Ситуация: цифровое мошенничество

Развитие новых технологий значительно упростило нашу жизнь, в том числе в области финансов. Теперь проводить денежные операции стало проще, достаточно воспользоваться онлайн-банком или позвонить по телефону. К сожалению, этим пользуются и мошенники, тем более что удаленность и анонимность новых коммуникаций им на руку: благодаря прогрессу их становится сложнее поймать. Этот буклет посвящен основным способам телефонного и интернет-мошенничества и тому, как от них защититься.

ИНТЕРНЕТ-МОШЕННИЧЕСТВО

Способов обмануть вас в Интернете огромное количество, каждому из них можно было бы посвятить отдельную брошюру. Все они отличаются друг от друга и требуют от мошенников разных ухищрений — от простого умения убеждать до сложных хакерских технологий. Мы остановимся на наиболее распространенных способах мошенничества, которые не устаревают десятилетиями и от которых вполне реально защититься.

Фишинг

Самым популярным и одновременно самым прибыльным для мошенников способом интернет-мошенничества является фишинг. Он работает просто: вы по ошибке сами вводите данные своей банковской карточки или логин с паролем от онлайн-банка на мошенническом сайте, злоумышленники получают эти данные и обчищают ваш счет до последней копейки.

Что это за мошеннические сайты?

- *Полные копии интернет-странички вашего банка.* Эти страницы полностью, за исключением адреса, похожи на оригинал, но на самом деле никак не связаны с банком. Введя на них свои данные, вы потеряете деньги. Попасть на них можно, совершив ошибку при наборе адреса сайта или перейдя по ссылке. Зачастую мошенники покупают рекламу у поисковиков, и тогда, введя в «Яндексе» или Google запрос с названием своего банка, в одной из первых строк поисковой выдачи вы получите ссылку на сайт-подделку.
- *Поддельные интернет-магазины.* Они могут как копировать известные магазины и агрегаторы (такое распространено, например, с агрегаторами авиабилетов), так и быть непохожими на них. Впрочем, и у тех, и у других технология одинакова: они предлагают огромные скидки и специальные предложения, переманивая клиентов у реальных продавцов. Зачастую мошенники покупают рекламу в соцсетях. Покупатели видят в объявлении знакомый бренд, но не замечают, что сайт на самом деле с брендом не связан. Люди пытаются совершить покупку, вбивают свои данные — и вместо покупки лишаются всех денег с карты.
- *Интернет-инвесторы.* Вообще, доверить свои деньги какому-то сайту в Интернете, который обещает крупные доходы, — дело сомнительное. Чаще всего подобные инвесторы ничего инвестировать даже не пытаются, а просто снимают деньги с вашего счета, используя данные, которые вы передали мошенникам.

Подарки с подвохом

Некоторые мошенники действуют более тонко. Они рассчитывают, что ради наживы вы будете готовы на сомнительные финансовые операции. Самый банальный вариант такого обмана — так называемые нигерийские письма, которые одно время рассылались сотнями и тысячами. Их автор, якобы опальный нигерийский олигарх, просил получателей переслать ему деньги, чтобы он мог отправить получателю миллионы, которые хочет вывезти из своей страны. После транша от получателя «нигерийский олигарх» обычно бесследно исчезал.

Некоторые мошенники создают страничку, на которой вы объявляетесь победителем лотереи, и все, что вам нужно, чтобы получить приз, — это ввести данные своей банковской карты или логин и пароль от онлайн-банка. В лучшем случае у вас спишут всю сумму, которая есть на банковской карте. В худшем случае сайт попросит ввести СМС-код, который на самом деле является кодом безопасности и позволит мошенникам заполучить доступ к вашему личному кабинету на сайте банка. В результате мошенники обчистят все ваши счета.

В таком типе мошенничества сочетаются фальшивый подарок и фишинг: очень часто сайты с призами мимикри-

руют под сайты банков, которые решили сделать приятное своим вкладчикам. Похож будет и адрес, отличаться он будет на одну-две буквы, и, если не обращать внимание на такие детали, обнаружить подвох невозможно.

