

Кибербезопасность в финансовой сфере ч.1.





Основные виды (места) мошенничеств

- Мошенничество в банкоматах и торговых точках.
- Мошенничество в сети интернет.
- Мошенничество с использованием мобильных устройств.
- Социальная инженерия.



Липецкая
область

Банковская карта ключ доступа к Вашим счетам

- ❖ Карта является собственностью банка и предоставляется Вам на определенный срок для использования в качестве электронного средства платежа.
- ❖ Держателем карты является лицо, получившее от Банка право на пользование картой, на имя которого выпущена карта, и образец подписи которого имеется на ее оборотной стороне.
- ❖ *Без Вашей подписи карта недействительна.*
- ❖ **Карта не подлежит передаче другому лицу.**



Липецкая
область

У банкомата (физическая безопасность)

При проведении операции с вводом
ПИН-кода

ВСЕГДА

прикрывайте клавиатуру, например,
свободной рукой.

СКИММИНГ

сошел на нет





Траппинг или «Ливанская петля»

“Ливанская петля” блокиратор, который крепится внутри картоприемника и блокирует вывод карты. То есть вы вставили карту, ввели пин-код, а получить карту не можете. Обычно в таком случае человек идет разбираться, а мошенники извлекают карту из банкомата.





«Незавершенная операция»

Злоумышленники на терминале выбирают необходимую операцию, но не вставляют банковскую карту, таким образом операция остается незавершенной. Следующий человек, пожелавший воспользоваться банкоматом, видит надпись «Вставьте карту». Клиент вставляет карту в устройство, вводит пин-код, операция завершается. Деньги уходят со счета.





Вы стоите в очереди к банкомату, перед вами человек «случайно» оставил в банкомате свою карту. Первая реакция — быстро вытащить «пластик» из банкомата, ведь мы все знаем, что через 30-60 секунд он ее проглотит.

Если вы берете в руки чужую карточку, тут же появляется ее владелец, который предъявит вам, что денег на счету было больше, а последним карту держали вы. Вместе с ним будут «свидетели» (обычно мужчины крепкого телосложения), которые подтвердят, что видели, как вы снимали средства. И тут вам предложат или вернуть недостающую сумму, или дождаться приезда полиции.

Если вы обнаружили в банкомате забытую кем-то карточку, не трогайте ее — пусть ее заберет владелец или проглотит банкомат. А если вы все-таки вытащили чужую карточку и вас обвиняют в краже, не отдавайте аферистам деньги, вызывайте полицию.





«Перевод случайному знакомому»

У банкомата Вас могут попросить снять деньги незнакомые люди. Они рассказывают душещипательные истории, что забыли карту и опаздывают к бабушке в больницу/к девушке на свидание/на встречу к другу и им нужны наличные (в такси или в аптеке не принимают карты). И предлагают перевести средства со своего счета на счет случайного прохожего, даже предлагают небольшой процент за услугу. Дело в том, что злоумышленники, крадущие деньги с чужой банковской карты, вынуждены запутывать полицейских, переводя сумму по несколько раз, на разные счета. Если вы согласитесь принять перевод от аферистов и поможете им обналичить заработанные преступным путем средства, вы можете стать соучастником преступления.

