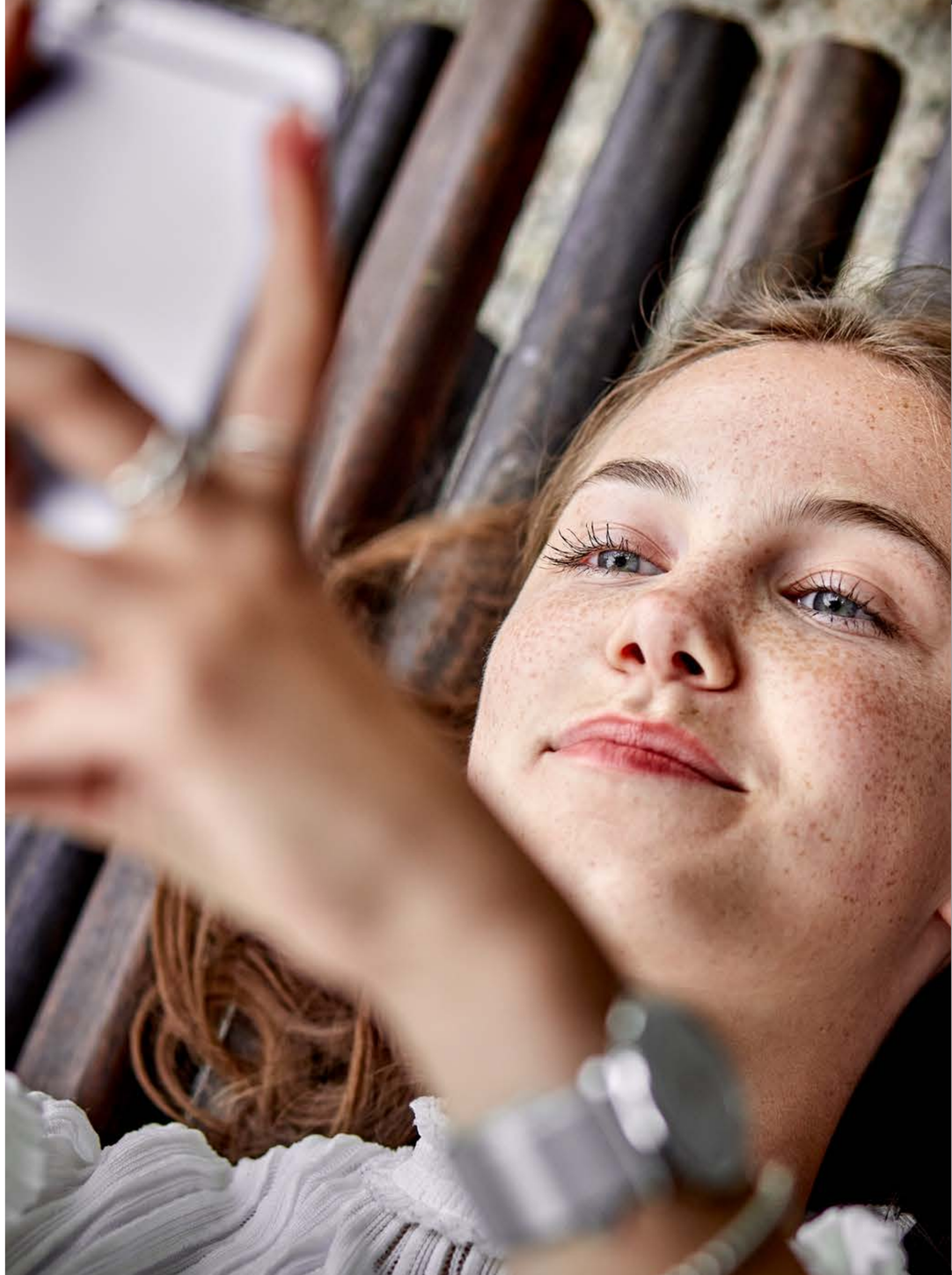
РЕКОМЕНДАЦИИ ДЕРЖАТЕЛЯМ КАРТ И ПОЛЬЗОВАТЕЛЯМ РОСБАНК-ОНЛАЙН

Защитите свои финансы

БУДУЩЕЕ – ЭТО ВЫ

РОСБАНК

SOCIETE GENERALE GROUP



ОГЛАВЛЕНИЕ

1. ИСПОЛЬЗОВАНИЕ КАРТ

1.1. НАЧАЛО ПОЛЬЗОВАНИЯ КАРТОЙ

ОБОРОТНАЯ СТОРОНА КАРТЫ

При получении новой банковской карты, не откладывая, поставьте свою подпись на ее оборотной стороне. Наличие подписи позволит снизить риск использования банковской карты без согласия держателя в случае ее утраты.

