ФИНАНСЫ

ЦЕНТР
ЗАЩИТЫ ПРАВ ГРАЖДАН

справедливо-центр.рф
8-800-755-55-77

КАК ЗАЩИТИТЬ ДЕНЬГИ ОТ ИНТЕРНЕТ-МОШЕННИКОВ

Способы цифрового мошенничества
Дополнительная защита счета и банковской карты
Что делать, если украли деньги со счета

Программа правового просвещения граждан в 2019 году

ЦЕНТР ЗАЩИТЫ ПРАВ ГРАЖДАН
справедливо-центр.рф
8-800-755-55-77

КАК ЗАЩИТИТЬ ДЕНЬГИ ОТ ИНТЕРНЕТ-МОШЕННИКОВ

Способы цифрового мошенничества
Дополнительная защита счета и банковской карты
Что делать, если украли деньги со счета

21 век фактически перевел нашу финансовую деятельность в цифровой формат. Сегодня уже трудно встретить человека, который не имеет счет в банке. Мы получаем зарплату на карту и расплачиваемся ей же в магазинах, управляем своими финансами в личном электронном кабинете, пересылаем друг другу деньги онлайн.

Но там, где появляются новые возможности, неизбежно возникают и новые опасности. Мошенники моментально освоили новые «экологические ниши». И изобретают все новые и новые уловки в попытках завладеть вашими финансами. В этой статье мы расскажем, как распознать банковское мошенничество и обезопасить свои средства в мире безналичных расчетов и онлайн-банкинга.

Преступления в сфере мошенничества с банковскими картами можно условно разделить на две группы:

Первая – связана со взломом и кражей данных (паролей, PIN-кодов и других данных) без ведома владельца и их последующим использованием.

Вторая – когда мошенники вступают в контакт с владельцем счета и втираются к нему в доверие. После чего тем или иным образом вынуждают человека сообщить реквизиты карты или даже перевести деньги на нужный счет. То есть в карман мошенникам.

ОСНОВНЫЕ ВИДЫ МОШЕННИЧЕСТВА ПО БАНКОВСКИМ КАРТАМ

Ниже подробно рассмотрим три основных вида мошенничества с банковскими картами. А затем разберем механизмы, которые позволят им противостоять.

ВИД №1 – ЦИФРОВОЕ МОШЕННИЧЕСТВО (КАРДИНГ)

Кардинг – один из самых массовых видов мошеннических операций, связанных напрямую с банковскими картами. Сюда относится использование украденных карт, подделка карт и т.д.

Кардинг условно делится на два вида:

1. Скимминг – самый высокотехнологичный вид мошенничества. На банкомат устанавливаются специальное устройство (скиммер) и скрытая видеокамера, а иногда даже поддельная клавиатура поверх настоящей. Скиммер считывает магнитную полосу карты (или встроенный чип) и копирует данные. Камера или поддельная клавиатура фиксируют ввод PIN-кода. После этого у мошенников в ру-

ках оказываются все необходимые данные для доступа к вашему счету.

2. Фишинг – создание точной копии сайта банка, интернет-магазина или электронного кошелька. На фальшивый сайт направляют с помощью интернет-рассылок или СМС от имени банка или магазина, которые содержат ссылки на нужную страницу. Затем под разными предлогами пользователей просят сообщить свои персональные данные. Более того, есть вирусные программы, которые при входе в личный кабинет перенаправляют владельца на копию-фальшивку сайта.

ВИД №2 – МОШЕННИЧЕСТВО В СОЦИАЛЬНЫХ СЕТЯХ

Еще 10-15 лет назад о таком виде мошенничества никто даже и не мог подумать. Но с активным внедрением соцсетей в нашу повседневную жизнь, в нее активно пытаются внедриться и мошенники. Которые пользуются доверием пользователей.

Один из самых классических примеров – взлом страницы друга владельца карты. То есть мошенник взламывает страничку и получает доступ ко всем личным перепискам человека. После чего ищет жертву, у которой под видом владельца страницы (а значит друга/знакомого жертвы) просит одолжить денег.

