Финансовая безопасность.
Пособие для пап, мам, бабушек и дедушек.

Седов С.Н.

Copyright ©

Выражаю благодарность Федорову Виталию Владимировичу
Начальнику управления по работе с персоналом ОАО Концерн ПВО «Алмаз-Антей»,
кандидату философских наук. Профессору. Генерал-лейтенанту
за помощь в подготовке материала

КАК ПРАВИЛЬНО ПОЛЬЗОВАТЬСЯ БАНКОВСКОЙ КАРТОЙ.

Поменяйте карту с магнитной полосой на карту с «чипом»- тогда при каждой новой операции будет использован новый код. Случай подделки чипа в мире не зафиксирован!

Не храните и не накапливайте все деньги на одной «зарплатной карте».

Не используйте «зарплатную карту» на отдыхе в магазине или для покупок в «интернет-магазине».

Заведите для этого отдельную карту с чипом и лимитированными суммами. Переводите на неё столько средств, сколько необходимо для покупок.

Вбейте в телефонную книгу номер телефона, указанный на карте.

Не привязывайте карту ко всем своим сбережениям.

Ограничьте регионы снятия наличных с карты.

- По возможности застрахуйте свою карту-Страхование производится от хищения наличных, снятых в банкомате в результате кражи, грабежа или разбойного нападения;
- Утраты карты вследствие неисправной работы банкомата, размагничивания, утери и т.п.

ФАЛЬШИВЫЙ БАНКОМАТ

Пользуйтесь банкоматами в отделениях банков.
Не используйте карту и не пользуйтесь банкоматом в «глухих» немноголюдных местах.
Не доверяйте деньги банкомату, вызывающему подозрение.
Не снимайте деньги в банкомате в день зарплаты- это приманка для мошенников.
При вводе ПИН-кода всегда прикрывайте клавиатуру рукой,
Наиболее безопасное использование банкоматов в зоне охраны в госучреждениях, подразделениях банков, крупных торговых комплексах, гостиницах.

СКИММИНГ- ХИЩЕНИЕ ДЕНЕЖНЫХ СРЕДСТВ С КАРТЫ С ИСПОЛЬЗОВАНИЕМ СЧИТЫВАЮЩЕГО УСТРОЙСТВА

- **Признак скиммера :**
- Вы заметили незнакомое для себя устройство
- Устройства банкомата крепятся изнутри и не должны иметь щели и другие признаки внешнего крепления
- Карточка долго вставляется и вытаскивается.
- Карточку неудобно забирать

ФАЛЬШ- НАКЛАДКА ДЛЯ СЧИТЫВАНИЯ ПИН-КОДА

убедитесь в том, что накладка не выступает над панелью.

Посмотрите, нет ли щелей. Поверхность должна быть цельнолитой

.

ЗАКЛЕИВАНИЕ СКОТЧЕМ БАНКОМАТА.

Если банкомат не выдает купюры проверьте, не заклеен ли кеш-диспенсер скотчем.

«ЛИВАНСКАЯ ПЕТЛЯ»

Внимательно осмотрите отверстие картоприемника- убедитесь, что там нет «ловушки».

- Ловушка вставляется в прорезь банкомата и блокирует возврат вашей карты.
- Если Вы заметили ловушку попробуйте извлечь ловушку с картой самостоятельно.
- В противном случае немедленно заблокируйте карту по телефону, указанному на оборотной стороне карты который Вы заранее вбили в телефонную книгу.

ДОСТУП В ПОМЕЩЕНИЕ С БАНКОМАТОМ

- Замки доступа в помещения, где устанавливаются банкоматы, не должны требовать от вас ввода ПИН-кода!

ВВОД ПИН-КОДА.

