СОДЕРЖАНИЕ

Безопасные покупки в интернете

Онлайн-шоппинг быстрее и удобнее, чем традиционные походы по магазинам. Но и рисков больше: шанс встретить киберпреступников в разы выше, чем реальных грабителей. Делимся советами, как сделать покупки в сети максимально безопасными.

Чаще всего мошеннические операции с банковскими картами происходят именно в интернете. И с каждым годом финансовые потери людей растут. Например, в 2018 году мошенники украли с карт в 1,5 раза больше денег, чем в 2017.

Где подстерегает опасность?

Риск возникает во время покупок на сайтах и в приложениях, использования электронных кошельков, мобильного и интернет-банкинга.

Главное оружие киберпреступников – фишинг. Другими словами – выуживание конфиденциальных данных: паролей, реквизитов карты или счета для кражи денег с карты или из интернет-кошелька.

Воры играют на психологии: рассылают СМС, электронные письма и сообщения в чатах с просьбой, например, «подтвердить аккаунт» или «восстановить доступ к банковскому счету».

Сообщения содержат ссылку на специальный фишинговый сайт – сайт-двойник банка, госоргана или другой организации. Если вы не заметили подмены, то после ввода своего логина, пароля интернет-банка или реквизитов карты сразу переведете деньги мошенникам.

Как защититься от фишинга и других видов кибермошенничества?

1. **Пользуйтесь только личными устройствами**

   Делайте покупки, заходите в свой интернет-банк или мобильный банк только с личного компьютера, планшета и смартфона. Обязательно ставьте на них пароль.

Если вы потеряете телефон или планшет, к которым подключено СМС-информирование или мобильный банк, срочно позвоните в банк и отключите от утерянного номера все услуги.

2. **Защититесь от вирусов**

   Обязательно поставьте антивирус на всех своих устройствах, включая мобильные, и регулярно обновляйте их. Хороший антивирусный пакет всегда включает защиту от фишинга и вирусных программ.

3. **Выбирайте безопасные сайты**
   - Никогда не переходите по ссылкам из писем и СМС от неизвестных отправителей. Даже если сообщение пришло от знакомого вам человека или организации, не спешите открывать их. Возможно, у мошенников появился доступ к их аккаунтам и они хотят получить доступ и к вашим данным.
   - Набирайте интернет-адрес банка вручную, а еще лучше – сохраняйте в закладках адреса ваших банков, госорганов и других организаций.
   - Всегда проверяйте адресную строку браузера. Иногда можно попасть на фишинговый сайт при переходе с одной страницы известного вам портала на другую.
   - Делайте покупки только на сайтах, которые обеспечивают безопасное соединение. Адрес такого ресурса начинается с https://. В адресной строке есть значок в виде закрытого замка.
   - Еще лучше – проверять сертификат безопасности сайта. Для этого нажмите на значок замка и в открывшемся окне выберите «Просмотр сертификатов». Убедитесь, что сертификат выдан именно тому сайту, на котором вы находитесь, и срок его действия еще не закончился.
   - Выбирайте известные интернет-магазины и сервисы. Изучите отзывы о них от других пользователей. Лучше всего посмотреть отзывы на нескольких независимых сайтах. Добросовестный продавец всегда дает полную информацию о себе: телефон, адрес и прочие контактные данные.

4. **Используйте систему безопасных платежей**

   Когда переходите на страницу оплаты, ищите логотипы программ MasterCard SecureCode, Verified by Visa и Mir Accept. Эти программы с

помощью технологии 3D-Secure дополнительно защищают вас во время покупок в интернете.

Если онлайн-магазин поддерживает эту технологию, после ввода реквизитов карты он перенаправит вас на безопасную интернет-страницу банка. Для подтверждения покупки банк отправит СМС с одноразовым паролем на номер мобильного телефона, привязанный к карте или счету. Никому не сообщайте этот код – просто введите его в специальное поле на странице оплаты.

