АИнформационное агентство
«WEB-мониторинг»
Свидетельство ИА № ФС7733219 от 19 сентября 2008 года

Научно-практический электронный журнал

ФИНАНСОВЫЕ ПРАВОНАРУШЕНИЯ И ПРЕСТУПЛЕНИЯ

№ 8 (83) 2013
(выходит с октября 2006 г.)

Тема номера: Киберпреступность набирает обороты
Фото с сайта: http://www.computerra.ru/74214/bezopasnost-onlayn-platezhey/

Учредитель
ИП **Фединский Ю.И.**
www.webmonitor.ucoz.ru
www.finprest.ucoz.ru
webmonitor@yandex.ru
тел. 8 985 333 87 59

Москва
2013

Оглавление

Тема номера: Киберпреступность набирает обороты

25.06.2013

Специалисты отдела «К» провели пресс-конференцию в Воронеже

Заместитель начальника отдела «К» БСТМ ГУ МВД России по Воронежской области Александр Перцев и оперуполномоченный Илья Стародубцев провели пресс-конференцию в Воронеже.

Сегодня специалисты отдела «К» активно работают в направлении борьбы с преступлениями в телекоммуникационных сетях, по выявлению и пресечению преступлений, связанных с осуществлением электронных платежей в теле- коммуникационных сетях, в т.ч. с использованием пластиковых карт. В числе задач - борьба с незаконным оборотом радиоэлектронных средств и специальных технических средств, в т.ч. выявление и пресечение каналов их контрабандного ввоза, незаконного изготовления, сбыта и использования, и ведение мониторинга открытых глобальных и локальных компьютерных сетей с целью добывания информации о правонарушениях и правонарушителях.

Как стало известно ИА «Воронеж-Медиа», также в компетенцию службы входит борьба с незаконным оборотом объектов интеллектуальной собственности на электронных (машинных) носителях и преступлениями в сфере незаконного оборота порнографических материалов, в том числе и с участием несовершеннолетних. Специалисты отдела «К» противостоят и преступлениям в сфере компьютерной информации.

По словам Александра Перцева, анализ борьбы с преступлениями в сфере интеллектуальной собственности показывает, что количество преступлений данного рода уменьшается. Это, в первую очередь, связано с информированностью пользователей программного обеспечения об ответственности за его незаконное использование и вреде использования такого рода программ.

Сотрудниками правоохранительных органов больший уклон в деятельности сделан на профилактику указанного вида правонарушений. Ведется значительная разъяснительная работа с организациями. Специалисты службы рассказывают о вреде использования нелицензионного программного обеспечения, ответственности за его незаконное использование (гражданско-правовая, административная, уголовная). Однако, несмотря на предпринимаемые меры, проблема использования нелицензионного программного обеспечения остается острой и при выявлении таких фактов сотрудниками правоохранительных органов проводятся соответствующие мероприятия.

Также специалисты отдела «К» рассказали о проблемах, которые могут подстерегать владельцев пластиковых карт. Так называемые зарплатные проекты банков, сделавшие очень удобным процесс получения денежного довольствия, были взяты на вооружение руководством разных по своей сути организаций. Вместе с объемами таких операций растет и уровень «пластиковой» преступности.

Большое количество случаев мошенничества осуществляется с помощью так называемого «белого пластика», ряд сведений о карточках мошенники находят в Интернете. На этом белом пластике, по размеру, естественно, совпадающим с размерами карты, присутствует магнитная полоса с кодом карты. И злоумышленники умудряются, совершая с ними манипуляции, похищать крупные суммы.

Часто банки и Интернет-магазины опасаются, что подача заявления в ОВД может вызвать утечку информации и повлечь за собой скандал, который приведет к потере клиентов.

Непонимание особенностей преступлений, связанных с мошенничествами с использованием пластиковых карт, - одна из причин недостаточного взаимодействия правоохранительных органов и служб безопасности членов платежных систем в борьбе с этим видом преступности.