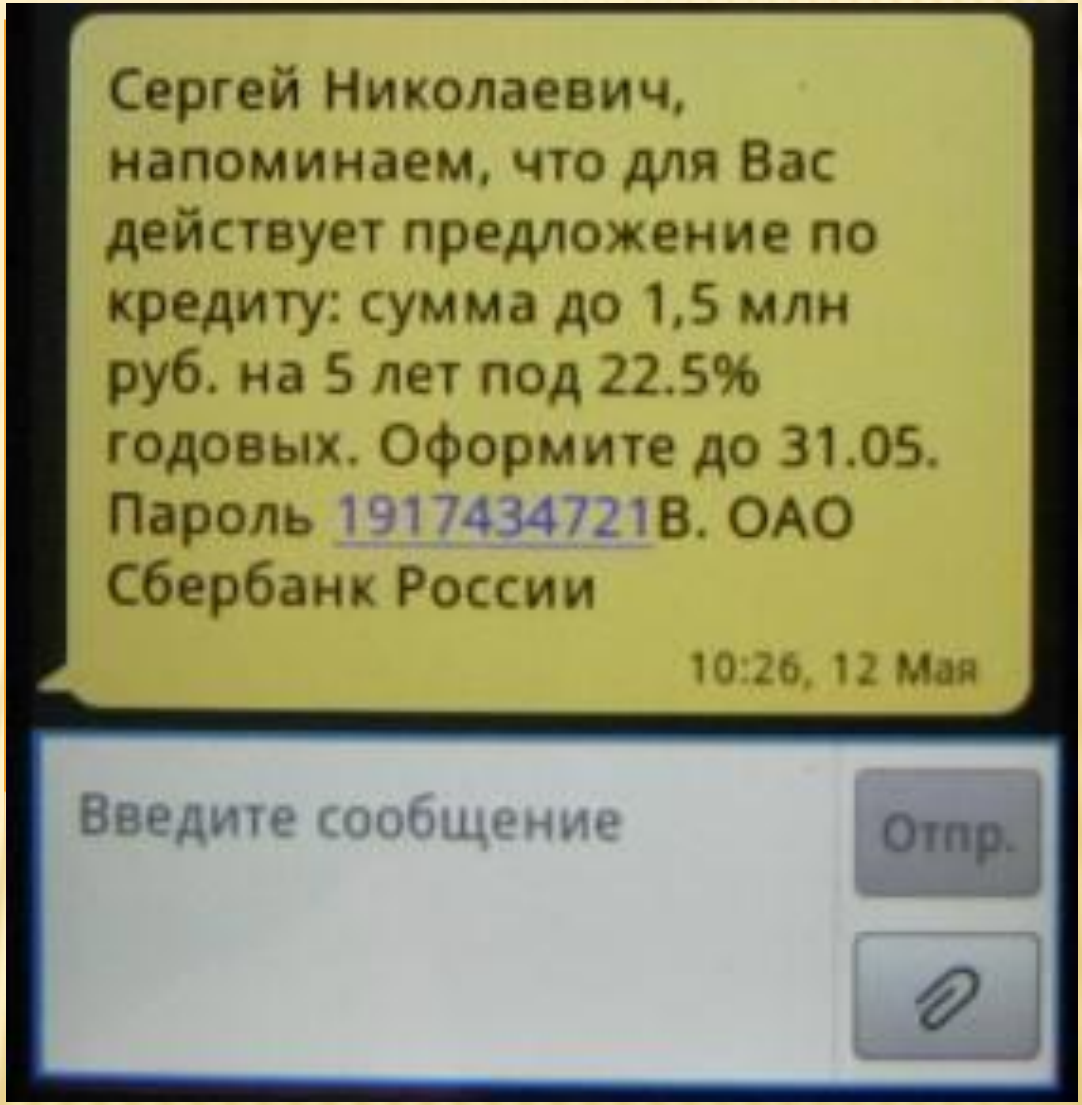
- При вводе Пин-кода всегда прикрывайте клавиатуру рукой.
- Ввод Пин-кода в вашем присутствии требует только кассир в магазине, операционист в банке и банкомат.
- Не реагируйте на действия лиц , призывающих, требующих указать данные вашей карты, ввести ПИН-код по телефону или путем СМС сообщения.
- Никому не сообщайте свой PIN-код в СМС сообщении или по телефону, при оформлении покупок в Интернете.
- Все уловки преступников направлены на получение пин-кода и доступ к мобильному банку.

ФАЛЬШИВОЕ СМС ОТ БАНКА

В сообщении от банка не должно быть номеров телефонов.

В сообщении не должно быть просьб позвонить на указанный номер.

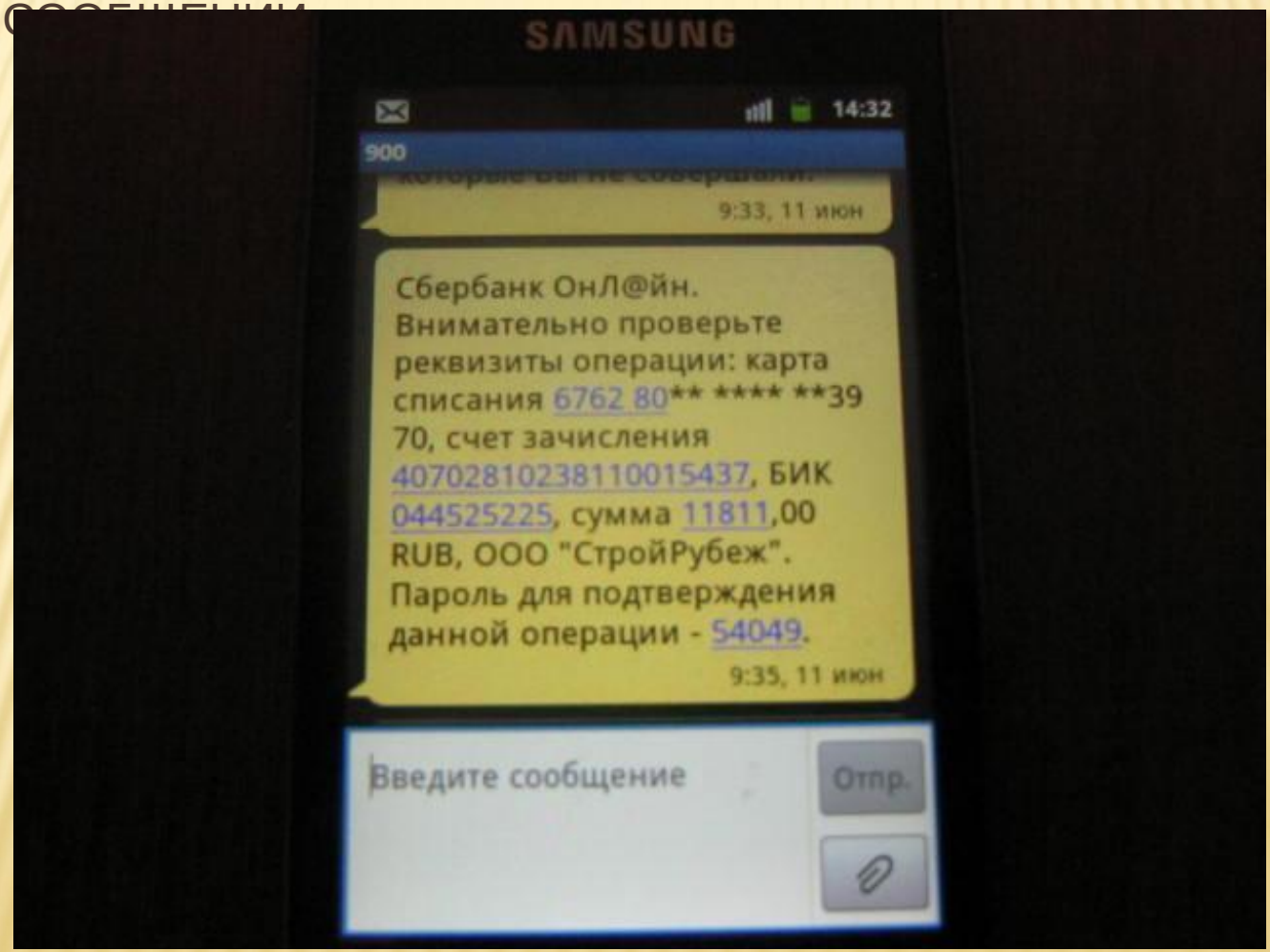
Если вам пришло сообщение о блокировке карты, задолженности, перезвоните по телефонам, указанным **на оборотной стороне вашей карты**.