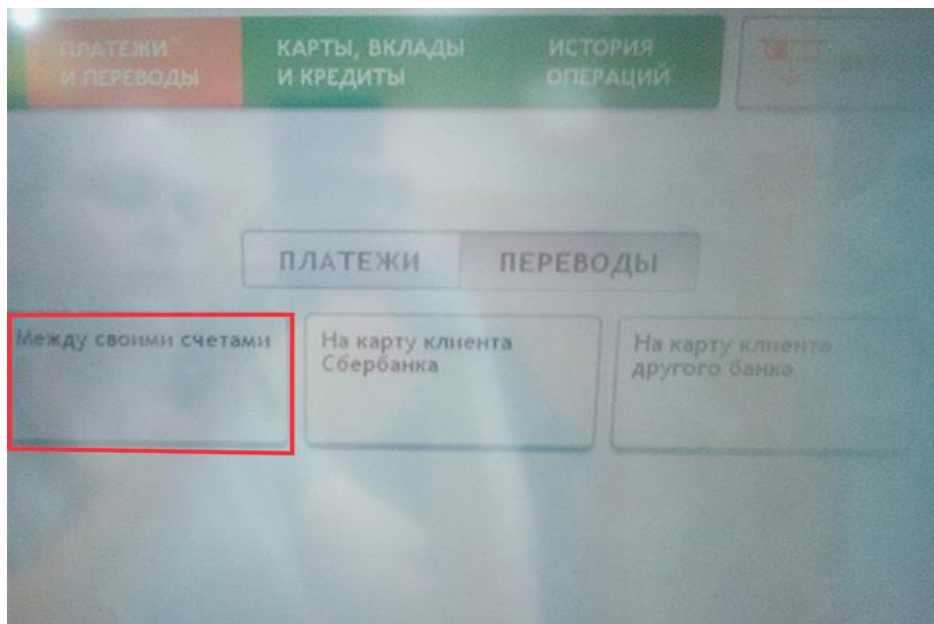
**Никогда не соглашайтесь обналичить деньги незнакомых людей.
Даже за процент.**





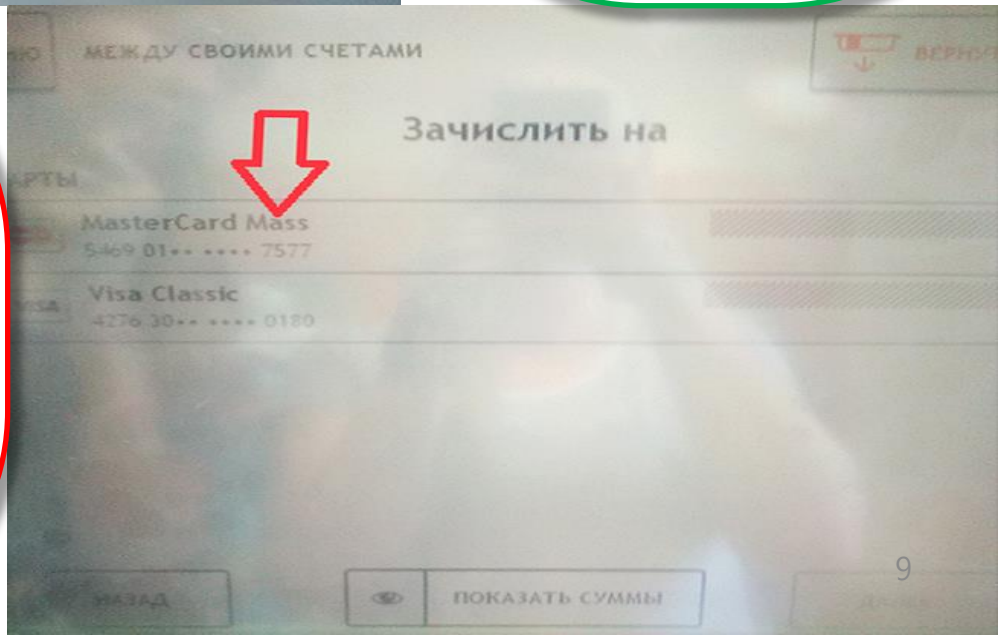
Липецкая
область

Перевод между своими счетами (картами)



В банкомате/Сбербанк @нлайн/мобильном приложении можно переводить между своими картами/счетами. Если у Вас есть карты на которых нет средств за ними следует также внимательно следить.

Никому не передавайте одну из своих карт даже если на ней нет средств. При утере (передаче) «пустой» карты (ПИН кода) ее необходимо сразу блокировать.