Но при всем этом полицейские уже имеют положительный опыт изобличения злоумышленников, осуществляющих хищения с банковских карт граждан. Так, пресечена и расследуется деятельность целой преступной группы, участники которой поставили на поток снятие денежных средств таким путем.

Полицейские рассказали журналистам о возможных способах мошенничеств и дали рекомендации, как избежать того, чтобы стать жертвой злоумышленников. Отмечалось, что многие думают, что неприятная ситуация может произойти с кем угодно, только не с ними, и легко оказываются в ловушке мошенников. Люди выполняют все действия, предложенные незнакомцами, видя малейшую выгоду. Например, рискуют немедленно делать перечисления за автомобиль, стоимостью более миллиона рублей, но предложенный через Интернет по цене в 300-400 тысяч. Или откликаются на предложение купить собаку породы «хаски», поступившее из Южной Африки, где такие животные не распространены. До сих пор граждане реагируют на

сообщения «ваш сын попал в ДТП, срочно нужны деньги, чтобы избежать ответственности». Сначала люди переводят деньги, и лишь затем проверяют правильность поспешного поступка.

Так же полицейские попросили журналистов довести до граждан информацию о необходимости быть более внимательными при подключении услуги «мобильный банк». Если она «привязана» к номеру телефона, то стоит быть особо осторожным при отказе от использования сим-карты. Номер телефона через определенное время может оказаться у другого человека, информация продолжит поступать и окажется доступна для постороннего. Было несколько случаев, когда новые обладатели телефонного номера использовали информацию в своих целях. Также важно правильно указывать свой номер телефона, прибегая к данной услуге. Иногда проблемами оборачивалась ошибка на одну цифру.

Так полицией пресечена деятельность преступной группы, которая изготавливала устройства, позволявшие вскрывать самые разные автомобили. «Услугами» воронежских злоумышленников пользовались преступники даже в других регионах.

http://www.voronezh-media.ru/news_out.php?id=41261

(*См.* также раздел **«Безопасное ведение бизнеса»**)

25.06.2013
Крытый банк
Деньги с карточек уходят осужденным?

«Ваша банковская карта заблокирована. Для разблокировки позвоните по номеру…», «Чтобы забрать приз — автомобиль — свяжитесь с нами по этому номеру», «Мама, положи 5 тысяч на телефон. Потом все объясню, попала в аварию, пишу с чужого номера».

Все это — примеры смс-мошенничества, с которыми сталкивался, пожалуй, уже каждый. Но если в ответ на последние две схемы не лишенные юмора челябинцы уже пишут обратные смс: «Вообще-то я папа…», «Сын, ты сменил пол?» или «Спасибо, я возьму деньгами», то сообщения, касающиеся банковских карт, до сих пор заставляют поволноваться многих.

Прощай, зарплата

Страна все больше переходит на безналичные расчеты, и почти все мы получаем свои «трудовые» на зарплатные карты. Однако это удобно не только для нас, но и для мошенников. Только по Челябинску и только по случаям незаконного перечисления денег с банковских карт за май было зафиксировано порядка 125 жалоб. Такие данные приводят в городском управлении МВД.

— Суть следующая. На телефонный номер приходит смс о том, что карта заблокирована в связи со взломом пин-кода (часто со ссылкой на Центробанк), а для разблокировки необходимо позвонить по определенному номеру, — поясняет Роман Самойлов, прокурор Калининского района Челябинска. — После чего поступят указания, что делать дальше.

Они будут нехитрые: мошенники предложат подойти к банкомату и провести серию не особо подозрительных операций, фактически продиктовав алгоритм перечисления денег с карты на мобильный телефон. Люди на это охотно ведутся, говорят правоохранители. Кто-то начинает волноваться в силу своего характера, у кого-то в этот момент карта — единственный способ расчета (допустим, за границей)…

Как объяснил Владимир Курочкин, сотрудник отдела уголовного розыска управления МВД России по Челябинску, номер сотового телефона — это своеобразный счет в банке. Когда сумма приходит на телефон, пользователь номера, имея подключенную услугу «Мобильный банк», может распорядиться деньгами как угодно, вплоть до оплаты заказов в интернет-магазинах. Чаще всего — платят «коммуналку» и перечисляют чужие заработки на телефоны своих родственников, подельников, друзей и подруг и т. п. И далее по цепочке.