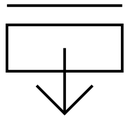
Создайте надежный ПИН-код. Не создавайте простые и очевидные комбинации цифр (0000, 1234, 0852, год своего рождения или пароль от телефона). Не устанавливайте одинаковый ПИН-код на несколько карт.

Не храните ПИН-код вместе с банковской картой, в том числе в чехле телефона, в памяти телефона, и ни в коем случае не записывайте ПИН-код на самой карте.

Не сохраняйте реквизиты цифровой карты Digital на устройстве. Злоумышленники могут получить доступ к устройству и воспользоваться этими данными.

Не сообщайте ПИН-код, CVC/CVV-код, код из СМС никому, это дает возможность совершить снятие денежных средств в банкоматах и покупки в магазинах без ведома клиента. В Банке или где-либо не хранится информация о Ваших ПИН-кодах, сотрудникам эта информация не нужна.

1.2. ОПЕРАЦИИ ПО КАРТЕ В БАНКОМАТАХ



Снимайте наличные в банкоматах РОСБАНКА либо в банкоматах банков-партнёров и известных банков.

Известны случаи обнаружения поддельных банкоматов, принадлежащих несуществующим банкам.

Такие банкоматы не выдают наличность, а лишь копируют данные Вашей карты (в том числе могут записывать Ваш ПИН-код).

Снимайте наличные в банкоматах, которые расположены в отделениях банков.

Не снимайте наличность в банкоматах, на которых есть подозрительно «лишнее» оборудование.

Если банкомат липкий или в царапинах, вполне возможно, что мошенники установили на этот банкомат своё оборудование, чтобы скопировать данные Вашей карты и записать ПИН-код Вашей карты.

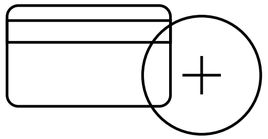
Иногда банкоматы ломаются и захватывают Вашу карту по техническим причинам.

Если такое случилось, позвоните в Банк по телефону и заблокируйте карту прежде, чем Вы отойдёте от банкомата.

Не принимайте помощь и не прислушивайтесь к людям из очереди.

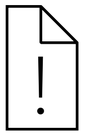
1.3. ОПЕРАЦИИ ПО КАРТЕ В ТСП (МАГАЗИНАХ)

Если терминал поддерживает бесконтактную оплату, рекомендуем Вам производить покупки данным способом. Это быстрее, удобнее и безопаснее.



При оплате в магазинах по ПИН-коду, закрывайте вводимый ПИН рукой, кошельком или рукавом. Старайтесь оплачивать покупки, не передавая карту сотруднику магазина, а если передали – следите, чтобы Ваша карта всегда была на виду.

Перед подтверждением оплаты проверьте сумму на корректность. Бывает, что кассир не там поставил запятую в сумме, и с карты может списаться сумма в 10 раз больше, чем надо.



В случае оплаты покупок картой или токеном, в том числе за границей, если при попытке оплаты вышел «отказ», попросите у кассира чек и сохраните его. Это понадобится, если сумма всё же будет списана (в том числе двойные списания).

1.4. ОПЕРАЦИИ ПО КАРТЕ В РЕСТОРАНАХ

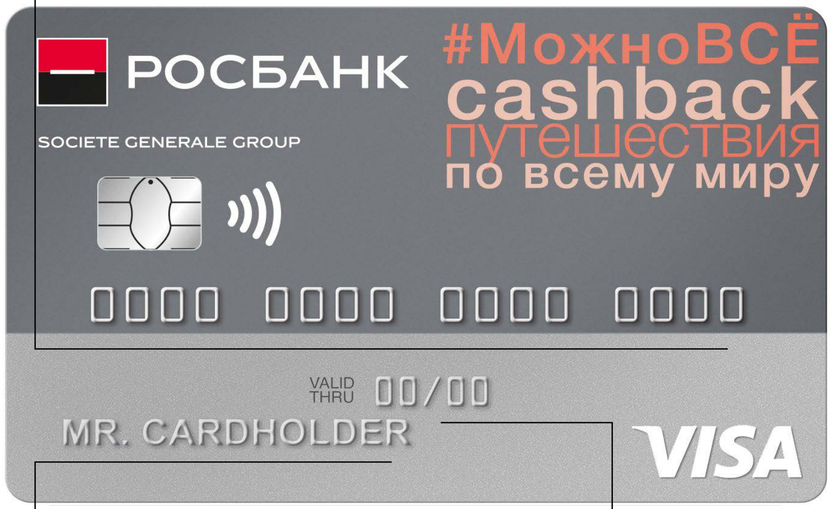
При оплате в ресторанах старайтесь не отдавать карту, а просите принести мобильный терминал либо самостоятельно подойдите к кассе.