Это может быть просто некая сумма в долг переводом на банковскую карту (обычно сумма относительно небольшая, чтобы не вызвать лишних подо-

зрений) или же просьба скинуть деньги на номер телефона. С которого потом мошенник переводит деньги на свою карту/счет/онлайн-кошелек.

Мошенники-профаны начинают рассылку всем друзьям по переписке подряд. Более умные мошенники сначала внимательно читают и анализируют переписки – к кому взломанный пользователь мог бы обратиться за деньгами, а к кому нет. Нередко даже копируют стиль автора. После чего пишут определенному кругу лиц и зачастую получают свое.

ВИД №3 – ПСЕВДОБАНКОВСКОЕ МОШЕННИЧЕСТВО

В последнее время распространен еще один вид мошенничества, когда обманщик звонит и прикидывается сотрудником вашего банка. Обычно звонят такие мошенники с московского номера, обращаются по имени-отчеству (личные данные человек узнает заранее), представляются службой безопасности банка и сообщают, что с вашего счета кто-то пытался увести деньги.

Напрямую в этом случае деньги никто не выманивает и коды сообщить не просит. Здесь «разводят» очень грамотно. Иногда так, что поначалу даже не возникает никаких подозрений. Человек на том конце провода общается как банковский сотрудник, апеллирует банковскими терминами, сообщает, например, что якобы была попытка снятия средств. Задает вопросы, к примеру, пытался ли снять конкретную сумму владелец карты, давал ли он кому-нибудь данные банковской карты и т.д.

И уже дальше в зависимости от предлога и импровизации, прощупав жертву, мошенник пытается выведать данные карты. Это может быть все что угодно, начиная от номера карты и секретного кода, заканчивая датой ее окончания или «правильным» написанием фамилии и имени владельца карты.

Заполучив даже часть этих данных, мошенник с легкостью сможет перевести деньги с карты жертвы. В лучшем случае снимут часть денег (зависит от баланса/лимита на переводы и пр.), а в худшем – вообще все деньги с карты жертвы.

МЕРЫ ЗАЩИТЫ ОТ ОСНОВНЫХ ВИДОВ БАНКОВСКОГО МОШЕННИЧЕСТВА

Как защититься от кардинга (скимминга и фишинга)

Чтобы защититься от скимминга, то есть считывания данных с вашей банковской карты, по возможности пользуйтесь одним

и тем же банкоматом. Лучше делать это в отделении банка или в крупном торговом центре, а не где-нибудь в непонятном темном переулке в дальнем районе города.

В любом случае всегда внимательно осматривайте банкомат на наличие подключенных посторонних устройств и проверяйте клавиатуру. Она не должна быть накладной. При обнаружении любых подозрительных изменений внешнего вида банкомата лучше всего не пользоваться им. Обязательно позвоните на горячую линию банка и предупредите сотрудников о возможной попытке саботировать работу устройства.

Чтобы защититься от фишинга, то есть попадания на возможный фейковый сайт банка/интернет-магазина и работы с ним, внимательно проверяйте URL-адрес интернет-страницы. Он указан в строке браузера наверху экрана. Сверьте имя сайта с официальной интернет-страницей финорганизации/магазина до окончание ссылки на .ru/.com/.рф и т.д. Если в своей основной части домен не совпадает и в нем есть посторонние буквенные приписки, черточки или символы, вероятнее всего это мошенники.

Кроме того, если вы частый пользователь конкретного банка/сайта магазина, вы наверняка знакомы с его особенностями. Поэтому обращайте внимание на любые отклонения и странности в работе анимации, логотипе, цветах и фоне, каталогизировании разделов и вообще на работу сайта в целом. Зачастую мошенники собирают сайт «на коленке», поэтому даже если внешне он будет похож на оригинал, наверняка при переходе большинство ссылок на нем окажутся «битыми» (будут открываться с ошибками).

Как защититься от мошенничества в социальных сетях?