— Суммы причиненного ущерба в нашей практике колебались от 7 до 40 тысяч рублей, — делится цифрами по Курчатовскому району Роман Самойлов. — Причем телефонные номера, как правило, принадлежат сотовым операторам других регионов, поэтому приостановить мошеннические операции маловероятно.

— Можно сказать, что 45 процентов таких преступлений не раскрывается, — подкрепляет практику статистикой Владимир Курочкин.

А все почему? Платежи, которыми пользуются мошенники — переводы денег с карты на сотовый, — работают в режиме онлайн. Это значит, что деньги перечисляются сию же секунду.

— Есть вероятность задержать средства, обратившись либо к своему сотовому оператору, либо в свой банк. Только очень быстро, — дает надежду Дмитрий Гасенко, заместитель начальника управления платежных средств ОАО «Челябинвестбанк». — Но люди, пострадавшие от действий мошенников, в себя приходят не сразу и звонят с большим опозданием, чаще всего на

следующий день. Поэтому случаев возврата денег мы не знаем. Озвученная статистика — это только часть общей картины: немало людей вообще не обращаются в органы МВД.

Ищи концы

Советы тем, кто получает «письма счастья»:

если вы вставили свою карту в банкомат, ввели пин-код, и она работает — это уже означает, что она не заблокирована, и не надо слушать мошенников и выполнять какие-то операции;

в первую очередь звоните в свой банк-эмитент. Операторы тут же проверят информацию и подробно все расскажут, ориентируясь на текст сообщения. Номер телефона указан на обратной стороне карты. У многих банков службы клиентской поддержки работают круглосуточно. Практически все телефоны бесплатны с любой точки;

сотовые компании анализируют все варианты мошенничества с использованием телефонов и приводят их на своих сайтах. Нелишне будет хотя бы иногда туда заглядывать.

Кроме перечисленных в статье есть и другие способы мошенничества с пластиковыми картами. Примеры мы попросили привести специалистов южноуральских банков и сотрудников правоохранительных органов.

Народные умельцы

Схема: Траппинг, или «ливанская петля», — вид мошенничества с использованием банкоматов. Мошенник в картридер вставляет кусок фотопленки (может быть использован и другой материал, чаще пластик), надрезанный таким образом, что карта, попадая в прорезь, не возвращается обратно владельцу, а попадает в некий конверт. Цель — подсмотреть пин-код, пока клиент мучается, вновь и вновь набирая его в попытках вернуть карту. Клиент потом сам карту не достанет, а мошенники смогут.

Как защититься: Обращайте внимание на наличие посторонних устройств на банкоматах, которые вы ранее не замечали.

Нехорошие айтишники

Схема: Злоумышленники устанавливают на банкоматы скимминговые устройства, считывающие данные магнитной полосы, а с помощью видеозаписи фиксируют пин-коды. Затем данные воспроизводятся на белом пластике и делаются копии пластиковых карт. Расследованием этих преступлений в Челябинске занимается специализированный правоохранительный отдел К.

Как защититься: Если стоит скимминговое устройство, карта выходит из картридера не полностью, ее трудно достать: там уже чисто геометрически все не так устроено. Сразу же обращайтесь в свой банк. Есть антискимминговые устройства, но это очень дорогие системы.

Давайте поговорим

Схема: Когда человек звонит на номер, указанный в сообщении, там его пытаются долго удерживать на линии, где минута соединения стоит, как потом оказывается, очень недешево. При этом пытаются выведать данные карточки. Мошенники запрашивают якобы для проверки и решения проблем безопасности номер карты, трехзначный код на обратной стороне карты и пин-код, и на всякий случай — кому принадлежит карта и какого она банка.