ЗАПОМНИТЕ!!!

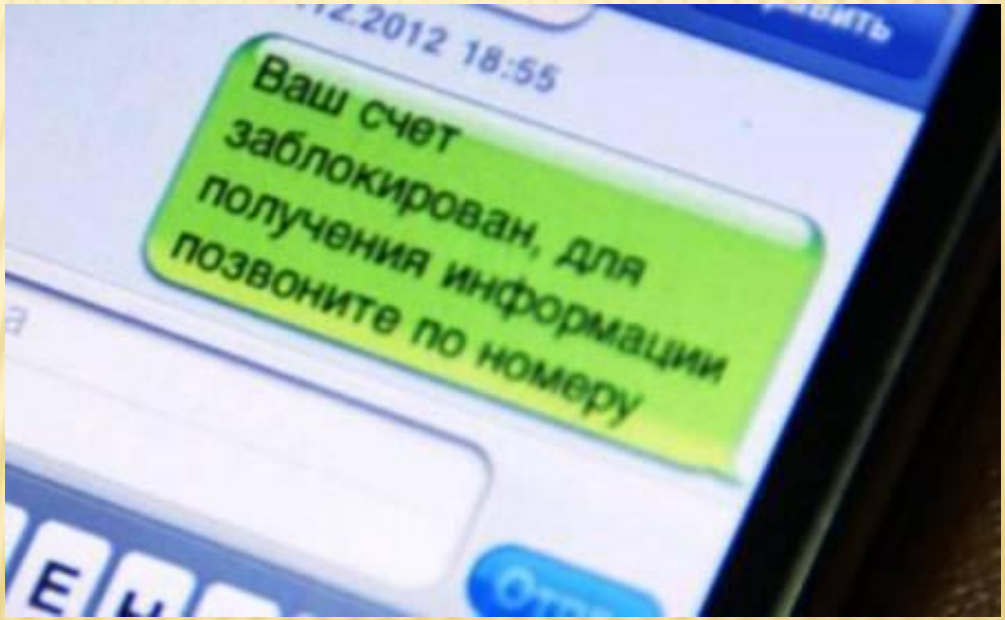
ВСЕГДА ПРОВЕРЯЙТЕ РЕКВИЗИТЫ ПЛАТЕЖА

ВВОДИТЬ ОДНОРАЗОВЫЙ ПАРОЛЬ СЛЕДУЕТ ТОЛЬКО ЕСЛИ РЕКВИЗИТЫ ВАШЕЙ ОПЕРАЦИИ СООТВЕТСТВУЮТ РЕКВИЗИТАМ В ПОЛУЧЕННОМ SMS — СООБЩЕНИИ



СОЦИАЛЬНЫЙ ИНЖИНИРИНГ- САМЫЙ ОПАСНЫЙ И РАСПРОСТРАНЕННЫЙ ВИД МОШЕННИЧЕСТВА.

Не выполняйте действий под диктовку!
Перезвоните по телефону, указанному на оборотной стороне вашей карты!



МОШЕННИЧЕСТВО С POS-ТЕРМИНАЛАМИ.

Операции по карте должны проводиться в вашем присутствии.
У продавца должна отсутствовать возможность скопировать данные вашей карты.

В случае изъятия карты требуйте расписку об изъятии с указанием даты, времени и причины изъятия, убедитесь, что карта разрезана в Вашем присутствии

Сообщите об изъятии карты в Службу помощи. по телефонам, указанным на оборотной стороне карты.

ВИД МОШЕННИЧЕСТВА «СОТРУДНИК БАНКА».

- Человек на улице, в форме сотрудника банка, просит вас предоставить ему личные данные или показать документы.
- Внимание! Все вопросы по вашей карте решайте только в отделении банка!

