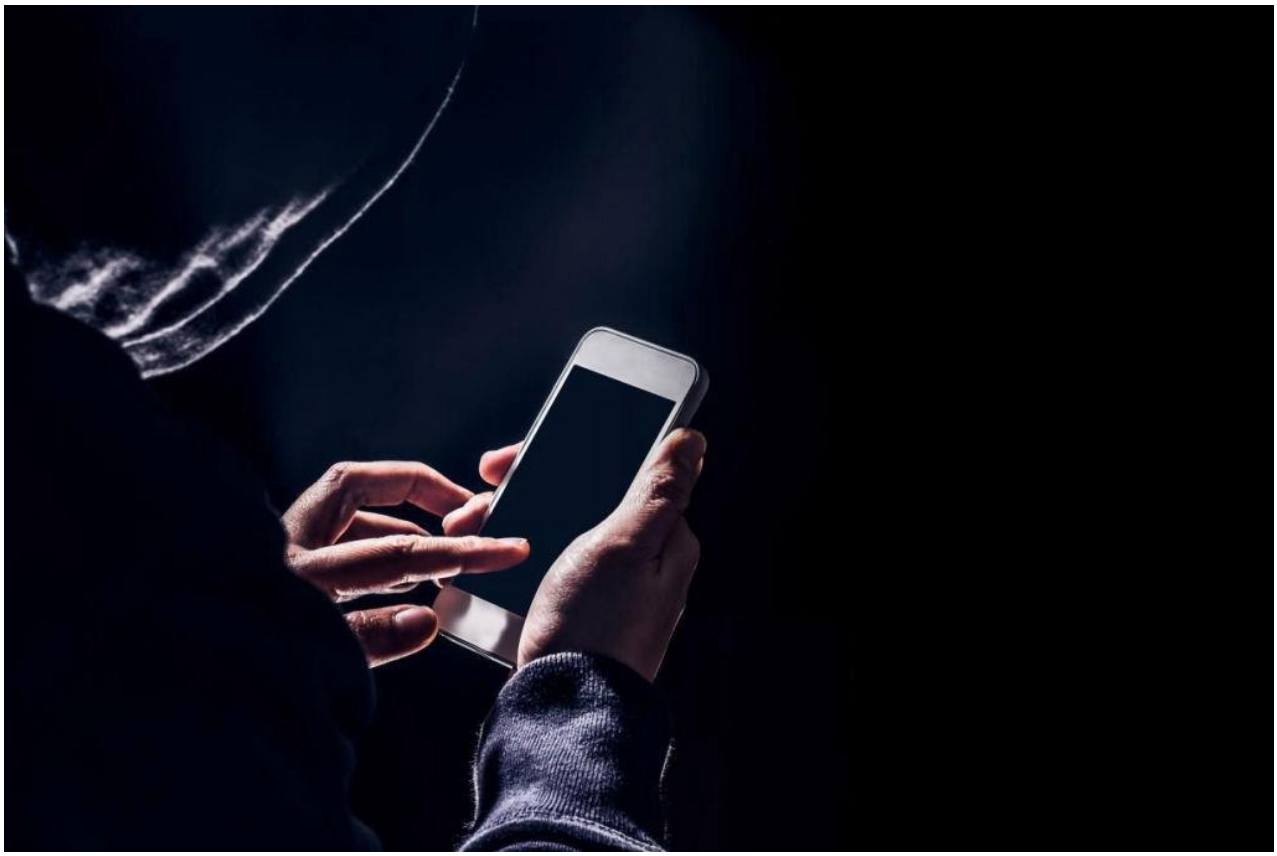
На телефон абонента поступает звонок (также возможно получение SMS). При этом звонящий представляется сотрудником известной радиостанции, банка, телеканала или туристической фирмы и поздравляет абонента с выигрышем ценного приза, туристической поездки и т.д.