Это снизит риск того, что злоумышленники скопируют или сфотографируют Вашу карту. Старайтесь не упускать карту из виду.

1.5. ОПЕРАЦИИ ПО КАРТЕ В ИНТЕРНЕТЕ

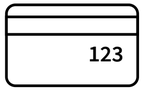
ЛИЦЕВАЯ СТОРОНА КАРТЫ

номер карты



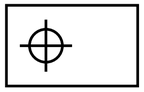
имя и фамилия

срок действия



Для оплаты покупок на интернет-сайтах потребуется ввести:

— полный номер Вашей карты,
— срок действия карты,
— CVC/CVV-код – это последние три цифры на обороте карты.

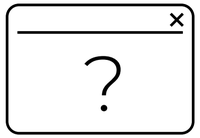


Не храните ПИН-код вместе с банковской картой, в том числе в чехле телефона, в памяти телефона, и ни в коем случае не записывайте ПИН-код на самой карте.

Не сообщайте ПИН-код, CVC/CVV-код, код из СМС никому, это дает возможность совершить снятие денежных средств в банкоматах и покупки в магазинах без ведома клиента.

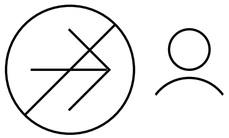
В Банке или где-либо не хранится информация о Ваших ПИН-кодах, сотрудникам эта информация не нужна.

1.5. ОПЕРАЦИИ ПО КАРТЕ В ИНТЕРНЕТЕ: БАЗОВЫЕ ПРАВИЛА



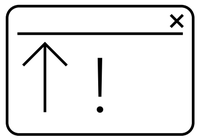
Будьте бдительны при покупке товаров на малоизвестных сайтах.

Скопируйте название сайта и поищите отзывы о нём в любом крупном поисковике.



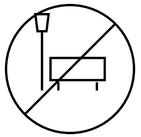
Рекомендуем не переводить оплату на карту физическому лицу при заказе в онлайн-магазинах.

Только реквизиты / платежный агрегатор / оплата курьеру.



Внимательно проверяйте адрес сайта и наличие сертификата безопасности https://

Не вводите на сомнительных сайтах свои персональные данные, данные банковских карт и данные для входа в Росбанк Онлайн



Не проводите через публичную сеть никаких финансовых операций на сайтах.

Если вам все же необходимо периодически совершать какие-то платежи через публичный Wi-Fi, используйте отдельную карту, где лежит небольшая сумма.

1.5. ОПЕРАЦИИ ПО КАРТЕ В ИНТЕРНЕТЕ: ЧТО ТАКОЕ ФИШИНГ

ФИШИНГ — (англ. phishing от fishing «рыбная ловля, выуживание)

Это вид интернет-мошенничества с целью кражи конфиденциальных данных пользователей (чаще всего логинов, паролей, данных лицевых счетов и банковских карт и др.) или установка вредоносного ПО на устройство жертвы.

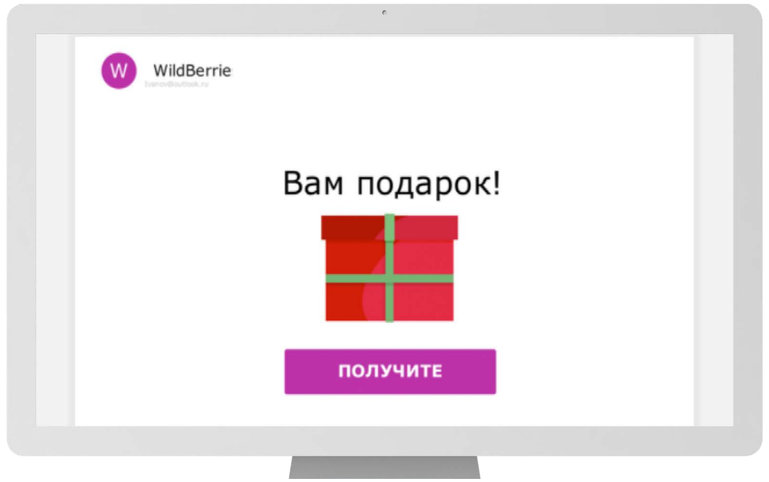
Для получения данных мошенники так же могут создавать копии сайтов различных ресурсов, социальных сетей, сервисов, а так же рассылать письма со ссылками на мошеннические сайты или содержащие вредоносное содержимое.

