*ЗА ПРАВА ЗАЁМЩИКОВ

ONF.RU/ZPZ
ЗАПРАВАЗАЕМЩИКОВ.РФ

ОБЩЕРОССИЙСКИЙ НАРОДНЫЙ ФРОНТ

Электронные деньги и платежи в сети Интернет

План лекции:

1. Развитие электронных платежей в России
2. Виды кибермошенничества и способы защиты от него.
3. Мошенничество на сайтах объявлений и в социальных сетях.

1. Развитие электронных платежей в России

Электронное средство платежа, согласно Федеральному закону 161-ФЗ от 27 июня 2011 г. "О национальной платежной системе", это средство и способ, позволяющие людям обмениваться безналичными денежными переводами с использованием информационно-коммуникационных технологий.

Электронные средства платежа – это

- **Платежные карты, обслуживаемые разными платежными системами (Visa, MasterCard, UnionPay, «Национальная система платежных карт» и др.),**
- **Системы мобильных и интернет-банков,**
- **Электронные счета-«кошельки» в платежных системах (Яндекс.Деньги, WebMoney, PayPal и др).**

Развиваются и другие технологии, например, технология NFC, позволяющая использовать сим-карту мобильного телефона в качестве средства бесконтактного платежа. Средства за оплату товаров и услуг списываются бесконтактно, при приближении телефона к терминалу оплаты.
В сентябре 2016 года о приходе на российский рынок электронных платежей объявила компания Apple. К приему и обработке платежей через ApplePay планируют присоединится крупнейшие банки России, в том числе Сбербанк. Для оплаты покупки с помощью Apple Pay достаточно просто поднести iPhone к терминалу оплаты и приложить палец к Touch ID. Провести оплату можно даже без подключения к сети. Сервис поддерживается на смартфонах Apple начиная с модели iPhone 5 и на часах Apple Watch.
Развивается технология блок-чейн, позволяющая проводить операции с криптовалютами типа биткоинов.
В сентябре 2016 года социальная сеть Вконтакте запустила сервис электронных платежей между своими пользователями. Сумма перевода может составлять до 75 тысяч рублей, комиссия – 1% от суммы перевода, минимум 40 рублей. При отправке перевода деньги будут списываться с банковской карты пользователя. Техническую поддержку сервиса обеспечивает банк ВТБ24, компания «МультиКарта» и процессинг Mail.Ru Group.

В России число активных пользователей электронных денег и платежей оценивается примерно в 20-22 млн человек (15% населения), большинство из них - люди в возрасте 25-34 лет. Примерно половина из них проживает в городах-миллионниках (Москва, Санкт-Петербург, Новосибирск, Екатеринбург, Нижний Новгород, Казань и др.), другая половина - в средних и малых городах.
Маркетинговые исследования позволили оценить, на какие цели обычно направляются электронные платежи:

- **Телекоммуникационные услуги (мобильная связь, Интернет, кабельное и спутниковое ТВ, фиксированная связь и т.п.);**
- **Оплата покупок в интернет-магазинах, ярмарках и каталогах;**
- **Оплата онлайн-игр;**
- **Услуги жилищно-коммунального хозяйства (квартплата, электроэнергия, вода)**
- **Погашение кредитов;**
- **Перевод денег третьим лицам (семье и близким, друзьям и др.);**
- **Благотворительность.**

Растущее число безналичных переводов и их сумм привлекли в эту сферу внимание преступности, в первую очередь кибер-мошенников и хакеров, которые могут действовать как «в одиночку», так и в интересах организованной преступности.

2. Виды кибермошенничества и способы защиты от него.

Мошеннические атаки, направленные на пользователей электронных платежей, можно условно разделить на два типа:

- **Технические:** вредоносные программы, технические устройства типа скиммеров и др.
- **Психологические:** трюки и обман, рассчитанные на введение в заблуждение пользователей.