**СМС не является подтверждением операции!
При возникновении спорных ситуаций необходимо звонить в банк
выпустивший Вашу карту.**

**Во избежание мошенничества с использованием Вашей карты
требуется проведения операций с картой только в Вашем
присутствии, не позволяйте уносить карту из поля Вашего зрения.**



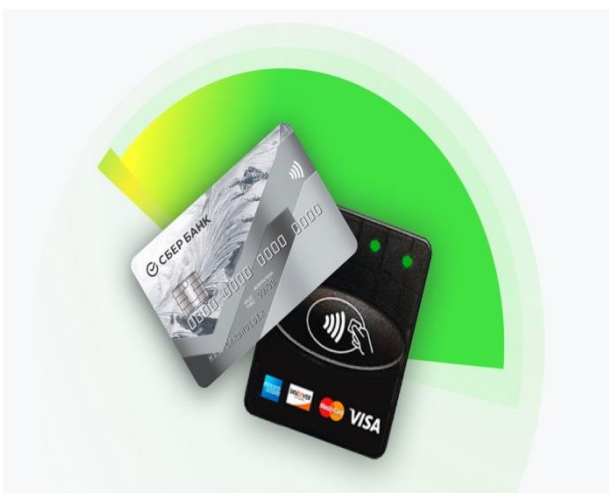
Липецкая
область

Бесконтактные платежи NFC



Важное отличие Apple Pay, Android Pay, Mir Pay и т.д. от платежной карты в том, что для проведения операции требуется подтверждение пользователя и до подтверждения телефон не передает никакие данные, а карта всегда доступна для считывания.

Подлимитные операции
(до 1000 р.) по карте можно осуществлять неограниченное количество раз.



Банкоматы с бесконтактным обслуживанием.
Вы не забудете карту в банкомате — её даже не придётся выпускать из рук.
Просто поднесите смартфон или карту к считывателю.



Отдельная (виртуальная) карта для интернет платежей!

Индивидуальные лимиты по карте.

Держателем карты могут быть установлены следующие лимиты:

- ✓ лимит на получение наличных денежных средств по карте в течение месяца;
- ✓ лимит на совершение безналичных операций по карте в течение месяца ;
- ✓ общий лимит на совершение расходных операций по карте в течение месяца.

**Текущую информацию об установке лимитов/ограничений
уточните в своем банке!!!**



Сбербанк 8(800) 555-55-50
Короткий номер: 900

ВТБ 8 (800) 100-24-24

В случае проблем при проведении операций обратиться в Контактный центр Банка ВЫПУСТИВШЕГО ВАШУ КАРТУ

В случае утраты/кражи/изъятия карты или если информация о ПИН-коде или реквизитах карты стала доступна третьим лицам, необходимо срочно:

- ✓ обратиться в Контактный центр Банка для блокировки карты
или
- ✓ направить сообщение о блокировке с помощью услуги «Мобильный банк»
или
- ✓ заблокировать карту с помощью услуги «Сбербанк Онлайн», «ВТБ Онлайн».

Подать в Подразделение банка письменное заявление.

По факту мошенничества рекомендуется подать заявление в правоохранительные органы.



Основные угрозы в сети интернет

Основная цель.

С помощью вирусов или социальной инженерии получить доступ к персональной (банковской) информации для дальнейшей

монетизации результата.





The screenshot shows a phishing website for Sberbank Online. The browser's address bar contains a URL that is circled in red. A callout box points to it, stating: "Адрес сайта не соответствует официальным: esk.sbrf.ru online.sberbank.ru".

The website header features the Sberbank logo and the text "Сбербанк ОнЛ@йн" with a phone number "+7 (499) 657 0232" circled in red. A callout box points to this number, stating: "Контактный телефон не соответствует официальным: +7 (495) 500 5550 8 (800) 555 5550".

The main banner reads "Сбербанк ОнЛ@йн — просто, быстро, безопасно!". Below it, a text box explains: "Запрос номера мобильного телефона со ссылкой на ошибку доставки SMS и необходимостью подключить услугу Мобильный банк — Банк **не** запрашивает мобильный телефон и другую персональную информацию для входа в личный кабинет".