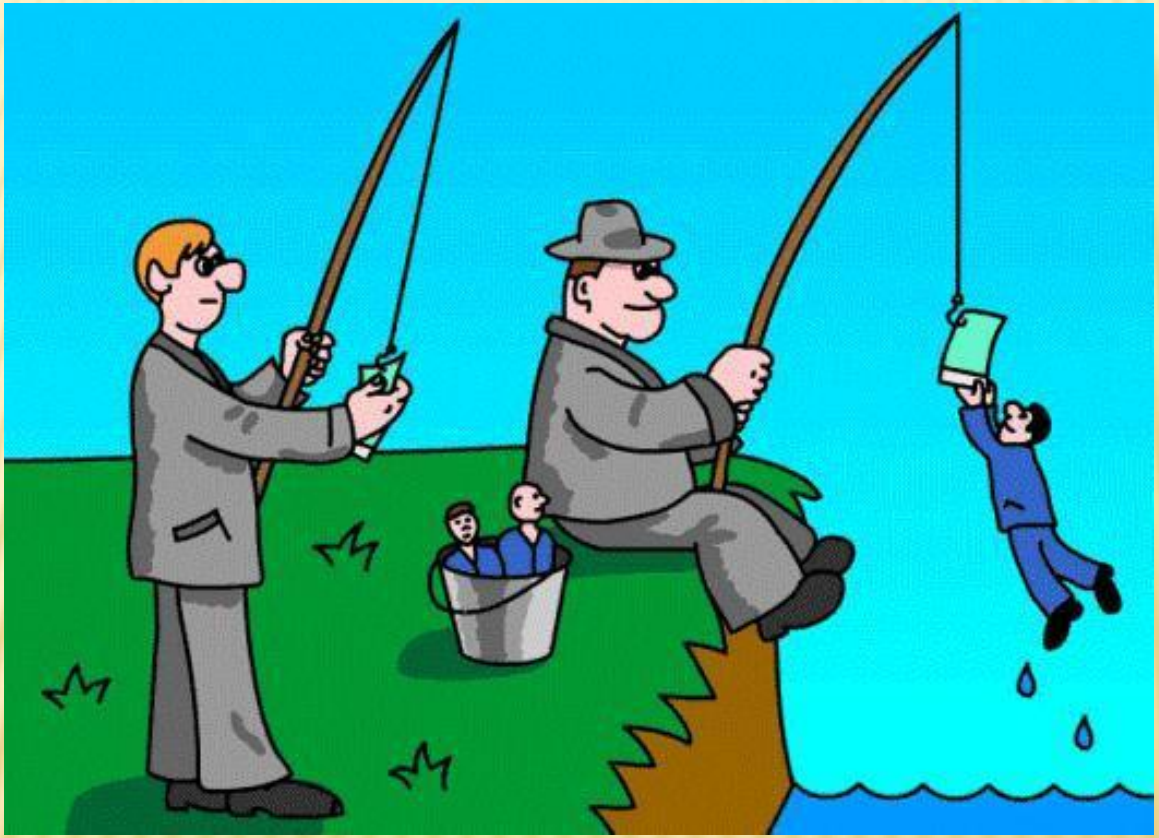
Вид мошенничества «Проверка документов»

НЕ ПОД КАКИМ ПРЕДЛОГОМ НЕ ПЕРЕДАВАЙТЕ СВОЮ КАРТУ, ДАННЫЕ ВАШЕЙ КАРТЫ ДРУГИМ ЛЮДЯМ- ДАЖЕ СОТРУДНИКАМ ПОЛИЦИИ И СИЛОВЫХ СТРУКТУР.

Вид мошенничества: «Считывание данных кредитной карты в ресторане».

НЕ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ НЕ ПЕРЕДАВАЙТЕ ВАШУ КАРТУ ДРУГИМ ЛЮДЯМ.

Вид мошенничества: «Получение данных карты при имитации приема на работу».



ЕСЛИ БАНКОМАТ «СЪЕЛ КАРТУ».

Не обращайтесь за помощью к сторонним лицам !

В случае блокировки карты банкоматом немедленно заблокируйте карту по телефону, указанному на оборотной стороне карты!

ВИД МОШЕННИЧЕСТВА: «ПОЛУЧЕНИЕ КРЕДИТОВ ПО УКРАДЕННОМУ ПАСПОРТУ».

«НЕЗАКОННОЕ ПОЛУЧЕНИЕ ДАННЫХ БАНКОВСКОЙ КАРТЫ ДЛЯ ПОСЛЕДУЮЩЕГО ХИЩЕНИЯ СРЕДСТВ».

Преступники просят назвать данные карты для внесения ими, якобы, аванса или предоплаты за покупку.

После этого деньги исчезают с вашей карты.

Никогда не называйте преступникам CVV код, и не выполняйте действий под диктовку.

Не называйте смс - пароли для подтверждения операций

Чаще всего преступники орудуют на сайтах объявлений о продаже вещей или машин

- В случае обнаружения утраты карты ***(или) её использования без вашего согласия незамедлительно направьте уведомление оператору по переводу денежных средств, но не позднее дня, следующего за днем получения от оператора по переводу денежных средств уведомления о совершенной операции.***
- ***После получения оператором по переводу денежных средств уведомления клиента в соответствии с частью 11 ФЗ №161 «О национальной платежной системе» оператор по переводу денежных средств обязан возместить клиенту сумму операции, совершенной без согласия клиента после получения указанного уведомления***.

НЕ ХРАНИТЕ НЕИСПОЛЬЗУЕМЫЕ БАНКОВСКИЕ КАРТЫ ДОМА! ИХ МОГУТ ОБНАЛИЧИТЬ ВОРЫ!

НЕ ВЫБРАСЫВАЙТЕ ЧЕК С НЕИСПОЛЬЗОВАННЫМИ ПАРОЛЯМИ. ЕГО МОГУТ ПОДОБРАТЬ ПРЕСТУПНИКИ

СБЕРБАНК РОССИИ ОАО

ул. Молодежная, 19.