ЗАЩИТА ОТ ТЕХНИЧЕСКИХ СРЕДСТВ, ИСПОЛЬЗУЕМЫХ МОШЕННИКАМИ

Платежные сервисы и их службы безопасности активно противодействуют мошенникам. Однако, их усилия направлены в основном против технических способов мошенничества. Для защиты данных о пользователях и операциях используются сложные технологические решения:

- **Защищенные протоколы передачи данных (например, протокол HTTPS),**
- **Шифрование данных,**
- **Уникальные цифровые ключи идентификации пользователей (одноразовые смс-пароли, электронная цифровая подпись).**

Платежные сервисы имеют специальное программное обеспечение, которое может проводить мониторинг всех совершенных операций в системе за период (например, за сутки), анализировать эти операции и выявлять подозрительную активность. Подозрительными могут показаться нетипичные операции, например, когда с одного счета быстро проводится много платежей в адрес различных получателей, или когда к счету подключился кто-то с нового устройства и сразу произвел крупный денежный перевод.

Сейчас активно развиваются новые способы высокотехнологичного мошенничества, когда злоумышленники пытаются получить удаленный доступ к компьютеру, мобильному телефону, планшету пользователя и завладеть его управлением. Для этого рассылается вредоносное программное обеспечение на электронные адреса граждан либо используются ссылки на вредоносные ресурсы. Преступники также активно используют социальные сети для рассылки вредоносного программного обеспечения и ссылок.

В защиту от таких действий операторы электронных платежей внедряют в свои сервисы антивирусное программное обеспечение или предлагают пользователям бесплатные антивирусные программы. Например, Сбербанк с 2015 года встроил в свое мобильное приложение Сбербанк Онлайн для Android антивирус Касперского, который следит за тем, чтобы пользователь не установил подозрительное ПО.

ЗАЩИТА ОТ ПСИХОЛОГИЧЕСКИХ ПРИЕМОВ, ИСПОЛЬЗУЕМЫХ МОШЕННИКАМИ

Как показывает практика, даже самая совершенная система безопасности не защитит пользователя, если он сам предоставил мошенникам доступ к своему счету. Как это происходит?

Способ «выуживания» конфиденциальной информации у пользователей электронных денег и владельцев платежных карт получил название фишинг (от англ. fishing — рыбная ловля, выуживание).

Фишинг ведется через рассылки sms-сообщений, сообщений в социальных сетях и мессенджерах, электронных писем. В качестве авторов таких сообщений могут указываться популярные бренды, крупные компании, банки. Мошенники пытаются различными психологическими приёмами побудить клиента перейти по ссылкам или открыть вложение письма, чтобы затем передать свои персональные данные и реквизиты карты.

Компрометированные данные используются для совершения операций в сети Интернет. В сообщении или письме может содержаться прямая ссылка для перехода на сайт банка, который внешне может быть не отличим от настоящего. Поэтому необходимо проверять, какой адрес указан в адресной строке браузера. Те держатели карт, которые «повелись на удочку» и не отличили поддельный сайт от настоящего, вводят все необходимые данные, после чего злоумышленники как можно быстрее стараются списать средства со счета.

Фишинговые сообщения стараются встревожить держателя карты и вызвать его немедленную реакцию. Поэтому в теме письма или сообщения обычно пишется «срочно», «важно», «заблокирован доступ к счету», «у вас обнаружена задолженность» и т.п. Такой призыв, как правило, привлекает внимание и заставляет человека пройти по веб-ссылке для получения более подробной информации.

Разновидностью фишинга является вишинг (voice fishing), то есть голосовой фишинг. Основное отличие вишинга в том, что так или иначе задействуется телефон. Целью также является получение доступа к конфиденциальным данным владельца карты.

Мошенники осуществляют массовые рассылки, побуждающий держателей карт позвонить на определённый телефонный номер. При звонке на указанный номер, держателю карты в автоматическом режиме зачитывается сообщение, в котором просят сообщить конфиденциальные данные. Беседу также может вести и обычный собеседник, представляющийся сотрудником банка.
Например, чтобы снять деньги с карты, достаточно узнать номер карты и CVV2-код (последние три цифры с обратной стороны карты, cvv2 – card verification value 2).

На телефон владельца карты приходит смс о том, что он выиграл приз в лотерее или по акции, например, ноутбук. Просят позвонить по указанному контактному телефону для получения приза. Если человек звонит, ему предлагают вместо ноутбука перевести деньги в

размере стоимости ноутбука на карту. Для осуществления перевода просят сообщить номер карты и CVV-код, и если владелец карты сообщит эти данные, то деньги с карты могут исчезнуть мгновенно.