Для получения приза абоненту предлагается в течение ближайших минут перезвонить на короткий номер указанной компании, где абонента в очередной раз поздравят с выигрышем ценного приза и предложат оплатить, например, налог на выигрыш, перечислив денежные средства на электронный кошелек или

предоставив в течение часа сотруднику компании данные карты экспресс-оплаты за услуги связи на определенную сумму.

После этого обманутый абонент приезжает за призом в офис известной компании и узнает, что никакого розыгрыша не проводилось.

Чтобы не стать жертвой такого мошенничества, не стоит спешить перезванивать на короткие номера и отправлять денежные суммы на электронные кошельки различных платежных систем. Самый верный способ – обратиться в офис названной компании, телеканала, радиостанции, банка или туристической фирмы и на месте уточнить у сотрудников все вопросы, связанные с возможным выигрышем. Не стоит забывать, что, как правило, компании всегда освещают в средствах массовой информации ход и результаты проведения различного рода розыгрышей и акций.



Звонки со стороны «банковских структур и организаций»

Всегда стоит помнить, что настоящий технический специалист или сотрудник банка никогда, ни в каких случаях не будет запрашивать у клиента конфиденциальную информацию, касающуюся реквизитов банковской карты, а также персональные данные из паспорта и т.д.

В случае возникновения подозрения, что с вами разговаривает злоумышленник, необходимо прекратить разговор, а для уточнения вопросов, возникших с вашей банковской картой или банковским счетом, самостоятельно перезвонить по номеру горячей линии банка, указанного на его официальном интернет-сайте.

Также не следует перезванивать на тот номер телефона, с которого вам звонили злоумышленники. Так как он с высокой степенью вероятности будет изначально подменен или вы сами можете дозвониться до злоумышленников, которые затем продолжат разыгрывать свой «спектакль».

Стоит в том числе иметь в виду, что в настоящее время существуют технологии, позволяющие злоумышленникам заблокировать телефонную линию жертвы и перенаправлять все последующие ее звонки на мошенников.

В данном случае, если у вас имеются достаточные подозрения, то для связи с банком воспользуйтесь, к примеру, стационарным телефоном.

Запомните, ни в коем случае не сообщайте злоумышленникам реквизиты вашей банковской карты и не осуществляйте перевод средств на другие счета, которые предложены звонящим злоумышленником.»

К вам пришла SMS с просьбой перейти по указанной ссылке для разблокирования вашей электронной почты, аккаунта в соцсети и т.д.

SMS-рассылка в настоящее время стала очень популярным инструментом для продвижения своих товаров, работ и услуг, а также информирования клиентов о новых акциях и т.д.

К SMS, которые содержат ссылку, следует относиться с настороженностью. Учитывая, что объем SMS ограничен, многие компании используют сервисы по сокращению ссылок и понять, на какой интернет-ресурс ведет конкретная ссылка, не представляется возможным.

Этим и пользуются злоумышленники, перенаправляя при помощи таких SMS, содержащих сокращенные ссылки, на свои ресурсы, где обычно на визуально схожей с оригинальной страницей интернет-ресурса злоумышленники предлагают, к примеру, ввести свой логин и пароль или иные данные, которые затем получают злоумышленники для доступа к вашему личному кабинету, странице соцсети и т.д.

Кроме того, переход по ссылке может означать автоматический акцепт предлагаемой услуги.

Перед переходом по ссылке, присланной в SMS, всегда следует еще раз перепроверить информацию, позвонив на горячую линию сервиса или зайдя на их интернет-ресурс.

Стоит помнить, что мошенники идут в ногу со временем, а общество постоянно повышает уровень своих цифровых знаний, всё больше узнает о социальной инженерии и иных методах злоумышленников, поэтому используемые сейчас последними способы и средства для хищения денежных средств в скором времени могут стать неактуальными, поэтому в любой ситуации нужно оставаться предельно внимательными и досконально разобраться в случившемся,

прежде чем сообщить кому-то свои персональные данные или совершить какие-либо действия по указанию мошенника.

По информации УВД Брестского облисполкома