ЧЕК
ИДЕНТИФИКАТОР ПОЛЬЗОВАТЕЛЯ И ПАРОЛЬ
ДЛЯ ДОСТУПА К БАНКОВСКОМУ
ОБСЛУЖИВАНИЮ В СЕТИ ИНТЕРНЕТ

22.11.10 13:51:19
НОМЕР ОПЕРАЦИИ: 0837
ТЕРМИНАЛ: 280262

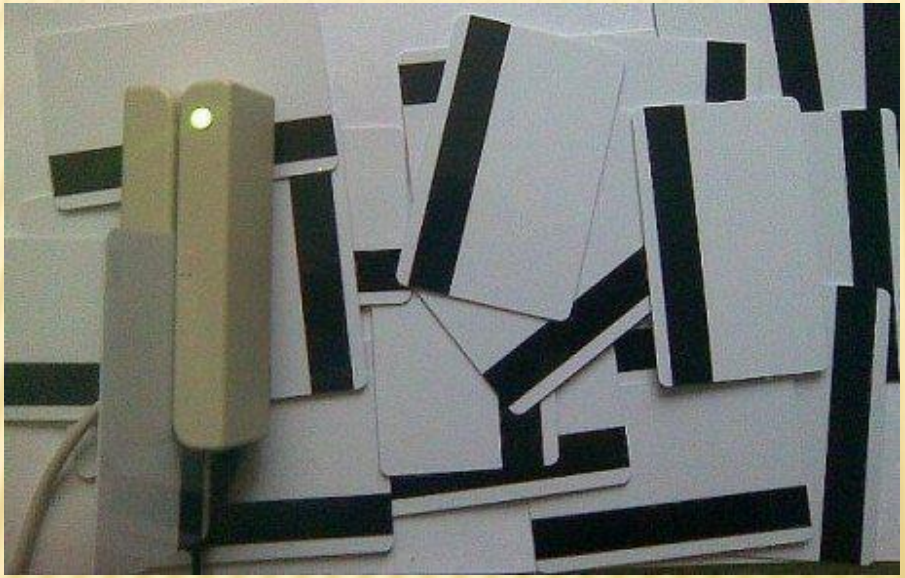
КАРТА: XXXXXXXXXXXX7201 1

ИДЕНТИФИКАТОР ПОЛЬЗОВАТЕЛЯ:
Тут будет ваш логин, состоит из цифр и букв
ПОСТОЯННЫЙ ПАРОЛЬ:
Тут пароль

ХРАНИТЕ ДАННЫЙ ЧЕК В НЕДОСТУПНОМ ДЛЯ
ТРЕТЬИХ ЛИЦ МЕСТЕ.
ПРИ УТЕРЕ ИЛИ КОМПРОМЕТАЦИИ ИНФОРМАЦИИ
ДАННОГО ЧЕКА НЕЗАМЕДЛИТЕЛЬНО СМЕНИТЕ
ПАРОЛЬ НА WEB-САЙТЕ БАНКА ИЛИ ПОЛУЧИТЕ
НОВЫЙ ЧЕК,
ЛИБО ПОЗВОНИТЕ ПО ТЕЛЕФОНУ
(495) 500-00-05

СПАСИБО

ВИД МОШЕННИЧЕСТВА: «ПОКУПКА БАНКОВСКОЙ КАРТЫ У ЕГО ВЛАДЕЛЬЦА ДЛЯ ОСУЩЕСТВЛЕНИЯ НЕСАНКЦИОНИРОВАННЫХ ОПЕРАЦИЙ С ЕГО КАРТОЙ».



ЗАКОН О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ФЗ №152 ОТ 27.07.2006Г

Не передавайте никому данные вашей карты кем бы он не представился!

Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей.

Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

При получении персональных данных по телефону или интернет необходимо согласие владельца персональных данных.

БУДЬТЕ ГОТОВЫ К ДЕЙСТВИЯМ МОШЕННИКОВ

- **Будьте готовы к сообщениям мошенников , в которых вас просят указать ваши личные данные.**
- Не заполняйте полученные по электронной почте анкеты, предполагающие ввод личных данных
- **Помните- сотрудники банка не имеют право запрашивать личные данные по телефону или электронной почте.**
- **Перезвоните в банк по телефонам, указанным на вашей карте и уточните, действительно ли вам посылали сообщение и действительно вам звонил сотрудник банка.**
- **Не заполняйте полученные по электронной почте анкеты, предполагающие ввод личных данных.**
- **Связывайтесь с банком по телефону всякий раз, когда ситуация кажется вам подозрительной.**

ВИД ТЕЛЕФОННОГО МОШЕННИЧЕСТВА: «Я ПОЦАРАПАЛА ВАШУ МАШИНУ».

- На телефон жертвы приходит смс «Я поцарапала вашу машину, (машину вашего сына». Потерпевший звонит по номеру и сего счета списывают крупную сумму денег.

ВИД МОШЕННИЧЕСТВА: «ЛЖЕ-КОНТРОЛЕРЫ».

- Мошенники под, видом контролеров, в общественном транспорте вымогают у пассажиров за безбилетный проезд, проезд по чужой социальной карте суммы, в несколько раз превышающие штрафы.

ВИД МОШЕННИЧЕСТВА: «УСИЛЕННАЯ АВТОРИЗАЦИЯ», «УСИЛЕННАЯ ЗАЩИТА».

- Вирус перенаправляет клиентов банка на сторонние сайты и предлагает воспользоваться "Усиленной авторизацией". Таким образом в руки мошенников попадают данные клиентов.

ВИД МОШЕННИЧЕСТВА: «ВИШИНГ».

- Вы получаете SMS или электронное письмо с просьбой позвонить на определенный городской номер. Когда вы звоните на этот номер, вам автоматически зачитывают информацию о проблемах с вашей картой и просят сообщить номер карты, пароли, PIN-код, код доступа или другую личную информацию , а так же просят установить дополнительное оборудование для защиты системы от вирусов.
- В целях избегания мошеннических действий Вас простят назвать номер телефона и кодовое слово.

Вид мошенничества «Фишинг»

- ***Фишинг***- создание поддельного веб-сайта, который выглядит как сайт банка или интернет- магазина (или как любой другой сайт, через который производятся финансовые операции).

Преступники пытаются завлечь с на этот сайт, чтобы вы выманить конфиденциальные данные, такие как логин, пароль или PIN-код.

Как не стать жертвой мошенников.

Банк никогда не запрашивает пароли для отмены операций.

Для входа в личный кабинет требуется только идентификатор и пароль.

Банк не имеет права требовать какую-либо персональную информациюВводить одноразовые пароли следует только в том случае, если операция инициирована Вами.Не сообщайте номер телефона и кодовое слово! Убедитесь, что адрес в адресной строке начинается с "https://"

найдите запертый замок.

Дважды щелкните мышью на замок и проверьте, совпадает ли адрес, указанный в сертификате безопасности, с текстом в адресной строке браузера.

