ФИНАНСОВАЯ ГРАМОТНОСТЬ

20 января во Владимирском отделении Банка России прошла информационная встреча с представителями СМИ, темой которой стал настоящий бич современности – кибермошенничество. Во встрече также приняли участие сотрудники МВД России по Владимирской области.

Если речь о деньгах и вас торопят – это повод насторожиться

В тесном сотрудничестве с Банком России

Управляющий Отделением Владимир Банка России Н.В. Калашникова в своем вступительном слове подчеркнула, что Банк России ОМВД и СМИ совместно проводят огромную работу по профилактике кибермошенничества. Отдельно она поблагодарила редакции средств массовой информации за сотрудничество с Банком России в сфере повышения финансовой грамотности граждан и вручила благодарности. Отмечу, что в число таких СМИ вошла и наша газета «Коммунар». Представители МВД также поблагодарили журналистов за взаимодействие и вручили грамоты самым активным изданиям.

Рассказала руководитель Владимирского отделения и о том, как строится взаимодействие между МВД и Банком России по профилактике и выявлению мошеннических действий. Так, в октябре 2022 года был подписан федеральный закон об оперативном взаимодействии между Банком России и Министерством внутренних дел для предотвращения кражи денег со счетов граждан.

В соответствии с ним, МВД будет подключено к автоматизированной системе Банка России, в которой собирается информация обо всех операциях без согласия клиента – с учетом того, что человек предварительно обратился по этому поводу в свой банк и был зафиксирован факт мошенничества. База данных содержит сведения ото всех российских банков. Это значит, что правоохранительные органы смогут практически в онлайн-режиме получать информацию о мошеннических операциях, конечно, с соблюдением всех норм о банковской тайне.

В свою очередь, база Банка России будет дополнена сведениями МВД о совершенных противоправных действиях. Эти данные помогут банкам эффективнее вести борьбу с мошенническими списаниями средств с банковских карт, в том числе с использованием социальной инженерии. Закон вступит в силу 21 октября 2023 года.

Более трех тысяч киберпреступлений совершено в регионе за год

Об истинных масштабах мошеннических действий в интернете помогли составить представление **представители МВД по Владимирской области И.А.Моисеев и И.Н.Гавриченко.** И.А.Моисеев отметил, что в 2022 году на 30% выросло количество дистанционного мошенничества, когда граждане под определенным психологическим воздействием добровольно переводили средства мошенникам. Число финансовых мошенничеств, совершенных с использованием различных информационных систем за прошлый год во Владимирской области, составило 2431. Всего же киберхищений, включая кражи денег с утерянных карт и оплаты с них покупок, составило более 3300. Самым опасным видом мошенничества сотрудники ОМВД назвали звонки с использованием IT-телефонии, когда мошенники работают в паре – представляясь сотрудником банка и сотрудником правоохранительных органов. Причем телефон, с которого совершается звонок, определяется как реально существующий. При его проверке через интернет зачастую выясняется, что это номер отделения ОМВД. Как отмечалось, в случае звонка «сотрудника ОМВД» психологическое давление, оказываемое на человека, очень велико. И даже если положить трубку – возможны последующие звонки с угрозами к привлечению к уголовной ответственности.

Еще один способ, который вновь начали использовать телефонные мошенники, – звонки пожилым родственникам от якобы их внуков о том, что те попали в ДТП и нужно передать деньги, чтобы уладить ситуацию. К сожалению, на эту «удочку» попадаются многие пожилые люди, лишаясь всех своих сбережений, отложенных на черный день. В нескольких таких ситуациях сотрудникам ОМВД удалось задержать курьеров, приезжающих за деньгами, однако организаторы такого вида мошенничества почти всегда находятся за рубежом, и привлечь их к ответственности невозможно.

И.Н. Гавриченко также отметила, что статистика по киберпреступлениям могла бы быть гораздо выше – но многие граждане, к счастью, из СМИ знали, как определить мошенника и на уловки аферистов не поддались.

Способы противостоять мошенникам – есть!