«Новые законы»

Многие мошенники пытаются заработать не на страсти к наживе, а на вере в «доброе государство». Делается это так: вы получаете сообщение (как вариант — звонок) об изменении законодательства, благодаря которому произошел перерасчет ваших налоговых поступлений или будущей пенсии. Из сообщения следует, что государство хочет вернуть вам часть денег, которую вы ему «переплатили». Иногда мошенники приводят «доказательства» — в сообщении обычно содержится ссылка, отдаленно напоминающая адрес сайта государственной организации, где вы можете по паспортным данным найти свой профиль и сумму, которую вам «должно» государство. На самом деле, конечно, и сумма, и сам сайт, и вся эта история — просто выдумка.

Далее все зависит от фантазии мошенников.
Обычно они поступают двумя способами.

1. Вытягивают из вас деньги за каждое действие: за доступ к базе данных, за получение той или иной информации, за перевод денег на счет и т. п. В результате, конечно, никаких денег вы не получаете, только тратите.
2. Мошенники просят у вас номер карты, на которую нужно перевести деньги, и персональные данные, в частности CVV-код. С таким набором данных они могут легко снять все деньги с вашего счета.

Этот тип мошенничества отличает психологизм: преступники играют на нашей мечте об идеальном «заботливом государстве», которое поддерживает своих граждан и даже готово просто «дарить» им деньги.

Работа, за которую надо приплачивать

Схожим образом действуют некоторые сайты, предлагающие заработок. В объявлениях они обещают быструю и непыльную работу — обычно из дома, не требующую каких-то специальных навыков. Кандидату обещают хорошую и стабильную зарплату, правда, никакой договор с ним не заключают, а просят просто выполнять определенные задания.

Жертва в итоге не получает ничего. Как только дело доходит до зарплаты, мошенники выписывают комиссию за перевод денег, за открытие счета и за кучу других мелочей. Обычно работник слишком поздно понимает, что зарплаты не будет, — к этому моменту немало его денег уже оказывается у злоумышленников.

Как уберечься от интернет-жуликов

Мы перечислили далеко не все виды интернет-мошенничества, но большинство из них работает именно так. Чтобы не пострадать от жуликов, соблюдайте следующие правила финансовой безопасности в Сети.

1. Следите за сайтами, которые вы посещаете. Не всякий сайт, похожий по оформлению и названию на сайт банка, им является. Сделать сайт, идентичный оригинальному по оформлению, не очень сложно и зачастую даже не очень дорого. Обращайте внимание не только на дизайн, но и на адресную строку. Если в ней немного отличающийся адрес сайта банка или нестандартное написание известной компании, это мошенники. Обращайте внимание и на начальную часть адресной строки: адреса, которые начинаются с «https», более безопасны, тогда как начинающиеся с «http» крайне рискованны.
2. Не сообщайте никому СМС-пароли. Единственное место, где ими можно пользоваться, — это платежная страница вашего банка.
3. Не храните данные в ненадежном месте, откуда их легко можно украсть. Например, в соцсетях (их регулярно взламывают), в телефоне.
4. Никогда не платите «работодателю» деньги за устройство на удаленную работу. Настоящие компании платят вам за работу, а не просят деньги за работу с вас.
5. Если вас просят выслать деньги сейчас, чтобы получить много денег потом, даже не надейтесь, что эти «много денег» вы когда-нибудь получите.
6. Игнорируйте письма о проблемах с вашими счетами. Банки никогда не рассылают такие письма по электронной почте или в соцсетях.
7. Не давайте в долг незнакомцам в Интернете: нет никаких гарантий, что деньги вам вернут.
8. Подумайте трижды, совершая покупку в Интернете. Не кажется ли цена, которую вам предлагают, подозрительно низкой? Помните, что отменить сделку в Сети очень сложно.
9. Проявляйте здравый смысл! Никто не будет просто так дарить вам деньги, а вот отобрать их могут запросто.

МОБИЛЬНОЕ МОШЕННИЧЕСТВО

Способы телефонного мошенничества по своей сути часто похожи на мошенничество в Интернете. Отличается лишь техническая сторона. Однако есть среди них и специфические разновидности.