Здесь все гораздо проще. Если друг в социальной сети попросил перевести вам средства (неважно на телефон, на лечение кошки или просто в долг), сперва проверьте, так ли это на самом деле. Проще всего будет позвонить этому человеку и уточнить все детали по телефону, а уже потом принимать решение.

Если позвонить у вас возможности нет, тогда попереписывайтесь. Но не в коем случае не открывайте никакие подозрительные присланные ссылки. Попробуйте спросить у собеседника что-нибудь такое, ответ на что знает только он, и информации об этом нет в истории переписки. В этом случае мошенник, вероятнее всего, «завалится», начнет вести себя странно или вовсе прекратит диалог.

Не забудьте сообщить о взломе администрации социальной сети (для временной блокировки взломанного аккаунта), возможным другим жертвам и, конечно, самому хозяину странички. Также на всякий случай мы рекомендуем сменить пароль от аккаунта соцсети и электронной почты. Поскольку сегодня существует масса фишинговых программ, которые мошенники используют для удаленного отслеживания активности пользователя-жертвы.

Как защититься от банковских мошенников?

Вывести фейковых работников банка на чистую воду может оказаться несколько сложнее, чем «друга» по переписке.

Конечно, многие мошенники действуют на удачу и, поняв, что у них ничего не вышло, вешают трубку. Но есть и мошенники-профессионалы, разговор с которыми может мало чем отличаться от настоящего сотрудника банка.

Прежде всего, обратите внимание на номер, с которого вам позвонили. Пробейте его через поисковик в интернете. Есть вероятность, что информация по нему найдется быстро. Вне зависимости от результата поиска, попытайтесь задать собеседнику наводящие вопросы: что именно произошло, почему позвонили, почему от клиента требуются конкретные данные.

Даже если вам ответят аргументированно, никаких данных, вроде номера карты, ее владельца, срока окончания действия и уж тем более CVV/CVC-кода, давать потенциальному сотруднику банка нельзя. Если что-то из этого заинтересует собеседника, значит это мошенник. Поскольку вся необходимая для работы с клиентом информация у реальных сотрудников службы безопасности банка есть в базе.

Как только вы убедились, что говорите с мошенником, сразу положите трубку. Далее обратитесь на горячую линию вашего банка (при необходимости можно и в ближайший офис) и сообщите им о случившемся. Также продиктуйте номер телефона, с которого вам звонили, чтобы его занесли в базу нежелательных номеров. А в заключение сами внесите номер мошенников в черный список вашего устройства, чтобы по нему вас больше не беспокоили.

КАК ПОВЫСИТЬ УРОВЕНЬ ЗАЩИТЫ ПРЯМО СЕЙЧАС?

С каждым годом цифровые мошенники, конечно, придумывают все новые и новые способы обмана владельцев банковских карт. Но, к сожалению, граждане сплошь и рядом сами помогают им узнать свои личные данные. Например, зачастую можно увидеть картину, как на кассе или даже у банкомата человек набирает PIN-код на глазах у всех. И даже не пытается закрыть клавиатуру. Так делать не стоит.

Всегда следует думать как о физической безопасности ваших личных данных, так и о безопасности информационной. Ведь даже если у человека не украдут карту, то всегда могут узнать ее реквизиты. А вкупе со знанием PIN-кода или CVV/CVC-кода – это прямой доступ к счету. Поэтому всегда будьте настороже.

Неважно, когда просто достаете карту из кошелька, когда расплачиваетесь ей в магазине или покупаете товары через Интернет. Всегда!

МЕРЫ ЗАЩИТЫ ПРИ ДИСТАНЦИОННОМ БАНКОВСКОМ ОБСЛУЖИВАНИИ

Здесь необходимо уделить внимание двум вещам – вашим электронным девайсам и вашим личным данным в интернете (электронная почта и номер телефона, пароли и возможности доступа к личным кабинетам и сетевым службам, безопасность интернет-соединения и т.д.).