Обычно мошенники стараются привлечь внимание обещанным вознаграждением или иной выгодой.

1.5. ОПЕРАЦИИ ПО КАРТЕ В ИНТЕРНЕТЕ: ПРИМЕРЫ ФИШИНГОВЫХ ПИСЕМ

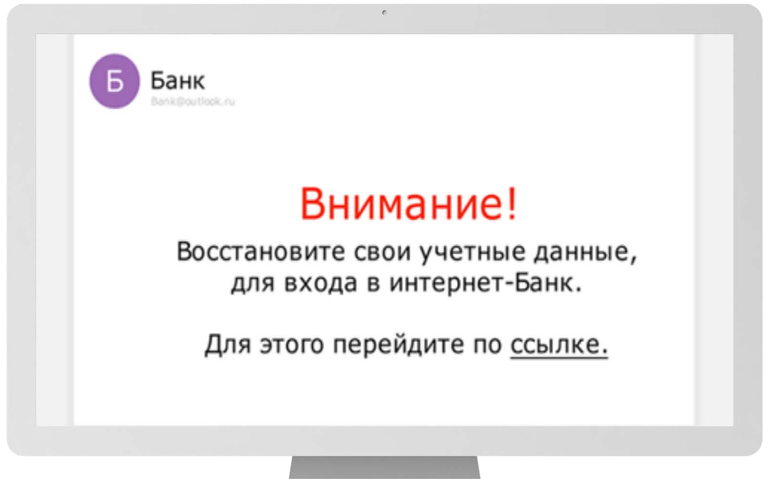
Почтовые рассылки от известных брендов.

Мошенники используют похожие названия брендов и предлагают пользователям принять участие в акции или получить выигрыш



Адресные электронные письма от банков.

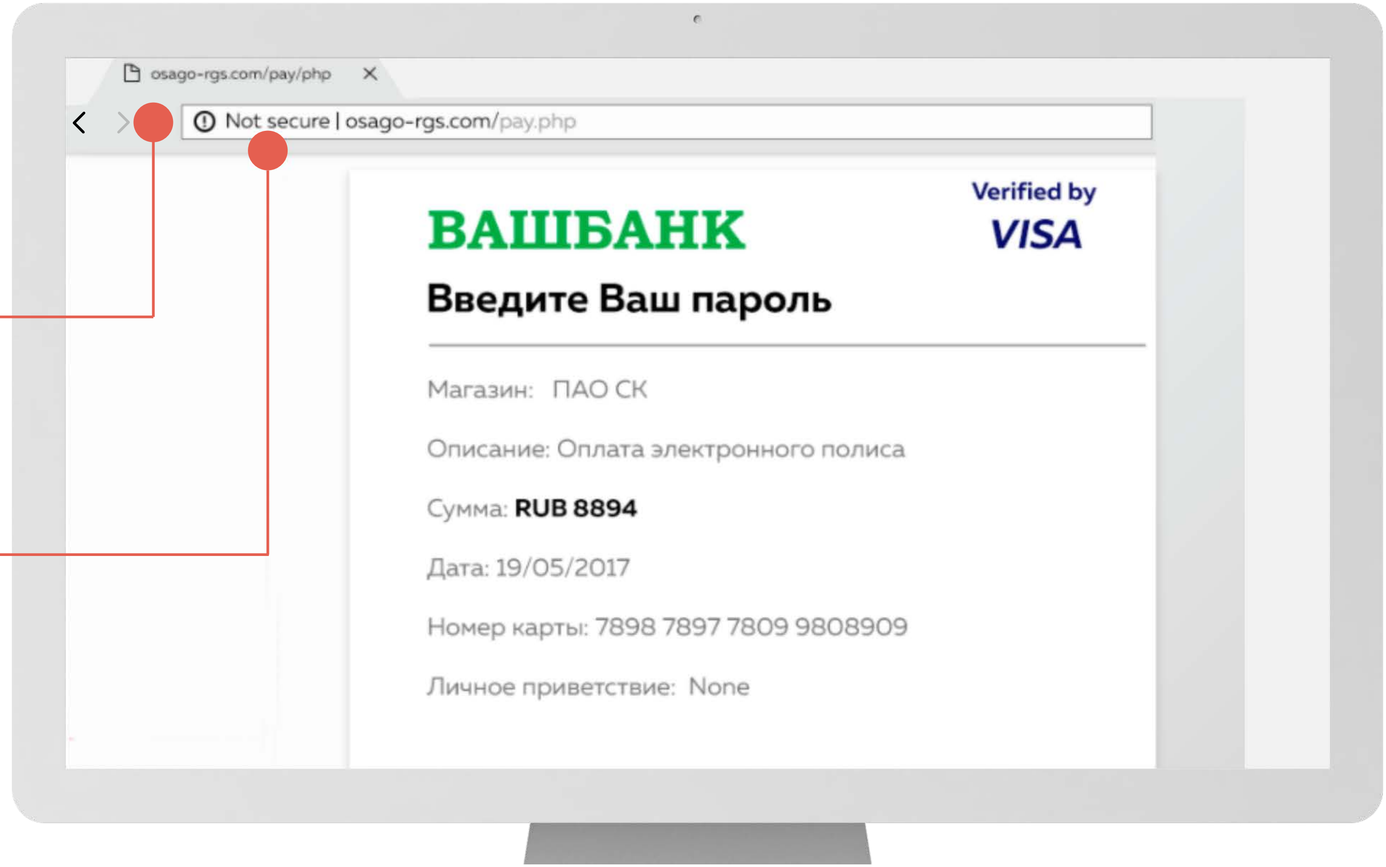
Фишинговое письмо предложит пользователю подтвердить логин и пароль для входа в Интернет-банк, используя специальную веб-форму