Звонок от «сотрудника»

Наиболее популярная разновидность телефонного мошенничества — звонок от «оператора банка», который под любым предлогом старается выманить у вас данные вашей карты. Обычно это выглядит так. Вам звонит (или пишет СМС) с короткого номера человек, представляющийся работником службы безопасности банка. Он сообщает, что банк заметил какую-то подозрительную активность на ваших счетах, например странный платеж картой. В связи с этим он предлагает вам отменить платеж, но для этого ему нужны ваши данные.

Сверка, согласно легенде, нужна для того, чтобы убедиться, что человек, с которым «оператор»-мошенник разговаривает, действительно владелец карты. Сначала он просит назвать имя и фамилию, потом номер карты и срок ее действия. Мошенник заявляет, что все верно, и клиенту остается сказать CVV-код с обратной стороны карты. После того как вы его сообщаете, собеседник бросает трубку и, используя этот код, списывает с вашей карты все деньги.

«Блокировка» карты

В другой популярной истории, которую мошенники рассказывают наивным гражданам, фигурирует блокировка карты. В этом случае обычно не звонят, а рассылают СМС-сообщения от имени сотрудников Центрального банка России или банка, выпустившего карту, о том, что она заблокирована. В остальном технология та же: запутать клиента, внушить, что он в опасности и что только мошенник может ему помочь.

Технологии выкачивания денег могут различаться. Иногда пишут СМС с просьбой перезвонить по указанному номеру, после чего с мобильного счета жертвы списывают все деньги. Любой контакт с мошенниками может ударить по вашему кошельку.

Выгодное предложение

Многие мошенники пользуются доверчивостью граждан, предлагая им в СМС-сообщениях или звонках «уникальные предложения» — товары и услуги. Иногда это делают даже от лица Центрального банка России, который вообще не работает с физическими лицами и по закону не может высылать никакие деньги гражданам. Людям обещают «высокодоходный накопительный сертификат», для приобретения которого надо перевести деньги на счет «представителя ЦБ». Как только деньги переводятся, этот «представитель» куда-то исчезает.

Как отличить мошенника по телефону?

В отличие от интернет-мошенников, которые зачастую придумывают абсолютно нереальные истории, мобильные мошенники отсылают к случаям, которые действительно могут произойти. Тем не менее есть способы понять, кто с вами общается по телефону: представитель банка или жулик. **Обращайте внимание на следующие признаки.**

1. Сотрудник банка не обращается к вам по имени. В настоящем банке должны знать, как вас зовут. Из соображений вежливости вас будут называть по имени или имени и отчеству. У мошенников таких данных, скорее всего, нет, поэтому, если ваш собеседник не знает, как вас зовут, кладите трубку.
2. Сотрудник банка хочет узнать ваши личные данные. Вообще-то у банка есть все данные о вашем счете, и сотрудник банка может узнать их в своей организации. Если собеседник утверждает, что он просто хочет удостовериться, что это вы, если он на чем-то настаивает и запугивает вас, скажите, что сами съездите в офис банка и во всем разберетесь.
3. Сотрудник банка обещает произвести операции по телефону. Все операции вы можете совершить сами с помощью онлайн-банка или непосредственно в отделении банка. По телефону нельзя разблокировать банковскую карту, в то время как мошенники очень часто предлагают именно это.
4. Нестыковки. Мошенники обычно хорошо продумывают разговор, но не просчитывают все возможные варианты. Их может выбить из колеи затянувшийся разговор, подробные расспросы с вашей стороны. Если собеседник нехотя рассказывает о себе, своем начальстве или отделе и вы чувствуете, что эти вопросы его смутили, это мошенник.
5. Собеседник вас торопит. Сотруднику нет смысла вас торопить, а вот мошеннику важно, чтобы вы не успели как следует все обдумать и совершили ошибку.

