



# «Безопасность интернет-платежей»

Презентация подготовлена ТО Управления  
Роспотребнадзора по Алтайскому краю в городе  
Славгороде, Яровое, Бурлинском, Хабаровском и  
Немецком национальном районах

# Правила безопасности при электронных платежах

- ◎ Согласно п.1 ст. 4 ФЗ от 27.06.2011г. № 161 «О национальной платежной системе» платежные услуги должны предоставляться на основе договора. Такие договоры обычно ссылаются на правила соответствующей системы и подразумевают автоматическое присоединение к ним при подписании. Перед использованием платежных услуг, до создания учетной записи в платежной системе и выполнения в ней первого платежа необходимо ознакомиться с правилами данной системы и с договором.

## При этом платежная организация обязана:

- ⦿ - информировать клиента о совершении каждой операции с использованием электронной системы платежей (ЭСП);
- ⦿ - уведомлять клиента о невыполнении платежа не позднее дня, следующего за днем, когда было сделано распоряжение, а для электронных платежей незамедлительно;
- ⦿ - фиксировать направленные клиенту и полученные от клиента уведомления и хранить соответствующую информацию не менее трех лет;
- ⦿ - обеспечить возможность направления клиенту уведомления об утрате (незаконном использовании) ЭСП;
- ⦿ - возместить потребителю сумму операции, совершенной без его согласия или в случае нарушения правил информирования клиента об оспоренной операции.

# Электронные деньги

- Бумажные деньги исчерпали себя полностью, как исчерпал себя и век бумажных денег - XX век. Сегодняшний мировой кризис - есть кризис перехода с бумажных денег на электронные.

Электронные деньги - денежная стоимость, измеряемая в валютных единицах, хранящаяся в электронной форме на электронном устройстве, находящемся во владении потребителя



## Свойства Э.Л. :

- 1. хранится на электронном устройстве;
- 2. эмитируется после получения денежных средств в размере не менее объема принимаемых на себя обязательств;
- 3. принимается в качестве средства платежа не только эмитентом, но и другими фирмами.

# Виды электронных денег

Электронные деньги разделяют на два вида по носителю: на базе карт (card — based) и на базе сетей (network — based). В свою очередь, и первая, и вторая группа подразделяются на анонимные системы, позволяющие проводить операции без идентификации пользователя, данные системы близки по сути к традиционному понятию наличных денег. Не анонимные системы требуют обязательной идентификации участников системы.

Из наиболее известных систем на базе карт, можно выделить такие проекты, как Mondex, Proton, CLIP, Visa Cash. К электронным деньгам на базе сетей можно отнести с той или иной долей отличий: WebMoney, Яндекс.Деньги, PayPal, E-Gold, RuPay, e-port, Rapida



Чарльз Фридмэн, известный американский исследователь, профессор отделения экономики Гарвардского университета, добавляет к этим двум группам еще «устройство доступа» (access devices) - торговые автоматы и системы дистанционных банковских услуг по телефону или через компьютер

# Пластиковые карты

Пластиковая карточка - это обобщающий термин, который обозначает все виды карточек, различающихся по назначению, по набору оказываемых с их помощью услуг, по своим техническим возможностям и организациям