1.5. ОПЕРАЦИИ ПО КАРТЕ В ИНТЕРНЕТЕ: ПРИМЕР ФИШИНГОВОГО САЙТА

Протокол шифрования отсутствует

Официальный сайт поставщика услуг имеет другое доменное имя

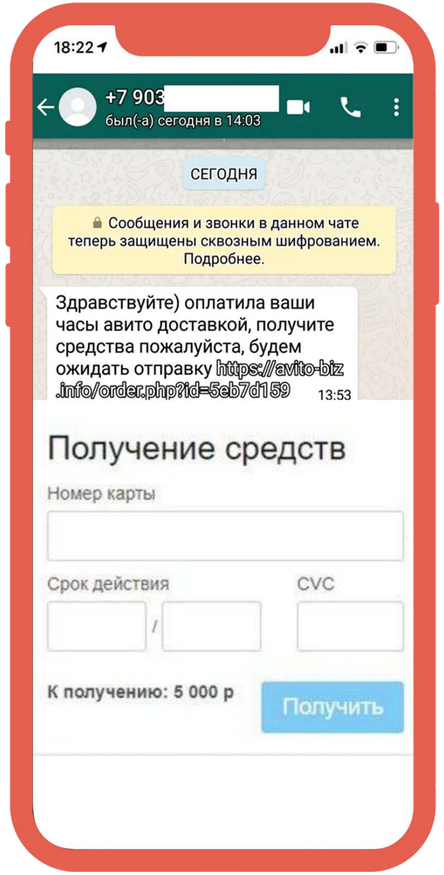


1.5. ОПЕРАЦИИ ПО КАРТЕ В ИНТЕРНЕТЕ: МОШЕННИЧЕСТВО С САЙТАМИ ОБЪЯВЛЕНИЙ

1. Вы выступаете продавцом, по телефону или в переписке к вам обращается мошенник под видом покупателя.

2. Злоумышленник предоставляет ссылку для получения средств, пройдя по которой необходимо указать полные реквизиты своей карты и ввести код подтверждения (в некоторых случаях мошенник просит озвучить ему код из СМС).

3. Далее следует перевод, но НЕ на карту, а списание средств с нее.



На что обратить внимание:

Переписка в стороннем от сервиса объявлений мессенджере.
Ссылка на оплату или получение денег обычно приходит во встроенный мессенджер Avito системным сообщением.
Настоящая ссылка всегда начинается с домена www.avito.ru

1.5. ОПЕРАЦИИ ПО КАРТЕ В ИНТЕРНЕТЕ: РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ОТ ФИШИНГА

Обратите внимание на адрес сайта.

ИмяСайта.ru — так выглядит адрес серьезного магазина или компании. Если домен выглядит так: ИмяМагазина.narod.ru/...-off.ru, или что либо еще — задумайтесь.

— Неизвестный доменный адрес:

к примеру, адрес почтового сервера компании — @компания.ру. Мошенники, рассчитывая на невнимательность клиента, могут изменить его на @компания1.ру. Измененные названия известных брендов: Aplle.com или qoogle.com.

