|  |
| --- |
| **Как не потерять деньги в сети** |

**По данным Сбербанка в последнее время значительно выросло число случаев мошенничества против клиентов коммерческих банков, управляющих своими счетами по сети Интернет через системы дистанционного банковского обслуживания, в том числе и через Сбербанк ОнЛ@йн. Элементарная осторожность и соблюдение базовых правил безопасности при работе с банковскими сервисами, помогут сохранить деньги от посягательств третьих лиц.**

Мошенники, «работающие» с банковскими картами, чрезвычайно изобретательны и придумали сотни способов отъема денег у честных граждан. Для того, чтобы понимать степень опасности, надо не только знать, как выглядят все используемые ими схемы, но и стараться не подставлять себя под удар.

**Будь осторожен**

При работе со своими счетами в системе «Сбербанк ОнЛ@йн» следует быть такими же внимательными и бдительными, как при обращении с наличными средствами в Вашем кошельке.

https://www.potrebitel-russia.ru/uploads/images/simvol_4.jpgИспользуйте современное антивирусное программное обеспечение и следите за его регулярным обновлением;

https://www.potrebitel-russia.ru/uploads/images/simvol_4.jpgРегулярно выполняйте антивирусную проверку для своевременного обнаружения вредоносных программ;

https://www.potrebitel-russia.ru/uploads/images/simvol_4.jpgСвоевременно устанавливайте обновления операционной системы, рекомендуемые компанией-производителем;

https://www.potrebitel-russia.ru/uploads/images/simvol_4.jpgИспользуйте дополнительное программное обеспечение: персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «спам»- рассылок и пр.

При любых подозрениях на компрометацию паролей (постоянного или разовых) посторонними лицами (в т.ч. представившихся сотрудниками банка) или запросах на выполнение неинициированных Вами операций, следует незамедлительно обратиться в службу помощи Банка: (495)-500-0005, (495)-788-9272 , 8-800-555-5550, 8-800-200-3747.

**Опасная подделка**

Если бы все мы соблюдали принятые в обществе правила поведения, нам было бы легко и просто жить. Но жизнь всегда сложнее любых схем и, в большинстве случаев, в условиях дефицита времени и постоянного стресса даже самые осторожные пользователи Сети попадаются на незамысловатые уловки мошенников. Довольно часто злоумышленники, распространяют вирусные программы через различные интернет-ресурсы – от социальных сетей до обычных новостных сайтов. Клиент, компьютер которого заражен, при попытке войти в личный кабинет на страничке банка перенаправляется на «фишинговые» сайты, которые внешне практически не отличаются от подлинных сайтов.

На поддельном сайте Вас могут попросить ввести идентификаторы и пароли, мобильный телефон и другие персональные данные, необходимые мошенникам. Для защиты от подобных действий в «Сбербанк **[ОнЛ@йн](mailto:%D0%9E%D0%BD%D0%9B@%D0%B9%D0%BD)**» предусмотрено подтверждение всех финансовых операций одноразовым SMS-паролем, который отправляется вместе с реквизитами самой операции. Помните, что одноразовый пароль – это один из важнейших элементов безопасности при работе с кредитной картой в Сети. Этот пароль никому нельзя сообщать. Также категорически запрещается указывать полученные в SMS-сообщении реквизиты, которые относятся к операции, которую Вы не совершали.

Иногда для входа в личный кабинет под различными предлогами у вас запрашивают номер мобильного телефона. Такая операция может проводиться в незащищенном режиме. Иконки браузера, указывающие на работу в защищенном режиме, неактивны. При входе на странный сайт в браузере может появиться предупреждение, что сертификату безопасности сайта нельзя доверять. Адрес такого псевдосайта может не совпадать с официальными адресами «Сбербанк **[ОнЛ@йн](mailto:%D0%9E%D0%BD%D0%9B@%D0%B9%D0%BD)**» (esk.sbrf.ru и online.sberbank.ru), на нем могут отсутствовать или быть неактивными ссылки по мерам борьбы с мошенничеством.

**Правила противодействия**

Как бороться с такой схемой? Очень просто – с помощью инструкции по безопасности. Поверьте, этого достаточно.

https://www.potrebitel-russia.ru/uploads/images/simvol_4.jpg Сбербанк никогда не запрашивает пароли для отмены операций в «Сбербанк ОнЛ@йн». Если Вам предлагается ввести пароль для отмены операции, то прекратите сеанс использования услуги и срочно обратитесь в банк.

https://www.potrebitel-russia.ru/uploads/images/simvol_4.jpg Для входа в личный кабинет требуется только идентификатор и пароль/одноразовый пароль. В случае, если от Вас требуют любую другую персональную информацию, немедленно прекратите сеанс использования услуги и срочно обратитесь в банк.

https://www.potrebitel-russia.ru/uploads/images/simvol_4.jpgВводить одноразовые пароли следует только в том случае, если операция инициирована Вами. При получении SMS с одноразовым паролем внимательно ознакомьтесь с его содержанием. Вводить пароль в систему следует, только если реквизиты Вашей операции соответствуют реквизитам в полученном SMS-сообщении.

https://www.potrebitel-russia.ru/uploads/images/simvol_4.jpgВ системе «Сбербанк ОнЛ@йн» отмена операций не предусмотрена. Если вы получили сообщение об отмене операции – это действия мошенников. Сразу же прекратите сеанс и срочно обратитесь в банк.