# Виды мошенничества

## 1. Телефонные мошенничества



## 2. Мошенничества с пластиковыми картами

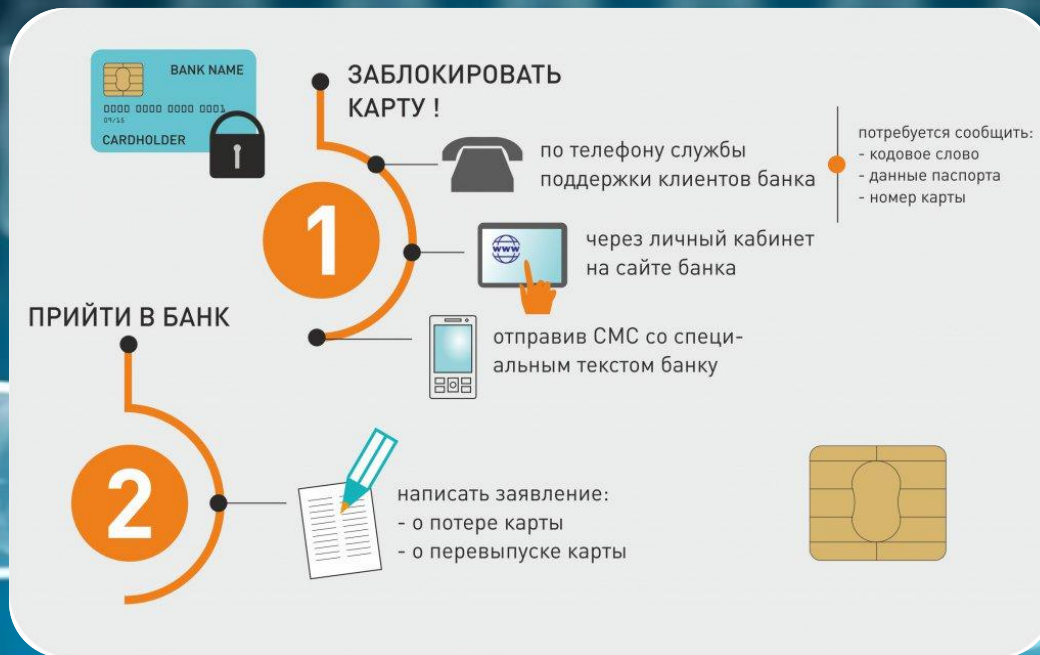


## 3. Фишинг



## 4. Мошенничества при операциях с банкоматами





- Если карта или данные о ней потеряны, а кошелек «взломан» — их нужно немедленно заблокировать, сообщив в платежную организацию. В случае ошибочного или несанкционированного платежа необходимо незамедлительно сообщить в платежную организацию до конца следующего дня, чтобы сумма этой операции была полностью возмещена. Если уведомление поступит позже, вернуть деньги будет гораздо сложнее. Чтобы платежная организация могла информировать клиента, он должен своевременно сообщать платежной организации актуальную контактную информацию.

# При расчетах с использованием электронных платежей следует руководствоваться основными правилами безопасности

- 1. Желательно подключить SMS-уведомления.
- 2. Вовремя обновлять контактные данные.
- 3. Не допускать посторонних к банковской карте, электронному кошельку, мобильному телефону и компьютеру (на которых имеется доступ для совершения электронных платежей).
- 4. PIN-код нужно помнить, не хранить на бумажном носителе в доступных местах, никому не говорить, никогда не вводить в интернете, прикрывать рукой при вводе через терминал.
- 5. Использовать сложные и разные пароли, регулярно их менять, никому не сообщать и не пересылать.
- 6. Не использовать функцию запоминания паролей и автоматической авторизации в платежных интернет-сервисах.
- 7. Желательно использовать режим «Инкогнито» (приватный) при совершении покупок через интернет. Удалять информацию о платежах с помощью очистки буфера файлов (cache) и файлов сохранения данных (cookies).
- 8. Избегать SMS-платежей на короткие номера для оплаты интернет-услуг и переводов непроверенным получателям.
- 9. Не реагировать на сообщения якобы от банка или оператора платежей, если предлагается перерегистрироваться, повторно ввести данные, перезвонить и т. п.
- 10. Совершать покупки в интернете нужно с помощью отдельной банковской карты и только на проверенных сайтах.
- 11. Незамедлительно сообщить в платежную организацию, если кошелек «взломан», карта потерялась, скомпрометирована или с нее без согласия держателя списаны деньги.
- 12. При пользовании банкоматом проявлять осторожность, обращать внимание на посторонних вокруг, на подозрительные устройства и наклейки в местах ввода PIN-кода и карты.

- При трансграничных покупках особенно высокое значение приобретает репутация продавца (это должна быть известная на рынке фирма с хорошей репутацией и отзывами людей, вызывающих доверие).
- С недобросовестного иностранного продавца взыскать денежную сумму будет очень сложно. В проблемных ситуациях стоит обратиться к администрации интернет-магазина — иногда они готовы возмещать потери покупателей за свой счет. Во избежание потерь на конвертации — выяснить в платежной организации ее порядок и размеры комиссий.
- Надежные системы безналичных платежей требуют при совершении платежа дважды пройти идентификацию по разным каналам. Например, банк может присылать клиенту на мобильный телефон дополнительный одноразовый пароль, который надо ввести в отдельную интернет-форму. В этом случае мошенник не может взять чужие деньги, даже если украл банковскую карту или узнал основной пароль.
- Данный метод защиты называется 3D Secure (или Secure Code).
- Неосторожность при пользовании интернетом может привести к утечке персональных данных. Злоумышленники также могут получить их путем обмана, взлома интернет-магазинов с данными плательщиков, установки шпионских программ.

# Безопасность интернет-платежей:

- 1. Не кликать по ссылкам, предлагающим получить призы, подарки, льготы и пр.
- 2. Избегать сайтов с большим количеством рекламы, автоматически открывающимися окнами, переадресацией.
- 3. Новые программы и обновления брать только из проверенных источников. Регулярно обновлять антивирусные и антишпионские программы. Пользоваться платежными системами, которые требуют двойной авторизации (3D Secure).
- 4. Не реагировать на e-mail или оператора платежей, если предлагается перерегистрироваться, повторно ввести данные и т. п. Перезванивать в справочную службу банка или оператора платежей, чтобы перепроверить подлинность подобного запроса.
- 5. При использовании интернет-сервисов, запрашивающих персональную информацию (почтовые ящики, социальные сети и пр.), убедиться, что в адресной строке браузера текст начинается с https — это признак защищенного протокола.

# Использованные материалы:

1. Сайт <http://46cge.rospotrebnadzor.ru/content/правила-безопасности-при-электронных-платежах>
2. <http://www.webmoney.ru>
3. <http://www.e-commerce.ru>
4. <http://ru.wikipedia.org>

A close-up, blue-tinted photograph of a calculator keypad. The focus is on the lower part of the keypad, showing several rows of buttons. The text 'Спасибо за внимание!!!' is overlaid in a bold, yellow, sans-serif font. The background is a blurred view of the rest of the calculator and its keypad.

**Спасибо за внимание!!!**