Как защититься: Ни при каких обстоятельствах нельзя передавать информацию о пин-коде третьим лицам.

Актерские труппы

Схема: Самый простой и самый действенный способ мошенников — это предложить свою помощь по снятию денег с карты пожилому человеку. Действуют, как правило, группами. Один, например, имитирует, что карта не вышла из банкомата, другой в это время уже бежит с этой картой и снимает деньги в соседнем банкомате.

Как защититься: Необходимо обращаться в центр клиентского обслуживания своего банка.

Копылова Эльвира Евгеньевна

http://up74.ru/rubricks/prestupnost-i-zakon/2013/06-ijun/krytyj-bank/

02.07.2013

В Первоуральске «электронные мошенники» за неделю «кинули» троих

Сразу три случая мошенничества с использованием банковских технологий и мобильных телефонов случились в Первоуральске в конце прошлой недели, сообщает пресс-служба главного управления МВД по Свердловской области. В каждом из случаев злоумышленникам удалось воспользоваться незнанием граждан и завладеть деньгами, которые находились на их банковских картах. Общая сумма ущерба составила почти 80 тысяч рублей.

Первый из печальных случаев произошел с мужчиной, который сам консультировал жителей города о том, как не попасться в лапы мошенников. О том, что он сам стал жертвой преступления, он узнал, когда проверял баланс своей банковской карты и не досчитался 12 880 рублей, сообщает пресс-служба ГУ МВД. Правоохранители установили причину: за несколько дней до случившегося, 25 июня, потерпевшему позвонил человек, который представился сотрудником

банка, и сообщил о том, что на счет мужчины якобы по ошибке перевели некоторую денежную сумму. Для того, чтобы установить этот факт, лже-сотрудник банка попросил мужчину проверить счет карты при первой же возможности и добавил, что вскоре перезвонит. Потерпевший сделал это, но изменений, по сравнению с прошлым обналичиванием карты, не заметил. Вскоре, действительно, поступил звонок от того же человека. Мужчина пояснил ему, что баланс карты не менялся, на что «сотрудник банка» предложил тому активировать услугу «Мобильный банк» с помощью указанного номера телефона. Мужчина, услышав о том, что услуга позволяет «в любой момент времени отслеживать движение средств на счете», согласился и совершил все предложенные действия.

Деньги пропали только на следующий день.

© «Вечерние Ведомости»

http://veved.ru/news/34087-v-pervouralske-yelektronnye-moshenniki-za-nedelyu-kinuli-troix.html

03.07.2013

Киберпреступность набирает обороты

Источник: CNews.ru

России еще предстоит столкнуться с проблемой интернет-мошенничества в полной мере, но эксперты рынка уже сейчас понимают, что необходим комплексный подход: сочетание законодательных мер, активного использования систем информационной безопасности основными операторами транзакций – банками и телекомом, интеллектуальной аналитики, организованного взаимодействия всех участников рынка позволяют добиться высоких результатов. И конечно, грамотность простого пользователя.

Чем выше уровень информатизации в стране, тем большую угрозу представляет киберпреступность. Например, за 2012 г. потери от мошенничества в Великобритании, по оценкам National Fraud Authority, достигли 73 млрд ф.ст., в других развитых странах наблюдается аналогичная ситуация.

России еще предстоит столкнуться с этой проблемой в полной мере.

http://www.crime-research.ru/news/03.07.2013/7640/

04.07.2013

Внимание: мошенники стали изощрённее!

На территории Белгородской области распространились факты мошенничеств. Потерпевшими в данных случаях, как правило, выступают люди пенсионного и пожилого возраста, которые входят в категорию самого социально-незащищённого слоя населения, что, в свою очередь, вызывает большой общественный резонанс. В результате преступных посягательств во всех случаях предметом хищения являются денежные средства, размеры которых колеблются от 5 000 до 200 000 рублей. В настоящее время преступники используют следующие схемы совершения мошенничеств.

«Ваш родственник попал в беду».

«Вы выиграли приз».