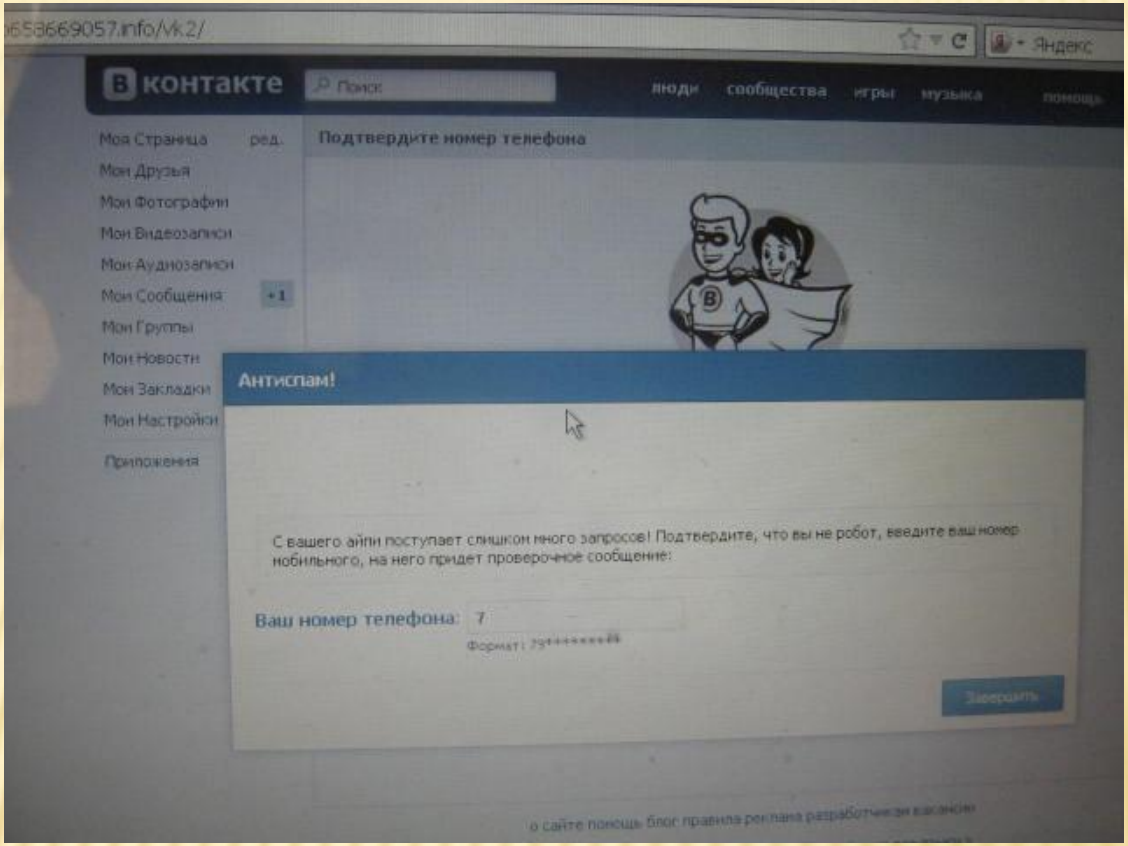
БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ!

Если необходимо посетить интернет-банк, онлайн-магазин, не проходите по ссылкам-вводите адрес сайта вручную!

Банки никогда не присылают по электронной почте сообщения, в которых просят клиентов ввести личные данные

- Если URL-адрес состоит из случайного набора букв и чисел или выглядит подозрительно, не вводите никакие данные.
- Ссылки для перехода на фишинговый сайт чаще всего приходят в письмах,анкетах или отображаются в сервисных окнах программ под видом:
- **важного сообщения**(например, от банка) с предложением срочной установки некоего сертификата безопасности, необходимого для дальнейшего получения финансовых услуг.
- **срочного обновления** операционной системы/браузера/приложения, для загрузки которого жертве следует указать в соответствующей форме свой номер мобильного телефона и ввести пришедший в ответном СМС код.
- **предложения ответить на вопросы анкеты** и получить подарок (для получения подарка требуется ввести номер банковской карты и пароль доступа к интернет-банку);

ОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ



- НИКОГДА не размещайте в открытом доступе и не передавайте информацию личного характера, которая может быть использована во вред.
- Не подтверждайте себя вводом личных данных
- Общение в сети в значительной мере обезличено, и за фотографией профиля может скрываться кто угодно.

- **Не используйте чужой компьютер для выхода в онлайн-банкинг.**

- Не используйте компьютеры с общим доступом в интернет-кафе, аэропортах, клубах, гостиницах, библиотеках и др. Эти компьютеры могут быть заражены шпионскими программами.

ОПАСНЫЙ WI-FI

- Киберпреступники отслеживают общедоступные Wi-Fi-сети и перехватывают данные, передаваемые по линии связи. Преступник может получить доступ к банковским учетным данным, паролям к учетным записям и другой ценной информации