— Мошеннические интернет-магазины –

это сайты-однодневки, они максимально простые. Заспамленные блоками рекламы сайты тоже вызывают вопросы.

— Обращайте внимание на ошибки:

неправильно подсчитанные скидки, пустые страницы.

— Сделайте контрольный звонок.

Проверьте адрес, указанный на сайте, обычно компании выкладывают на сайте схему проезда к офису и фотографии как пройти. Отсутствие номеров телефонов магазина, а также его юридического адреса указывают на неблагонадежность ресурса.

— Обратите внимание на цену товара.

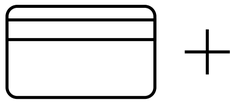
Задумайтесь, если цена слишком низкая. Например, мошенники часто привлекают внимание дешевыми авиабилетами и низкими ценами на электронику.

— В письмах ваше внимание будут пытаться привлечь срочностью вопроса:

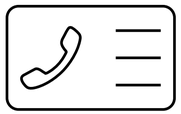
«последнее предупреждение», «срочная проверка», «скорая блокировка» или «внезапный выигрыш».

1.6. ОПЕРАЦИИ ЗА ГРАНИЦЕЙ

Сообщите в банк о поездке
(страны пребывания, период)



Возьмите в поездку несколько карт разных платёжных систем,
но также имейте запас наличных денежных средств, учитывайте возможную конвертацию в валюту счёта



Запишите номера телефонов банка
(используйте контакты только с официального сайта банка, с оборота банковской карты или в мобильном банке)

Удостоверьтесь, что вы подключаетесь к официальной сети Wi-Fi отеля или заведения, в котором вы находитесь.
При входе в РОСБАНК-Онлайн через общественный Wi-Fi, используйте платный VPN. Бесплатный VPN может не шифровать трафик или содержать вредоносный код

2. ОПЕРАЦИИ В МОБИЛЬНОМ И ИНТЕРНЕТ-БАНКЕ

2. ОПЕРАЦИИ В МОБИЛЬНОМ И ИНТЕРНЕТ-БАНКЕ

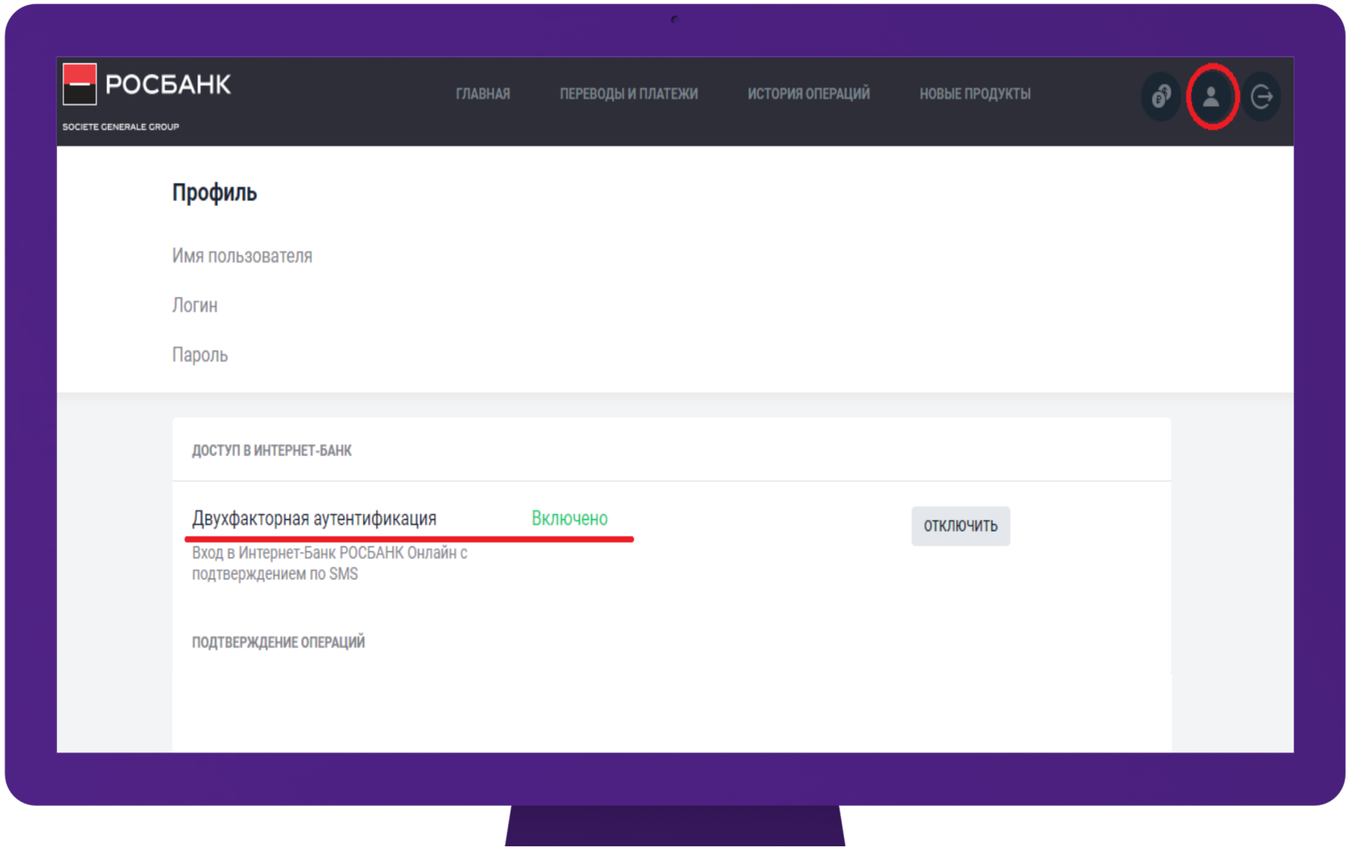
Для подтверждения операций в Интернет-Банке необходимо ввести специальный одноразовый пароль, который Банк направит Вам на контактный номер телефона в виде СМС.