5. **Заведите отдельную карту для покупок в интернете**

   Если вы часто делаете покупки или оплачиваете услуги в интернете, например телефонную связь или штрафы, безопаснее использовать для этого отдельную карту. Вносите на нее лишь ту сумму, которую собираетесь потратить, и установите лимит по количеству операций в сутки. Некоторые банки позволяют создать виртуальные карты, которые действительны только для одной онлайн-покупки.

6. **Никому не сообщайте персональную информацию**

   Чаще всего в краже средств со счета виноваты вовсе не банки, платежные системы или онлайн-магазины, а сами доверчивые пользователи.

   Мошенники знают множество уловок, чтобы втереться к вам в доверие. И ваша задача на эти уловки не попасться. Никогда не сообщайте посторонним данные своей карты, персональные данные и коды из СМС.

   Никому не говорите ваш ПИН-код и код проверки подлинности карты (CVV2/CVC2/ППК2) – последние три цифры на ее оборотной стороне. Даже сотрудники банка не вправе требовать от вас эти данные. Если кто-либо пытается их узнать, будьте уверены – это мошенник.

   Тех же правил следует придерживаться и при пользовании интернет-кошельком: никогда и никому не сообщайте логин и пароль от своего аккаунта.

7. **Подключите СМС-оповещения об операциях по карте**

   В этом случае вы сразу же узнаете о платеже, которого вы не совершали, и сможете быстро отреагировать: заблокировать карту и опротестовать операцию.

Что делать, если деньги все-таки украли?

- **Заблокируйте карту**

  Если с карты списали деньги без вашего ведома, позвоните в банк и заблокируйте карту.

  > **Номер горячей линии банка указан на оборотной стороне карты. Запишите этот телефон и храните в отдельном кармане – на случай, если украдут телефон или кошелек.**

  Так же нужно поступить, если вы потеряли карту или даже просто подозреваете, что ее данные стали известны посторонним людям.

- **Опротестуйте операцию**

  В тот же день, когда вы получили уведомление о незаконной операции (максимум – на следующий), обратитесь в отделение банка. Запросите выписку по счету и напишите заявление о несогласии с операцией, которую не совершали. Экземпляр заявления с отметкой банка, что оно принято, оставьте у себя.

  Если банк докажет, что вы нарушили правила использования карты, то вернуть деньги не получится. Например, когда вы сами сообщили кому-то реквизиты своей карты, верификационный номер с ее оборотной стороны или ПИН-код.

  > **Случаи возврата денег, когда они ушли с карты без вашего ведома, регулирует Федеральный закон «О национальной платежной системе».**

  Но этот закон не поможет в случае проблем с электронным кошельком, обезличенными предоплаченными картами и другими неперсонифицированными платежными средствами.

- **Обратитесь в полицию**

  Расследованием преступлений в интернете занимается Бюро специальных технических мероприятий (БСТМ) МВД России. Подайте заявление в территориальное учреждение БСТМ. Можно просто написать заявление в отделение полиции по месту жительства. Чем быстрее вы это сделаете, тем больше шансов найти преступников и вернуть деньги.

Иточник: https://fincult.info/article/bezopasnye-pokupki-v-internete/

ДАВАЙ ПОГОВОРИМ О БЕЗОПАСНОСТИ

Какие мошенничества часто встречаются в нашей жизни? Рассмотрим несколько из них.

Света сидела в кафе с подружками, и когда принесли счет, решила расплатиться картой. Официант взял карту и пошел проводить оплату, а света осталась с подругами. Правильно ли она поступила?

Если оставить банковскую карту без присмотра, мошенники могут получить ее данные и украсть деньги. Верить людям и в людей – прекрасно, но некоторые из них пользуются чужой наивностью и неосторожностью, чтобы лишить всех денег.

В 2012 году два московских официанта обворовали посетителей кафе и ресторанов на общую сумму 10 миллионов рублей. Они уносили карту из поля зрения владельца «для совершения оплаты», копировали данные – и в последующие дни снимали со счетов все имевшиеся на них деньги. Масштабы подобных преступлений с тех пор выросли.