АНТИВИРУСНАЯ ЗАЩИТА

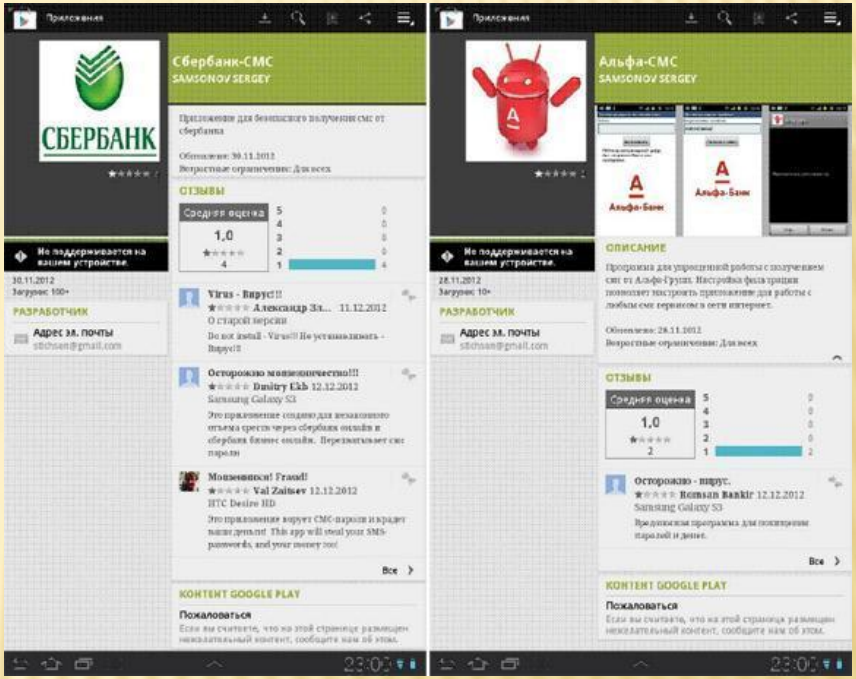
- Используйте антивирусное программное обеспечение и следите за его регулярным обновлением.
- Регулярно выполняйте антивирусную проверку для своевременного обнаружения вредоносных программ

ВНИМАНИЕ ! «ОПАСНЫЕ НАХОДКИ»
ЛЮБАЯ НАХОДКА МОЖЕТ СОДЕРЖАТЬ ВРЕДОНОСНОЕ ПО.
НЕ БЕРИТЕ ЧУЖОГО!

«МОБИЛЬНЫЕ ШПИОНЫ».

Прежде чем скачать и установить банковское приложение на смартфон убедитесь в том,что это приложение принадлежит банку!

Никогда не скачивайте приложения не установленных разработчиков из неизвестных источников.



ВИДЫ МОБИЛЬНЫХ МОШЕННИЧЕСТВ.

- ***Звонок от техподдержки оператора***
- "Здравствуйте, это инженерная служба вашего сотового оператора. Мы перенастраиваем сеть. Чтобы оставаться на связи, вам необходимо набрать..."
- Мошенники в день рождения рассылают владельцам мобильных устройств сообщения с предложением загрузить «открытку», «подарок» и т.п., для чего необходимо пройти по интернет-ссылке.

СПЕКУЛЯНТЫ МИРОВОГО МАСШТАБА

- Валютные спекулянты мирового масштаба активно «играют» на понижение курса рубля. Центральному банку РФ не хватает «мозгов» достойно противостоять им. Сбережения стремительно обесцениваются. «Спасение утопающих- всегда дело рук самих утопающих».
- Задача простых граждан знать основные правила игры валютных спекулянтов. Для этого достаточно установить на свой ПК бесплатную торговую платформу, которая поддерживает недельный график «Доллар-Рубль».
- На графике «Доллар- Рубль» красной горизонтальной жирной линией показан пробой первого верхнего уровня сопротивления российского рубля на уровне 33,5 рубля за доллар США. .(см.график).Нужно привыкать самим выставлять уровни сопротивления и поддержки
- Спекулянтам и даже студенту первого курса любого финансового ВУЗа в январе 2014 года было понятно, что рубль будет дешеветь по отношению к доллару.
- Красной пунктирной линией показан пробой «второй линии сопротивления Российского рубля»,который произошел в начале сентября 2014 года на уровне 36,9 рублей за доллар США.

25 Aug 2013
22 Sep 2013
20 Oct 2013
17 Nov 2013
15 Dec 2013
12 Jan 2014
9 Feb 2014
9 Mar 2014
6 Apr 2014
4 May 2014
1 Jun 2014
29 Jun 2014
27 Jul 2014
24 Aug 2014

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

- ***1. Как можно дополнительно защитить себя от кражи денег?***
- А.) Прятать деньги подальше в одежду;
- Б.)Заниматься боксом и бегом;
- В.)Хранить кошелек и карту в разных местах;
- Г.)Не хранить все свои сбережения на одной карте;
- Д.) Завести для себя и близких карту с «чипом».
- Е.) Открыть несколько карт для разных целей с небольшими лимитированными суммами и ограничить регионы снятия наличных.
- ***2. Совершая операцию в банкомате необходимо:***
- А.) Сначала оценить новый дизайн банкомата;
- Б.)Снимать сразу большую сумму денег желательно в день зарплаты;
- В.) Если очередь к банкомату большая, нужно совершить свои платежи как можно быстрее, в спешке.
- Г.)Пользоваться банкоматом нужно именно тогда, когда куда-то опаздываешь и срочно нужны наличные деньги.
- Д.)Предварительно убедиться в том, что банкомат находиться на территории банка, бизнес- центра, торгового центра поблизости от пункта охраны.
- Е.) Внимательно осмотреть панель банкомата, убедиться в том, что нет щелей в картоприемнике отсутствует «ливанская петля»,нет подозрительных предметов
- З.) Отказаться от операций, если оборудование вызывает подозрение.
- И.) Подозрительное оборудование нужно проверить на прочность.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

- ***3. ПИН-код, номер карты, идентификатор и логин, CVV и другие персональные данные необходимо вводить или сообщать:***
- А.) Чтобы попасть в комнату, где установлен банкомат;
- Б.) Если сотрудник банка для входа в комнату с банкоматом, требует от вас ввести ПИН-код;
- В.) Для проведения операций по телефону с сотрудником банка;
- Г.) По требованию сотрудников полиции и силовых структур;
- Д.) По просьбе официанта или продавца в магазине;
- Е.) При заполнении анкеты вашего банка;
- Ж.) В ситуации, когда внушающие доверие люди сообщают данные своих карт и ПИН-коды ;
- З.) Если банкомат съел карту, нужно перезвонить по телефону, указанному на банкомате и продиктовать сотруднику данные по карте.
- И.) Никому не называть свой Пин-код и не сообщать данных карты. Все операции по карте должны проходить только при моем личном присутствии;
- К.) Если по телефону требуют назвать личные данные, нужно перезвонить по телефону, указанному на оборотной стороне карты
- **4. Фишинг это:**
- А.) Рыбалка.
- Б.) Игра с фишками;
- В.) Болезнь;
- Г.) Получение персональных данных с целью похищения средств.
- Д.) Создание поддельных сайтов банков, интернет-магазинов с целью получения данных карты.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