ОБРАТИТЕ ВНИМАНИЕ!

Данные пароли никому нельзя сообщать!

Этот пароль нужен только для проведения операций списания с Вашего счёта.

2. ОПЕРАЦИИ В МОБИЛЬНОМ И ИНТЕРНЕТ-БАНКЕ



Ещё один элемент безопасности РОСБАНК Онлайн – это поддержка двухфакторной аутентификации. То есть подтверждение входа по одноразовому паролю из СМС.

Данная функция опциональна и может быть активирована Вами. Это необходимо, чтобы обезопасить Вас, если мошенникам станут известны Ваши логин и пароль для входа в РОСБАНК-Онлайн.

2.1. БАЗОВЫЕ ПРАВИЛА

1. Скачивайте РОСБАНК Онлайн только из официальных магазинов App Store, Google Play и AppGallery или осуществляйте вход официального сайта rosbank.ru (имеет особую отметку верификации – синяя галочка)

2. Не устанавливайте в качестве пароля/PIN для доступа в систему легко угадываемые данные (например, ПИН-код Вашей банковской карты или дату рождения и пр.).

3. Используйте и регулярно обновляйте на Ваших устройствах антивирус для исключения случаев заражения вредоносным кодом

4. Если Вы получили сообщение, что выполнен вход в Систему, и этот вход совершили не Вы, то немедленно обратитесь в банк

5. В случае утраты устройства, на который установлен РОСБАНК Онлайн, немедленно сообщите об этом в банк для блокировки доступа

3. КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

3.1. Чем звонок из банка отличается от звонка мошенников
3.2. Резюме
3.3. Базовые правила

3.1. ЧЕМ ЗВОНОК ИЗ БАНКА ОТЛИЧАЕТСЯ ОТ ЗВОНКА МОШЕННИКОВ

В последние годы самая популярная схема мошенничества – звонки клиентам банков.

Поскольку в РОСБАНКЕ есть подразделение, которое в круглосуточном режиме и без выходных проводит мониторинг подозрительных операций на предмет наличия признаков мошенничества, мошенники стараются имитировать поведение настоящих сотрудников.

Злоумышленники представляются сотрудниками банка (техническими специалистами, менеджерами, сотрудниками безопасности \ финансового мониторинга и пр.) и под любыми предлогами пытаются получить информацию, которая предназначается только для клиентов и необходима для проведения операций.