Также Вам могут позвонить, представится сотрудником банка и сообщить о просрочке по кредиту. Вы возмутитесь, особенно если Вы не брали никаких кредитов. Тогда Вам предложат сверить номер карты, заставив его назвать, а также подтвердить CVV-код. Аналогичный звонки могут поступать от якобы сотрудников интернет-магазинов, которые сообщают что платеж не прошел и просят сверить номер карты и CVV-код.

Помните, все что нужно мошенникам - получить номер Вашей карты и CVV-код. Если такое мошенничество сработает, то вскоре Вы обнаружите, что Вашей картой расплатились где-то в интернет-магазине или сделали с нее перевод на другой счет.

СОВЕТЫ ПО ЗАЩИТЕ ОТ ФИШИНГОВЫХ СООБЩЕНИЙ

Внимательно относитесь к поступающим на Ваши электронный адреса и аккаунты письмам и сообщениям. Не спешите переходить по предлагаемым ссылкам. Лучше самостоятельно вводить веб-адрес в адресную строку.

Если Вы перешли по ссылке и Вам предлагается ввести фамилию, имя, отчество, номер карты, CVV или ПИН код – никогда не делайте этого.

Банки не рассылают срочных писем для своих клиентов и сообщений по email, соц.сетям и мессенджерам. Если сотруднику Банка нужно срочно связаться со своим клиентом, он использует телефонную связь.

Мошенники не обладают информацией о персональных данных клиента (в частности его фамилией, именем и отчеством), поэтому в своих письмах используют общие обращения, например, «Уважаемый клиент Банка» и т.п.

При получении sms-сообщений, информирующих о каких-либо проблемах с банковской картой и содержащих просьбу перезвонить на указанный в сообщении телефонный номер, не перезванивайте. Банки обычно не рассылают сообщений с подобным содержанием. Зайдите на официальный сайт своего банка и позвоните на горячую линию и спросите о правомерности полученных сообщений.

Если Вы сомневаетесь в том, что Вам на самом деле поступил звонок из Банка, не вступайте в диалог и положите трубку. Зайдите на официальный сайт своего банка, позвоните на горячую линию и спросите о правомерности предыдущего звонка.

Сотрудники банка никогда не будут спрашивать данные Вашей карты и другую персональную информацию, так как эти данные (кроме секретного ПИН-кода, который должны знать только Вы) записаны в базу данных банка и доступны для сотрудников банка.

3. Мошенничество на сайтах объявлений и в социальных сетях.

ФИНАНСОВЫЕ СХЕМЫ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ КОШЕЛЬКОВ

На разных форумах размещается сообщение, в котором публикуется список из 3-6 электронных кошельков. Пользователю предлагают участие в схеме: отправить на каждый кошелек небольшую сумму денег, а потом разместить такое же сообщение на десятках других форумов, добавив свой кошелек в данный список вместо последнего. Приводится подробный расчет, как в течение нескольких месяцев сумма, полученная пользователем, возрастет в десятки раз.

На самом деле с вероятностью 99% пользователь не получит ничего, злоумышленники таким способом просто обирают доверчивых и склонных к азарту людей. Возвратить уже перечисленные деньги не представляется возможным, так как местонахождение мошенников обнаружить практически невозможно.

Меры электронной гигиены: не стоит пускаться в сомнительные финансовые схемы, напоминающие сетевые пирамиды. В результате пользователь потеряет собственные средства, не получив взамен ничего, кроме негативного опыта.

ВЫМОГАТЕЛЬСТВО ЗА РАЗБЛОКИРОВКУ КОМПЬЮТЕРА (ТЕЛЕФОНА, ПЛАНШЕТА)

На разных форумах размещается сообщение, в котором публикуется список из 3-6 электронных кошельков. Пользователю предлагают участие в схеме: отправить на каждый кошелек небольшую сумму денег, а потом разместить такое же сообщение на десятках других форумов, добавив свой кошелек в данный список вместо последнего. Приводится подробный расчет, как в течение несВ результате посещения сайта, открытия письма или сообщения из соц.сети, зараженного вредоносной программой, происходит блокирование интернет-браузера или компьютера.