- **5. Социальный инжиниринг:**
- А.) Вид франдрайзинга
- Б.) Новый вид благотворительности
- В.) Человек, представившийся сотрудником банка, который просит сообщить конфиденциальные данные по телефону и и выполнить под его диктовку определенные действия.
- **6. Кардинг это:**
- А.) Новый вид спорта;
- Б.) Езда на машинках;
- В.) Аттракцион в парке;
- Г.) Получение данных о вашей банковской карте с целью хищения находящихся на ней средств.
- ***7. Что такое «банковские троянцы»?***
- А.) Сотрудники «мобильного банка»;
- Б.) Специалисты отдела маркетинга банка;
- В.) Зловредные программы, создаваемые с целью похищения и или перехвата персональных данных;
- **8. Защищенное соединение это:**
- А.) Когда мы видим в начале адресной строки http;
- Б.) Когда мы видим в начале адресной строки https;
- В.) Когда мы видим в начале адресной строки или http или https;
- Г.) Когда мы видим, что замок закрыт.
- Д.) Когда мы видим,что замок открыт.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

- **9. Фишинговый сайт это:**
- А.) Сайт,где контактные телефоны не совпадают с телефонами банка;
- Б.) Адрес сайта в адресной строке не совпадает с адресом сайта банка;.
- В.) На сайт попали, перейдя по ссылке с «всплывающего окна» или рекламного баннера;
- Г.) Сайт, имеющий защищенное соединение;
- Д.) Сайт или анкета, где требуется ввести номер телефона, номер кредитной карты, пин-код;
- Е.) Защищенный сайт, где для входа в систему необходимо ввести идентификатор пользователя и постоянный пароль;
- Ж.) Защищенный сайт, где для входа в систему необходимо ввести номер телефона и Пин-код или секретное слово, указанное в договоре с банком;
- З.) Незащищенный сайт, где требуется ввести номер телефона и секретное слово, указанное в договоре с банком;
- И.) Любой сайт, где адрес не защищен.
- К.) Адрес сайта банка или магазина состоит из случайного набора букв и чисел
- **10. В каких случаях нельзя пользоваться общедоступным WI-FI?**
- А.) Всегда -может прийти счет за оплату траффика;
- Б.) Преступники могут перехватить мои данные и получить доступ к моему банковскому счету;
- В.)Если компьютер не защищен антивирусом.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

- **11. Почему желательно не пользоваться найденными устройствами?**
- А.) Может быть накоплено много отрицательной энергии прошлым хозяином;
- Б.) Устройство может содержать «банковский троян», который будет перенаправлять мои данные преступникам.
- **12.Антивирусная защита это:**
- А.) Пустая трата денег;
- Б.) Антивирус не нужно устанавливать тому, кто не посещает подозрительных сайтов.Можно смело оставлять в компьютере персональные данные,пин- коды,кодовое слово.
- В.) Защита компьютера «банковских троянцев».
- Г.) Не панацея, но хотя-бы какая-то защита.
- **13. Мобильные мошенники это:**
- А.) Популярная молодежная группа.
- Б.) Мошенники, которые быстро передвигаются и их сложно поймать.
- В.) Те, кто под любым предлогом выманивает деньги.
- Г.) Умело зарабатывающие на человеческом доверии и слабости.
- Д.) Незнакомые, которые просят перезвонить на незнакомый номер.
- Е.) Берутся по телефону решить проблемы родственников.
- **14. Почему лучше не проводить финансовых операций на чужом или общественном компьютере?**
- А.) На нем могут остаться мои данные.
- Б.) Компьютер может быть заражен вирусами шпионами.
- В.) Можно спокойно проводить платежи.

- **Ответы:** **1абвгде, 2дези, 3ик, 4гд, 5в, 6г, 7в, 8бг, 9абвджзк, 10бв, 11б, 12вг, 13вгде, 14аб**

СОДЕРЖАНИЕ

Как правильно пользоваться банковской картой……3
«Фальшивый» банкомат……4
«Скимминг»……5
«Заклеивание» банкомата……7
«Ливанская петля»……8
Доступ в помещение с банкоматом……9
Ввод «Пин-кода»……10
«Фальшивые» СМС от банка……11
Социальный инжиниринг……13
Мошенничество с POS-терминалами……14
«Лжесотрудник банка»……15
«Проверка документов»……16
«Считывание данных банковской карты»……17
«Прием на работу»……18
Что делать, если банкомат «съел карту»……19
Получение кредита по украденному паспорту……20
Незаконное получение данных банковской карты
с целью хищения средств с карты……21

СОДЕРЖАНИЕ

Опасно хранить конверты с банковскими картами дома……..23
Незаконное использование чека с одноразовыми паролями……..24
Покупка банковской карты у владельца с целью незаконного использования……25
Закон о персональных данных……26
Готовность к действиям мошенников……27
«Я поцарапала вашу машину»……....28
Вид мошенничества «Лжекондуктор»……29
«Предлагаем вам усиленную авторизацию»……30
«Вишинг»……31
«Фишинг»…… 32
Безопасность в интернете……33
Безопасность в социальных сетях……..34
Опасный WI-FI……..36
Антивирусная защита ПК……..37
«Опасные находки»……39
Мобильные «шпионы»……...40
Спекулянты мирового масштаба…….....41
Вопросы для самоконтроля……..43