Основной способ защитить деньги – сохранять бдительность! Не отдавай карту в руки продавцам, официантам и даже друзьям. Требуй, чтобы оплату проводили в твоем присутствии, и не посещай заведения, где так не принято.

При оплате картой всегда внимательно следи за ней и пресекай любые подозрительные манипуляции продавца или официанта. Не стесняйся – ведь речь о твоих деньгах.

Есть и более «продвинутый» и надежный способ. Закажи в банке дополнительную карту: она будет привязана к твоему счету, но ее реквизиты будут отличаться от реквизитов основной. Заблаговременно переводи на дополнительную карту нужные тебе суммы для оплаты покупок в магазинах или посиделок в кафе – и плати там этой картой. Даже если карту скопирует злоумышленник, большая часть денег останется в безопасности.

Если же ты еще установишь суточный лимит расходов по дополнительной карте и запретишь покупки с нее в Интернете, – мошеннику вообще будет нечем поживиться... И, конечно, блокируй карту, если подозреваешь, что в заведении что-то нечисто.

Лене на электронную почту пришло письмо, что она выиграла в лотерею миллион рублей! Чтобы его получить, нужно просто ввести в специальную форму данные маминой банковской карты. Что делать?

Письма о выигрышах в лотерею (а еще об огромном наследстве из Африки или благотворительном пожертвовании в адрес твоей семьи) рассылают мошенники – они пользуются наивностью и незнанием детей, чтобы украсть средства со счетов родителей. Никогда нельзя передавать сведения о картах родителей или своей собственной неизвестным людям и организациям.

Как это работает? Ты указываешь платежные реквизиты карты, а мошенники быстро снимают с нее деньги. И надеемся, что карта не кредитная – иначе снять могут больше, чем на карте было. А расплачиваться придется твоим родителям...

Даже по ссылкам из таких «писем счастья» переходить опасно: на сайте мошенников может быть вредоносное программное обеспечение, способное передавать важные сведения с твоего компьютера ребятам, которые уж придумают, как воспользоваться ими во вред!

Если же неприятность уже произошла: ты сообщил незнакомым людям реквизиты карты кого-то из родителей – срочно расскажи об этом маме, чтобы она успела заблокировать карту до того, как с нее исчезнут деньги. Если повезет – все обойдется.

Лизе позвонил человек, представился сотрудником банка и сказал, что для каких-то банковских целей нужно уточнить пароль от ее карты. Должна ли Лиза сообщить свой пароль?

Давай поговорим о безопасности

Начнем с очевидного. Как Лиза может быть уверена, что звонят именно из банка? Способов выяснить, в каком банке у нее выпущена карта, много. Базы телефонных номеров обычных граждан можно найти в Интернете. А чтобы представиться сотрудником банка, достаточно уверенности в голосе и прописанных «скриптов» (сценариев разговора).

Согласно правилам банков, их сотрудники и операторы колл-центров ни под каким предлогом не имеет права выяснять платежные реквизиты клиентов банка, например, CVV-код.

Да, иногда они звонят, чтобы поинтересоваться, насколько ты доволен качеством услуг банка. Иногда могут звонить, чтобы предложить выгодные условия по депозитам или кредитам. В остальных случаях будь уверен: твой собеседник – мошенник.

Если сомневаешься, закончи разговор, набери номер справочной своего банка и уточни, действительно ли тебе оттуда звонили с предложением или запросом об информации.

Пароль от карты ни в коем случае нельзя сообщать по телефону. Нельзя также сообщать точное написание имени и фамилии, срок действия карты, CVV-код с ее обратной стороны. Всей этой информации с избытком хватит, чтобы избавить тебя от денег, хранящихся на твоей карте.

Виталик собирается продать через интернет свой старый плеер. Покупатель просит Виталика сфотографировать карту с двух сторон и прислать, чтобы он мог перевести деньги. Это правильный способ оплаты?