Подробно о действиях кибермошенников рассказал **эксперт по кибербезопасности Отделения Владимир Банка России Е.Г. Гаврилюк**. Основной инструмент аферистов, по мнению эксперта, — применение методов воздействия на сознание человека, так называемая социальная инженерия. Телефонные аферисты привязывались к любым новостным поводам, чтобы ввести жертв в заблуждение, похитить конфиденциальные данные и затем средства, либо принуждали людей самостоятельно переводить деньги на счета мошенников. Чаще всего - используя формулировку о некоем якобы «безопасном счете». Говорили об угрозе для средств в связи с отключением от системы «Свифт», об уходе «Visa» и «Mastercard», о дефиците валюты, об угрозе деньгам на вкладах – словом, использовали все возможные информационные поводы.

Также зачастую мошенники представляются сотрудниками Банка России или присылают на электронную почту документы с логотипом Банка России. В таких случаях просто нужно помнить, что Банк России не работает напрямую с физическими лицами и не открывает счетов. Отметил эксперт также, что эффективной формой для мошенников служат различные рассылки в том числе в соцсетях – предложения работы или покупок на маркетплейсах. Если начинаются вопросы о номере вашей карты, просьбы сообщить код или предложения внести предварительный взнос для получения чего-либо – скорее всего вы общаетесь с мошенниками.

Евгений Геннадьевич подробно рассказал и о работе, направленной на борьбу с мошенничеством. Банк России вместе с участниками рынка и экспертами предлагает изменить законодательство, чтобы люди могли рассчитывать на возврат средств даже тогда, когда они были введены в заблуждение и поэтому перевели деньги на счета злоумышленников. Такой законопроект уже рассматривается в Госдуме.

Банк России ведет базу о случаях и попытках перевода денежных средств без согласия клиентов. В ней аккумулируются данные, которые банки направляют в ЦБ, в том числе содержатся сведения о дропперских счетах. То есть о счетах, которые злоумышленники используют для вывода и снятия похищенных средств. Банк России предлагает следующий механизм возмещения гражданам похищенных злоумышленниками средств: если банк—отправитель платежа получил от ЦБ информацию из базы, но не учел ее в своих бизнес-процессах и совершил перевод на такой счет, то он будет обязан вернуть клиенту все похищенные средства. Даже если мошенническая операция произошла с использованием методов социальной инженерии.

Для защиты интересов граждан Банк России призывает банк-плательщик на два дня приостанавливать зачисление денег на счет, информация о котором содержится в базе ЦБ. Другими словами, внедрить так называемый «период охлаждения», когда у гражданина будет время обдумать и оценить совершаемые действия. По закону перевод совершается в срок до трех рабочих дней, таким образом, банк не нарушит права добросовестных граждан и законодательство.

Кроме того, проверять операцию на признаки мошенничества должен и банк-получатель средств. Если он видит, что деньги перечисляют на счет, содержащийся в базе регулятора, то у банка должно быть право приостанавливать доступ владельца такого счета к дистанционному обслуживанию. То есть получатель подозрительного счета не сможет сразу же распорядиться деньгами, перевести их на любой другой счет, что обычно сразу делают мошенники. Чтобы разблокировать эту возможность, владельцу счета придется прийти в отделение банка с паспортом, на что вряд ли пойдут дропперы. В то же время будут соблюдены все гражданские права добросовестных банковских клиентов.

Пока этот закон на рассмотрении, но уже сейчас банки помогают своим клиентам приостановить перевод мошеннику. Наиболее внимательные сотрудники банков, видя неадекватное состояние клиента (особенно пожилого человека) и его намерение снять или перевести большую сумму денег, делают временную блокировку счета до выяснения всех обстоятельств.

Также спикер дал несколько рекомендаций по кибербезопасности: «При подозрительных звонках сохранять бдительность и скепсис. Если кто-то инициативно выходит на связь, говорит о ваших деньгах, то это уже повод максимально насторожиться. Просто завершайте разговор и кладите трубку. А затем сами перезвоните по официальному телефону организации, из которой якобы был совершен звонок, чтобы уточнить подробности. Никогда и никому ни под каким предлогом не сообщайте секретные данные вашей карты: код на оборотной стороне, коды из СМС, пин-код, логин и пароль для входа в онлайн банк.

Банковская система настроена на защиту ваших средств, настоящие сотрудники банка никогда не будут торопить, запугивать, требовать совершать какие-то странные действия, вроде установки какого-то приложения удаленного доступа, требовать пойти к банкомату снять деньги, взять какой-то кредит, перевести деньги на «безопасный счет» и тому подобное. Повторюсь, при странном звонке, не вступайте в диалог, просто кладите трубку».

Ольга ЧИКИРЕВА.