Below this, a message says: "Для того, чтобы войти в Сбербанк ОнЛ@йн, подключите услугу «Мобильный банк»:". A yellow warning box below that states: "Доставка SMS не выполнена. Карта, по которой был осуществлен вход в систему, не подключена к услуге «Мобильный банк». Услуга предоставляется бесплатно".

At the bottom, there is a form with the label "Введите номер телефона:" and a text input field containing "+7". A callout box points to the form area, stating: "Обратите внимание - номер мобильного телефона вводится без кода страны".

On the left side, there are news items under the heading "НОВОСТИ". One item is dated "07 ноября 2011" and titled "ВНИМАНИЮ КЛИЕНТОВ ДАЛЬНЕВОСТОЧНОГО БАНКА!!". Another is dated "25 сентября 2011" and titled "ВНИМАНИЕ КЛИЕНТОВ СЕВЕРО-КАВКАЗСКОГО БАНКА".



Адрес отправителя может оканчиваться на @sbrf.ru и @sberbank.ru - так же, как официальные адреса банка. В официальных письмах банк всегда обращается к клиенту по имени и указывает конкретные реквизиты, в зависимости от типа письма (например - тип карты, номер счета). Мошенникам такая информация как правило не известна и письма от них всегда будут выглядеть "обезличенными" (в обращении указаны только общедоступные данные, например адрес электронной почты) или содержать неверные (другого человека) данные.

Варианты имени отправителя:

- Сбербанк ОнЛ@йн
- Сбербанк России
- Руководитель подразделения (ФИО)
- Сбербанк Информ

Возможны другие имена.

К письму может быть прикреплен файл (вложение). Название зачастую указывает на его важное содержание, с которым надо немедленно ознакомиться. Расширение такого файла может быть различным.

Варианты темы письма:

- Сообщение об увеличении задолженности
- Сообщение увеличения долга
- Сообщение об увеличении задолженности на ДД.ММ.ГГГГ

Возможны другие варианты в поле «Тема:»

От кого: Сбербанк Информ <statistics@sber.ru>
 Кому: <[адрес вашей почты](#)>
 Дата: дата получения письма
 Тема: Сообщение о увеличении задолженности

очень_важный_документ.exe

Варианты адреса отправителя:

- statistics@sber.ru
- noreply@sber.ru
- info@sber.ru
- reply@sber.ru
- reply@sberf.ru
- statistika@sber.ru
- statistix@sber.ru
- manager@sberb.ru
- SberbankOnlineStatistics@sber.ru
- sberbankinfostatistics@sber.ru
- info@unitex-temac.ru
- stat@sber.ru

Возможны и другие варианты.



СБЕРБАНК РОССИИ

СООБЩЕНИЕ ОБ УВЕЛИЧЕНИИ ДОЛГА

Здравствуйтесь [адрес вашей почты](#)

По нашим данным на ДДММ.ГГГГ Вы превысили максимальную отсрочку платежа
посмотреть статистику по счету вы можете по ссылке ниже

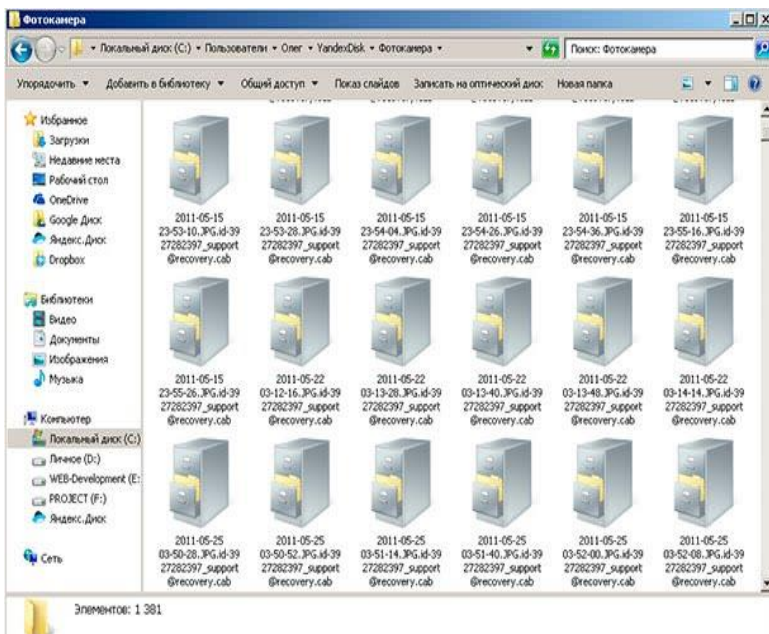
[ПОСМОТРЕТЬ СТАТИСТИКУ](#)