Пользователь получает сообщение следующего содержания "Для возобновления работы отправьте SMS на указанный номер, и Вы получите код для разблокировки". При отправке SMS происходит списание всех денег со счета абонента.
Меры электронной гигиены: будьте внимательны к ресурсам, которые Вы посещаете или которые Вам предлагают посетить путем рассылок e-mail, сообщений и смс.
Установите и регулярно обновляйте антивирусное программное обеспечение своих электронных девайсов.

Если произошла так называемая «блокировка» – не паникуйте! Перезагрузите компьютер, осуществите проверку компьютера на вирусы. Если указанные меры не помогли - обратитесь к профессиональным специалистам технической поддержки.
кольких месяцев сумма, полученная пользователем, возрастет в десятки раз.
средства, не получив взамен ничего, кроме негативного опыта.

На самом деле с вероятностью 99% пользователь не получит ничего, злоумышленники таким способом просто обирают доверчивых и склонных к азарту людей. Возвратить уже перечисленные деньги не представляется возможным, так как местонахождение мошенников обнаружить практически невозможно.

Меры электронной гигиены: не стоит пускаться в сомнительные финансовые схемы, напоминающие сетевые пирамиды. В результате пользователь потеряет собственные

СХЕМЫ ОБМАНА ПОЛЬЗОВАТЕЛЕЙ НА ДОСКАХ ОБЪЯВЛЕНИЙ (AVITO.RU И ДР.)

Мошенники размещают на популярных досках объявлений (например, Avito.ru) объявления о продаже квартиры, машины и других ценных товаров по цене, значительно ниже среднерыночных. Например, автомобиль, обычная цена продажи которого 500-600 тысяч рублей, предлагают по 300 тысяч рублей.

В случае звонка по указанным контактным данным, клиенту сообщают, что продавец согласен на сделку, но просит срочно прислать задаток или предоплату, так как на данный товар поступает много других заявок.

Не стоит торопиться и переводить деньги - с большой вероятностью Вы их лишитесь. Похожие схемы применяются на сайтах объявлений о поиске работы. Человек находит интересную вакансию с указанным высоким уровнем заработной платы и откликается на нее. Ему сообщают, что его кандидатура подходит и будет одобрена на указанную вакансию. Однако, сначала ему надо оплатить какие-нибудь обучающие курсы или материалы, или внести какой-либо денежный взнос.

Меры электронной гигиены: сообщайте о подозрительных объявлениях администраторам (службе поддрежки) сайтов объявлений.

Отдавайте предпочтение работе с "проверенными" продавцами, то есть имеющими большое число отзывов, подтвержденный статус, проверенные контактные данные и т.п.
Избегайте подозрительных предложений с нереалистичными ценами, отказывайтесь от предоплат и задатков.

«ЛИПОВЫЕ» ИНТЕРНЕТ-ОБМЕННИКИ

В России криптовалюты пока не получили широкого распространения. Однако способы обмана владельцев биткоинов и других криптовалют уже есть. В частности, поддельные обменные пункты криптовалют в Интернете.

На этих сайтах пользователям предлагают бесплатный обмен криптовалют по очень выгодному курсу, который существенно отличается от курсов, определенных на общепризнанных интернет-биржах криптовалют.
На самом деле никакого обмена валют не происходит, у пользователя похищаются средства, переведенные для обмена. Пользователь может получить сообщение о том, что «проводятся технические работы». Возвратить уже перечисленные деньги не представляется

возможным.

Меры электронной гигиены: не осуществляйте обмен криптовалют на малоизвестных, новых, подозрительных сайтах.

Сверяйте предлагаемый курс обмена криптовалют с курсами обмена на общепризнанных интернет-биржах

* **https://ru.bitstamp.net/**
* **https://www.cryptonit.net/**
* **https://btc-e.com/ и другие.**

*ЗА ПРАВА ЗАЁМЩИКОВ

«При реализации проекта используются средства государственной поддержки, выделенные в качестве гранта в соответствии с распоряжением Президента Российской Федерации от 05.04.2016 № 68-рп и на основании конкурса, проведенного Общероссийской общественной организацией «Российский союз ректоров».