Для получения любого платежа на карту необходимо и достаточно лишь сообщить покупателю свой номер карты. Иногда покупатель уточняет, действительно ли ты Василий Иванович Т., который высвечивается у него в реквизитах при проведении платежа. В том чтобы подтвердить, что ты действительно Василий – ничего страшного нет.

Если же покупатель просит/требует фото обеих сторон банковской карты, ты имеешь дело с мошенником. Чтобы произвести платеж в интернете, нужно указать номер карты, срок ее действия, точные имя-фамилию (как напечатаны на карте), плюс CVV-код с обратной стороны карты. Этого достаточно, чтобы оплатить покупку и для перевода денег с карты третьему лицу. Теперь представь, что ВСЕ эти сведения известны постороннему человеку (которого ты в лицо не видел, а лишь обсуждал с ним детали купли-продажи через интернет!).

Что произойдет дальше? Правильно!
С твоей карты со скоростью света исчезнут деньги.

Вывод:
сообщать посторонним людям что-либо,
кроме номера карты и имени-отчества, нельзя!

Володя собирается купить и оплатить картой джинсы в интернет-магазине, адрес которого начинается с http://. Это безопасно?

Если ты посоветовал Володе держаться надежных магазинов с адресом https, ты очень бдителен, молодец! Если уверен, что знакомого названия магазина для безопасного шопинга в сети достаточно, читай дальше.

Способов отъема денег у населения тысячи, и один из них – онлайн-шоппинг. Причем речь сейчас вовсе не о бестолковых покупках. Выбирая и оплачивая желанные покупки, человек временами теряет голову – а с ней и деньги.

Какие опасности подстерегают нас на сайтах интернет-магазинов?

фишинг, т.е. выяснение платежных реквизитов и паролей наивного покупателя через сайт-подделку (сайт, который названием, оформлением и даже адресной строкой очень похож на оригинальный, надежный сайт);

банальный обман, т.е. получение за свои деньги товара другого качества, более дешевого товара или даже просто потеря денег (оплата ушла – товар не пришел).

Есть и другие способы интернет-мошенничества, не ленись узнавать о них больше из любых надежных источников.

А мы расскажем о безопасных покупках в интернете.

Важно, чтобы адрес сайта начинался с https – это надежное, закодированное интернет-соединение, и мошенники держатся от него подальше.

Пользуйся популярными магазинами, желательно, чтобы у них были не только виртуальные площадки, но и реальные торговые точки по всей стране или в крупных городах, либо чтобы это были всероссийские «гиганты», которые у всех на слуху.

Обращай внимание на адресную строку – держись подальше от «неточных» (поддельных) названий.

Не переходи по спамовым ссылкам, подписывайся на официальные рассылки интересных тебе магазинов – и переходи на сайты по ссылкам только из таких рассылок.

Остановимся вкратце и на покупках через торговые площадки и доски объявлений, такие как Авито, Юла, Из рук в руки. Несколько правил безопасности:

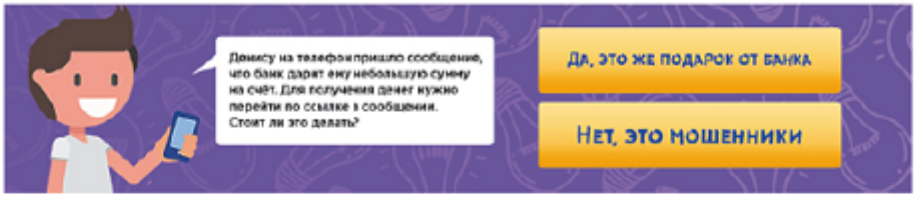
не оплачивай покупку с рук заранее – только по факту;

проверяй качество товара, прежде чем его оплатить;

если продавец находится не в твоем городе, то договаривайся о каких-либо гарантиях получения товара (если не получается оплатить покупку по факту получения, предлагай схему «50/50» или оплату наложенным платежом при получении товара на почте);

тщательно изучай профиль продавца, отзывы о нем, его рейтинг в системе.