Первое. Необходимо защитить от вторжения ваш смартфон или компьютер, с которого вы производите банковские операции. Надо сделать так, чтобы в ваше отсутствие никто не мог воспользоваться вашим девайсом и получить доступ в ваш личный кабинет или к вашим данным.

Помните, что вы можете пострадать даже в отсутствие злого умысла. Так, сегодня дети удивительно находчивы, и в один прекрасный день вы можете обнаружить, что ваш ребенок совершил кое-какие операции с вашими счетами. Причем сделать это он может, сам того не зная.

Второе. По возможности лучше вообще не пользоваться интернет-банкингом с мобильных устройств, а делать это только с личного компьютера. Но сегодняшние реалии не всегда позволяют так поступать. Поэтому используйте надежные пароли (их необходимо периодически менять), блокировку экрана (со включенным паролем/отпечатком пальца/распознаванием лица для доступа в смартфон), шифровку телефона (эта опция

есть в настройках многих аппаратов). Все это снизит вероятность утечки информации.

Особую осторожность необходимо соблюдать при работе за компьютером в офисе, в гостях или в интернет-кафе: отключайте сохранение паролей в браузере, а по завершении работы очищайте историю просмотров. Используйте VPN-соединение при работе через сети Wi-Fi в публичных местах.

В остальном правила безопасности те же, что и для любых безналичных расчетов.

ЧТО ДЕЛАТЬ, ЕСЛИ ВАС ВСЕ-ТАКИ ОБМАНУЛИ

К сожалению, иногда по тем или иным причинам мошенникам удается получить доступ к банковской карте/счету жертвы. Если такая ситуация произошла, необходимо оперативно принять специальные меры. Которые воспрепятствуют возможности пользоваться картой и снимать с нее деньги.

МОШЕННИКИ ПОЛУЧИЛИ ДОСТУП К БАНКОВСКОЙ КАРТЕ

Если у вас возникли подозрения, что кто-то получил доступ к вашей карте/счету, прежде всего, немедленно отключите интернет на вашем устройстве (на случай, если каким-то образом мошенники получили доступ к данным через него). После чего немедленно позвоните в контактный центр вашего банка и сообщите о подозрении на взлом. Заблокируйте вашу учетную запись, все карты и счета (их может быть несколько).

Сразу после этого следуйте рекомендациям сотрудника банка. Вам нужно будет сменить логин и пароль вашей учетной записи.

А также поменять пароли на электронной почте и в основных социальных сетях, поскольку взлом мог произойти через них.

Далее необходимо написать несколько заявлений. В банке потребуется написать заявление о блокировке и перевыпуске карты (в течение двух недель). Также мы рекомендуем написать и направить заявления о хищении карты/личных данных карты и средств (если они были похищены) в правоохранительные органы – в полицию и прокуратуру. Не факт, что это поможет найти злоумышленников или вернуть ваши деньги. Но так у вас будет дополнительное подтверждение, что вы оказались жертвой мошенников. Последнее особенно полезно, если хищение средств произошло по вине банка, поскольку тогда ответственность за пропажу денег ляжет именно на него.

ВАЖНО ЗНАТЬ!

Федеральный закон «О национальной платежной системе» обязывает банк вернуть похищенные с банковской карты средства. Но только при соблюдении ряда условий. Во-первых, клиент должен сообщить о краже в течение суток после получения от банка уведомления об операции. Во-вторых, компрометация данных карты не должна произойти по вине клиента (когда он сам выдал личные данные мошеннику). Если же банк не уведомил пострадавшего клиента о какой-либо операции по карте после сообщения об ее утрате или же разрешил ее, вся ответственность ляжет на плечи банка.

БАЗОВЫЕ РЕКОМЕНДАЦИИ ВСЕМ ПОЛЬЗОВАТЕЛЯМ БАНКОВСКИХ КАРТ

Существует ряд базовых правил пользования банковскими картами (как дебетовыми и овердрафтными, так и кредитными), которые всем владельцам карт стоит соблюдать:

1. Правило «Храните PIN-код отдельно от карты» известно всем, но лучше всего не хранить его нигде. Самый безопасный вариант – придумать такой код, который вы вспомните всегда и в любой ситуации. Разумеется, нужно избегать очевидных вариантов, вроде собственной даты рождения, первых цифр номера телефона и т.д.