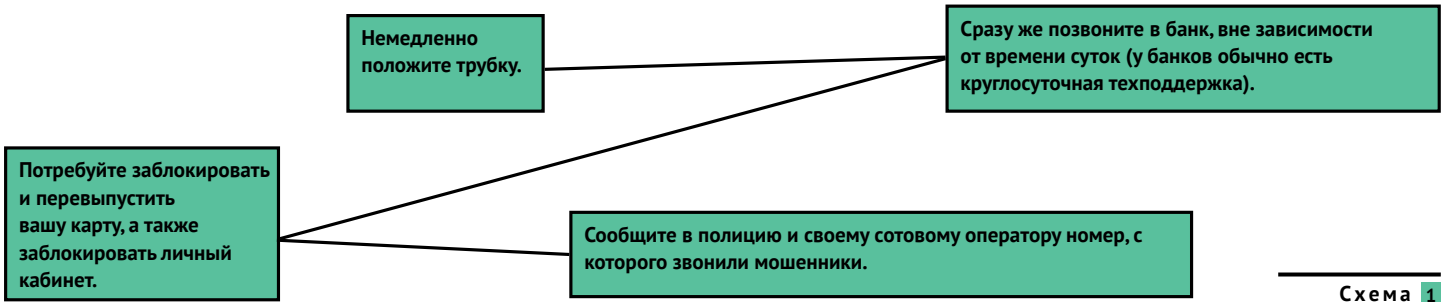

Схема 1

Что делать, если я все-таки сказал незнакомцам свои данные?

Если вам позвонил мошенник и вы по неосторожности выдали ему свои данные, будь то CVV-код вашей карты или пароль от онлайн-банка, действуйте следующим образом. (схема 1)

Если вы проделаете все это сразу же, то вы, скорее всего, успеете защитить свои деньги до того, как мошенники переведут их на свой счет. В худшем случае они украдут только деньги с карточки — вклады они украсть точно не успеют. Банки неохотно возвращают украденные деньги на счет, поэтому лучше действуйте как можно скорее, пока вы ничего не потеряли.

Дополнительные меры предосторожности

Чтобы не стать жертвой ни описанных выше мошенничеств, ни других способов обмана через сотовую связь и СМС, запомните следующее.

1. Не открывайте ссылки из сообщений с неизвестных и подозрительных номеров. В лучшем случае с вас снимут деньги, в худшем — вовлекут в мошенническую схему.
2. Не переходите по ссылкам и не звоните по телефонам, по которым вас просят позвонить в сообщениях с неизвестных номеров или с номеров, напоминающих номера банков, — это точно жулики.
3. Не посылайте СМС на короткие номера, о которых ничего не знаете, — это может обойтись в круглую сумму.
4. Никогда не сообщайте по телефону свои персональные данные людям, которые вам звонят, — те, кому это надо, обычно эти данные знают. Можно позвонить в организацию, представителями которой себя называют звонящие, — так вы точно убедитесь в том, что это мошенники.
5. Не верьте звонкам и СМС, в которых у вас требуют взятку, сообщают, что ваш родственник в опасности, пострадал или совершил преступление, что ему нужна помощь, — это тоже почти всегда мошенники. Перезвоните родственнику и спросите, что происходит. Скорее всего, он даже не знает, что кто-то просит деньги от его имени или для его «защиты». Даже если родственник не берет трубку, не спешите соглашаться, возможно, мошенники специально блокируют его телефон. Позвоните другим родным, соседям родственника, дайте себе время обдумать ситуацию.
6. Не храните всю важную информацию в телефоне. Во-первых, хранить всю информацию в одном месте — плохая идея, во-вторых, с мобильного телефона данные не так сложно украсть.

Подготовлено по заказу Министерства финансов Российской Федерации в ходе реализации совместного проекта Российской Федерации и Международного банка реконструкции и развития «Содействие повышению уровня финансовой грамотности населения и развитию финансового образования в Российской Федерации» в рамках «Конкурсной поддержки инициатив в области развития финансовой грамотности и защиты прав потребителей».
ООО «АНСЭП-Центр». 620142, г. Екатеринбург, ул. Щорса, д. 51Б. финшок.рф, www.ansep.ru. Рисунки Алексея Меринова.
Отпечатано в ООО «Группа М типография» Юридический адрес: 197376, Санкт-Петербург г., Реки Карповки набережная, дом № 5, корпус 3 комната 5, Тел/факс 325-24-26, 325-10-60. ИНН 7813293772. Заказ: 948637 Тираж: 3 000 экземпляров. Дата выпуска: 03.10.2018 г.

Финшок.рф