**Странные банкоматы**

Довольно часто объектом для атаки мошенников становятся банкоматы, на которых устанавливают специальные программы, выявляющие ПИН-коды, или же монтируются миниатюрные видеокамеры.

До проведения операции в банкомате осмотрите его лицевую часть, в частности, поверхность над ПИН-клавиатурой и устройство для приема карты в банкомат. В этих местах не должно находиться прикрепленных посторонних предметов или рекламных буклетов. При обнаружении подозрительных устройств незамедлительно сообщите об этом сотрудникам банка или позвоните по телефону контактного центра.

При проведении операции с вводом ПИН-кода ВСЕГДА прикрывайте клавиатуру – например, свободной рукой. Это не позволит мошенникам увидеть ПИН-код или записать его на видеокамеру. Замки доступа по картам в специальные помещения, где устанавливаются банкоматы, не должны требовать ввода ПИН-кода. Если требуется ввести ПИН-код – незамедлительно обратитесь в банк (разумеется, не вводя код). Если же вы все-таки ввели свой ПИН, постарайтесь сразу же заблокировать карту.

При приеме и возврате карты банкоматом не толкайте и не выдергивайте карту до окончания ее прерывистого движения в картоприемнике. Неравномерное движение карты – это не сбой в программе, а необходимое средство защиты пластиковой карты от взлома.

**Опасные SMS**

В последнее время участились случаи мошеннических SMS-рассылок с различных номеров мобильных телефонов или коротких номеров, в которых сообщается о блокировке карты, окончании срока ее действия, изменениях ПИНа и др. Отправители подобных рассылок просят перезвонить на указанный номер мобильного телефона. Все эти сообщения замаскированы под официальные сообщения банка и требуют от Вас каких-либо быстрых действий или ответа.

Специалисты по безопасности Сбербанка России не рекомендуют перезванивать на номер мобильного телефона, указанного в SMS-сообщении, и советуют ни в коем случае не предоставлять какую-либо информацию о реквизитах карты (номере карты, сроке ее действия, ПИН-коде, коде безопасности), или об одноразовых паролях.

В ряде случаев Сбербанк России рассылает собственные информационные SMS-сообщения, но в них обязательно указываются последние цифры номера карты (мошенникам они не известны).

Сотрудники Сбербанка России никогда не запрашивают у клиента информацию о реквизитах карты, пароле/одноразовых паролях. Ни при каких обстоятельствах не сообщайте реквизиты карты позвонившим лицам!

Все SMS-сообщения Сбербанка отправляются только с номера «900». В теле письма указываются только официальные телефоны банка, опубликованные на сайте Сбербанк России.

**Вирусный спам**

Мошенники активно проводят массовые email-рассылки, маскируясь под бренд Сбербанка. Основные цели таких рассылок – заманивание получателей сообщений на сайты-ловушки, на которых мошенники попытаются получить Ваши персональные данные. Часто на таких сайтах размещаются вирусы, заражающие компьютеры при открытии страниц. Получателей писем принуждают открыть файл-вложение, содержащий вирус, или перейти по ссылке для загрузки вирусного файла.

**Есть ряд признаков, указывающих на то, что email-сообщение является мошенническим:**

https://www.potrebitel-russia.ru/uploads/images/simvol_4.jpgсообщения замаскированы под официальные письма банка и требуют от Вас каких-либо быстрых действий или ответа. Например, в адресной строке указаны такие адреса, как Сбербанк ОнЛ@йн (info@sber.ru), Сбербанк России (noreply@sber.ru), Сбербанк Информ (statistics@sber.ru)

https://www.potrebitel-russia.ru/uploads/images/simvol_4.jpgадрес отправителя и тема сообщения замаскированы под обращения от имени банка. Например, «сообщение об увеличении задолженности», «сообщение увеличения долга», «сообщение об увеличение задолженности на ДД.ММ.ГГГГ»;

https://www.potrebitel-russia.ru/uploads/images/simvol_4.jpgписьма содержат ссылки на интернет-ресурсы, похожие на настоящие ресурсы банка.

В большинстве случаев URL-адрес ссылки в письме отличается от официального адреса (www.sberbank.ru), возможно также появление всплывающих окон на официальном сайте, в котором запрашивается ввод или подтверждение Ваших персональных данных. К сообщению прилагается вложение, которое настойчиво рекомендуют открыть, а в самом тексте содержатся явные опечатки или орфографические ошибки.

**Между тем, Сбербанк России никогда:**

https://www.potrebitel-russia.ru/uploads/images/simvol_4.jpgне отправляет сообщения с просьбой подтвердить, обновить или предоставить персональные данные (ФИО, данные документа, удостоверяющего личность, номер мобильного телефона, информацию по банковской карте, CVV, ПИН, кодовое слово и пр.);

https://www.potrebitel-russia.ru/uploads/images/simvol_4.jpgне отправляет сообщения с формой для ввода Ваших персональных данных;

https://www.potrebitel-russia.ru/uploads/images/simvol_4.jpgне просит Вас зайти в личный кабинет системы «Сбербанк ОнлЛа@йн» по ссылкам в письмах.

[**источник**](https://krugdoveriya.mail.ru/articles.html?id=2797)

https://www.potrebitel-russia.ru/?id=573