2. Избегайте банкоматов в малолюдных темных местах. Именно ими чаще всего пользуются мошенники для скимминга. Даже если банкомат расположен в людном месте, проверяйте его на наличие посторонних предметов и оригинальность его клавиатуры, чтобы избежать считывания данных вашей карты и набранного PIN-кода.

3. Если вы передали карту кассиру, платеж должен совершаться на ваших глазах. Помните, что с карты можно быстро снять реквизиты, включая CVV/CVC код, или даже полностью скопировать магнитную полосу и изготовить дубликат вашей карты.

4. Не давайте номер своей карты для участия в различных лотереях и розыгрышах. Ни один честный розыгрыш лотерейных билетов/призов не будет использовать эти данные. В интернете для этого обычно используются ники, уникальные id того или иного сайта или же номер телефона (последнее гораздо реже).

5. Не сообщайте свои PIN-коды и пароли никому, включая сотрудников банка. У настоящего сотрудника банка все основные ваши данные, которые необходимы для работы с кли-

ентом, всегда будут отражены в компьютерной базе банка. Максимум, что вас могут попросить назвать в определенных случаях, это кодовое слово (для некоторых операций/действий).

6. Не оставляйте карту в салоне автомобиля или в другом месте, где с нее могут снять данные. Ведь с современной техникой даже стекло и расстояние будет не помехой.

7. Уничтожайте все ненужные чеки, билеты и квитанции, в которых указаны ваши личные данные или реквизиты вашей карты. И уж тем более не допускайте, чтобы документ с вашими данными не оказался на снимке, который вы выкладываете в соцсети. Сегодня любая информация может быть использована против вас.

8. При каждой крупной покупке храните все документы, включая чеки и квитанции, минимум в течение 45 дней (а лучше – дольше). В идеале заведите отдельную папку, куда будете складывать все чеки, желательно в хронологическом порядке.

9. Регулярно отслеживайте операции, совершенные по карте: подключите услугу СМС-банк, запрашивайте банковские выписки. Это не только позволит вам следить за расходами, но и поможет грамотнее планировать ваш бюджет и привьет определенные навыки финансовой грамотности.

10. Установите суточный лимит снятия средств. Тогда даже в случае хищения карты мошенники не смогут снять всю сумму сразу. Что позволит вам оперативно заблокировать карту и избежать потери всех средств.

Мошенничество с банковскими картами – не просто неприятная проблема. Это труднодоказуемое и труднорасследуемое преступление. К сожалению, российское финансовое законодательство еще только догоняет западные страны. В связи с этим присутствует много правовых пробелов, и часто у правоохранителей нет ни людей подходящей квалификации для расследования подобных случаев мошенничества, ни ресурсов для возврата средств их законному владельцу.

Профилактика в этом вопросе обойдется вам значительно дешевле, чем ликвидация последствий мошенничества. Поэтому будьте бдительны и повышайте вашу финансовую грамотность!

ЦЕНТР
ЗАЩИТЫ ПРАВ ГРАЖДАН
справедливо-центр.рф
8-800-755-55-77

Телефон горячей линии

8 800 755 55 77

Сайт Фонда «Центр защиты прав граждан»

справедливо-центр.рф

Пособие: «КАК ПОПАСТЬ В ГОСУДАРСТВЕННУЮ ПРОГРАММУ
ПО БЛАГОУСТРОЙСТВУ ДВОРОВ»

Изготовитель: ООО «Статус Офис», 143306, Московская область,
г. Наро-Фоминск, ул. Ленина, д. 28, офис 2, тел. 499-707-17-91.
Заказчик: Фонд «Центр защиты прав граждан» ИНН 9710010183,
Тираж 7 000 экз. 2018 год
Распространяется бесплатно

В ТРУДНОЕ ВРЕМЯ РЯДОМ С ТОБОЙ!