Вирусы-шифровальщики или криптографические вирусы.

Особый вид программного обеспечения, который осуществляет шифрование файлов на жестком диске.

Наибольшей угрозе подвержены файлы документов, офисных программ и фото изображений (**.jpg, .txt, .rtf, .doc, .xls, .zip**), а так же базы данных.



Криптовirus преобразовал все фотографии на компьютере в файлы, которые нельзя открыть, расшифровать и переименовать.



Windows.

Методы
заражения
вредоносным ПО
существуют для
всех платформ –
Windows,
Android,
Apple.

Зловреды

Антивирусное
ПО должно
присутствовать
на всех
устройствах –
компьютерах,
ноутбуках,
телефонах.



iOS.



Android.



Липецкая
область

Интернет вещей (Internet of Things, IoT)

**Обязательная смена всех заводских паролей.
Обновление «прошивки» устройств.**

Типичный функционал Smart TV:

- Чат, блоги, переписка с друзьями и семьей пока вы смотрите ТВ.
- Доступ к Facebook, Twitter and Google Talk одним нажатием.
- Возможность сидеть в социальной сети без использование доп. устройств таких как ПК.
- Возможность общения с помощью известного оператора звонков — Skype
- Видеозвонки также возможны при подключении **web-камеры.**

"Интернет Вещей"
(Internet of things, IOT) -
единая сеть, соединяющая
окружающие нас предметы
с виртуальным миром.



Хакеры получают доступ к:

- К настройкам телевизора и списков каналов.
- SecureStorage счетов.
- Виджетам и их конфигурациям.
- Историям фильмов на USB.
- Firmware.
- Всем разделам телевизора.
- USB-дискам присоединенным к телевизору.
- **Возможность наблюдать за вами через веб-камеру встроенную в ТВ.**⁹



**Ввод логинов, паролей (персональных данных)
только с компьютеров (мест) в которых Вы уверены!**

- Совершать покупки на «доверенных» сайтах.
- При совершении платежа в интернете, отдавать предпочтения магазинам поддерживающим технологию Verified by Visa /или MasterCard SecureCode (после ввода информации о банковской карте Вы будете перенаправлены на аутентификационный сервер банка для подтверждения правомерности операции).
- Использовать виртуальную карту.
- При выборе способа оплаты отдавать предпочтения сервисам электронных платежей (PayPal, Яндекс деньги, WebMoney и т.д.)





Липецкая
область

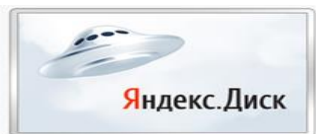
Что делать???

(Резервное копирование
и антивирусы)

АНТИВИРУС НЕ ОБЕСПЕЧИВАЕТ 100% БЕЗОПАСНОСТИ!

Обновление Windows

Обновление программ



Google Drive

Dropbox

- Простота использования
- Доступ с любого устройства
- Бесплатный объем 5-10 Гб

- Лицензионный антивирус (бесплатная версия)
- Обновление 1-3 дня
- Не выключать



McAfee
Proven Security™



symantec.

Спасибо за внимание!
Вопросы?

Шахнюк Михаил Наумович
Администрация Липецкой области
Ведущий консультант отдела
Отдел информационной безопасности
Управление делами
Эл.почта: mikh@admlr.lipetsk.ru