ПОЛУЧИТЬ ДОСТУП К СЧЕТУ МОШЕННИКИ МОГУТ ТОЛЬКО В ТОМ СЛУЧАЕ, ЕСЛИ КЛИЕНТ САМ СООБЩИТ СВОИ ДАННЫЕ

3.1. ЧЕМ ЗВОНОК ИЗ БАНКА ОТЛИЧАЕТСЯ ОТ ЗВОНКА МОШЕННИКОВ

ЗВОНОК ИЗ БАНКА

- Сотрудники банка и иных финансовых структур не связываются с клиентами через мессенджеры или социальные сети.
- Сотрудники банка не имеют возможности переводить звонки на сторонние организации. Например, в «безопасность другого банка», а лишь рекомендуют клиенту самостоятельно обратиться в другой банк.
- Специалист не уточняет дополнительных данных по Вашим картам, счетам, вкладам, так как у сотрудника банка есть вся необходимая информация для общения с клиентом.
- Сотрудники во время разговора оперативно блокируют карты в случае мошенничества

ЗВОНОК ОТ МОШЕННИКА

- Как правило, представляются сотрудниками Службы безопасности Банка, Технической поддержки, Правоохранительных органов, Центрального Банка, а так же иногда биржевыми брокерами и т.п.
- Мошенники уточняют, есть ли карты других банков, и могут «соединить» со специалистом службы безопасности стороннего банка, чтобы и с неё списать денежные средства.
- Мошенники сообщают о подозрительной операции по Вашей карте, для этого запрашивают остаток по счёту или вкладу, а для экстренной блокировки просят провести некоторые манипуляции по карте или счёту

3.1. ЧЕМ ЗВОНОК ИЗ БАНКА ОТЛИЧАЕТСЯ ОТ ЗВОНКА МОШЕННИКОВ

СОТРУДНИКИ БАНКА И ДРУГИХ УЧРЕЖДЕНИЙ

НИКОГДА

НЕ ЗАПРАШИВАЮТ
конфиденциальную информацию (например, полный номер карты, PIN и CVC/CVV-коды, код из СМС, данные для входа в Интернет-банк)

НЕ ПРОСЯТ
сообщить ваши данные «роботу в тональном режиме» \ «автоматизированной голосовой системе»

НЕ ТРЕБУЮТ
осуществить перевод средств (через банкомат\ мобильное приложение\ через кассу отделения…)

НЕ ПРЕДЛАГАЮТ
установить дополнительные программы

НЕ ОТПРАВЛЯЮТ
ссылки для установки приложений

Если вас просят назвать что-то из перечисленного, завершите разговор и обратитесь в банк самостоятельно

«СМС нельзя называть обычным сотрудникам, а мне скажите…»

«Для вас есть выгодное предложение, давайте я зайду в Ваш РОСБАНК-Онлайн…»

«Скорее подойдите к банкомату, я вам продиктую Ваши действия…»

«Если вы сейчас же не назовёте мне цифры из СМС, операция пройдёт…»

«Давайте скачаем и установим приложение для телефона, чтобы настроить ваш РОСБАНК-Онлайн…»

3.2. РЕЗЮМЕ

КОМУ НУЖЕН

код подтверждения из СМС, Ваши логины и пароли к РОСБАНК-Онлайн, а также ПИН-код карты, срок её действия и CVC/CVV-код?

- **Вам**
- **мошеннику** !

КОМУ НЕ НУЖЕН

- сотрудникам банков
- техническим специалистам
- сотрудникам контакт-центров
- сотрудникам службы безопасности
- сотрудникам Центрального Банка РФ
- сотрудникам операторов сотовой связи
- сотрудникам Национальной Системы Платёжных Карт

3.3. БАЗОВЫЕ ПРАВИЛА

1 **НЕ СООБЩАЙТЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ**

Только мошенники просят дополнительные «уточнения» по счетам, транзакциям, открытым продуктам и ФИО

2 **ДАННЫЕ КАРТ КОНФИДЕНЦИАЛЬНЫ**

Не разглашайте номера карт, CVC/CVV-коды. Сотрудники банков никогда не запрашивают подобную информацию.

3 **НИКАКОГО СТОРОННЕГО ПО**

Сотрудники банка никогда не просят установить дополнительные программы на ваш телефон или ПК

4 **КОД ИЗ СМС – ТОЛЬКО ДЛЯ ВАС**

Коды из СМС никогда не разглашаются: ни голосом, ни самостоятельным вводом «в тональном режиме роботу по телефону»

5 **КОДОВОЕ СЛОВО – ТОЛЬКО ДЛЯ ВАШЕГО ОБРАЩЕНИЯ В БАНК**

Вам потребуется назвать его для идентификации, только если вы САМИ звоните в банк

НИКАКИХ ПЕРЕВОДОВ СРЕДСТВ В ЦЕЛЯХ «БЕЗОПАСНОСТИ»

Не бывает случаев, когда для сохранности денег нужно перевести их на другой счёт

БУДУЩЕЕ –
ЭТО ВЫ

РОСБАНК

SOCIETE GENERALE GROUP