Денису на телефон пришло сообщение, что банк дарит ему небольшую сумму на счет. Для получения денег нужно перейти по ссылке в сообщении. Стоит ли это делать?



Какова главная характеристика людей, решивших зарабатывать мошенничеством? Изобретательность!

С зарождения человечества мошенники придумали миллиарды способов вытянуть из наивных или недостаточно бдительных людей деньги, и каждый день придумывают еще по одному.

А уж цифровые и мобильные технологии подарили мошенникам дополнительный «козырь» – анонимность. Врага теперь можно заподозрить и даже вычислить, но почти невозможно найти и наказать.

Закончим с лирикой – и перейдем к практике. Денису следует знать, что мошенники могут рассылать сообщения якобы от имени банка и таким образом распространять вирусы и программы, которые крадут данные с телефонов – в том числе информацию о картах.

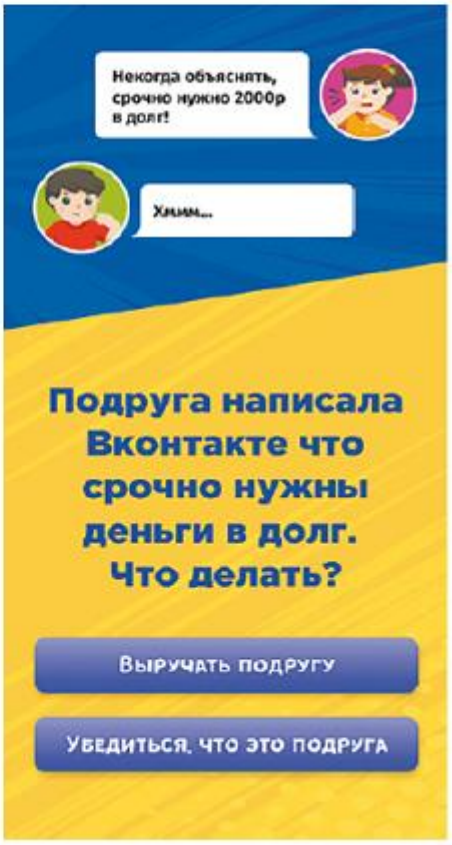
Если тебе пришла такая смс (якобы от банка, якобы ты что-то выиграл, или

наоборот, тебе нужно подтвердить или ввести какую-то конфиденциальную информацию) – ни в коем случае нельзя переходить по ссылкам и передавать данные о себе и своих картах и счетах.

Если соблазн очень велик, нужно позвонить в банк и узнать, действительно ли проводится какая-то акция с призами. Можно даже уточнить, действительно ли ты что-то в этой акции выиграл.

Подруга написала Сереже Вконтакте, что ей срочно нужно 2000 рублей в долг. Объяснять, в чем дело, некогда, все потом, главное перевести деньги прямо сейчас. Что следует делать Сереже?

Существует огромное количество видов и вариантов мошенничества, и с каждым годом это число растет. Один из распространенных видов мошенничества связан со взломом профилей в интернете. Злоумышленник подбирает логин-пароль от страницы ВКонтакте или Фейсбуке, пишет душещипательное послание о том, как ему нужна твоя помощь – и очень надеется на то, что человек, с чьего аккаунта отправлено письмо, тебе близок и дорог. А потому ты не задумываясь ринешься выручать этого человека. При плохом раскладе деньги уйдут «в никуда», а ваши отношения с другом, которого взломали, испортятся.



Но опасности легко избежать. Задай уточняющий вопрос, ответ на который может знать только тот человек, который попросил о помощи. Впрочем, здесь есть «подводные камни»: во-первых, мошенник может просто угадать или найти ответ на вопрос на страницах профиля; во-вторых, часто мошенники – хорошие психологи, которые умело «заговаривают зубы». Есть и более эффективный способ убедиться, что именно близкий тебе человек просит помощи. Просто позвони ему (или ей)!

Источник: http://keskil14.ru/finansovaya-gramotnost-bankovskie-vklady-pokupki-v-internete-semejnyj-byudzhet/