«Ваша банковская карта заблокирована».

«Приобретение автомобиля через Интернет».

«Вам полагается компенсация». Мошенничества данного вида совершаются в отношении престарелых граждан, т.к. они зачастую приобретают посредством сетевого маркетинга различные препараты, аппараты, предлагаемые им под видом медицинских. Неизвестные в ходе беседы с потерпевшим выясняют, приобретал ли он какой-нибудь товар из сферы сетевого маркетинга, помог ли он потерпевшему. Мошенник представляется работником прокуратуры и поясняет, что проводилась прокурорская проверка, либо что работников данной организации привлекают к уголовной ответственности, и товар, который был реализован, является не сертифицированным, а лицам, приобретавшим его, полагается компенсация в довольно крупном размере. При этом поясняет, что для получения денежных средств необходимо внести определённую сумму на расчётный счёт, для того, чтобы можно было провести операцию, открыть индивидуальную ячейку и т.д. После чего неизвестным оставляются либо абонентские номера якобы службы безопасности банка, либо просто номер расчётного счёта. Перечисление денежных средств совершается в несколько этапов. Зачастую мошенничества, совершённые указанным способом, имеют большую латентность, т.к. потерпевшие ожидают обещанной компенсации и длительное время не обращаются в правоохранительные органы, а лишь спустя 2-3 месяца. Описываемая схема получила распространение на территории Московской области.

http://belpobeda.ru/?module=articles&action=view&id=2149

08.07.2013

Сбербанк России объявил, что прекращает выпуск пластиковых карт без чипов.

Чипизация карт: новое дыхание

Неманья Никитович, управляющий директор Optima Infosecurity (Группа Optima)

Продиктовано это решение стремлением повысить безопасность хранящихся на карте данных и сделать борьбу со скимингом более эффективной. Карты с чипом и в самом деле обладают большей степенью защиты, чем карты без чипа: информацию, содержащуюся на чипе, невозможно скопировать, а любая операция по такой карте требует ввода пароля.

Возразить против этого нечего: карты с чипом, безусловно, значительно надежнее карт с магнитной лентой, именно поэтому в развитых странах Европы карты с магнитной лентой – это позавчерашний день, а карты с чипом (те самые, на которые бодро переходит один из крупнейших российских банков) – день уже почти что вчерашний. И вот почему.

Дело в том, что чип помогает справиться только с одним риском при платежах через карту, но никак не решает ситуацию с другими рисками, которые становятся все более распространенными. Связаны они как с физическим использованием пластиковых карт, так и с использованием только счета карты, а именно с платежами в Интернете.

Наличие чипа способно защитить пользователя от скимминга – кражи данных карты при помощи считывающего устройства, однако неспособно уберечь от фишинга – кражи данных о вашем онлайн-счете или вашей карте без считывающих устройств, удаленно и даже с использованием социального инжиниринга. Если скимминг – это арифметика, то фишинг – это уже алгебра.

http://bankir.ru/publikacii/s/chipizatsiya-kart-novoe-dykhanie-10003644/#ixzz2atEMOc1Y

09.07.2013

Киберпреступность набирает обороты

России еще предстоит столкнуться с проблемой интернет-мошенничества в полной мере, но эксперты рынка уже сейчас понимают, что необходим комплексный подход: сочетание законодательных мер, активного использования систем информационной безопасности основными операторами транзакций – банками и телекомом, интеллектуальной аналитики, организованного взаимодействия всех участников рынка позволяют добиться высоких результатов. И конечно, грамотность простого пользователя.

Чем выше уровень информатизации в стране, тем большую угрозу представляет киберпреступность. Например, за 2012 г. потери от мошенничества в Великобритании, по оценкам National Fraud Authority, достигли 73 млрд ф.ст., в других развитых странах наблюдается аналогичная ситуация. России еще предстоит столкнуться с этой проблемой в полной мере.

20 июня Информационное агентство РБК провело конференцию «Защита от мошенничества: современные подходы», в ходе которой эксперты обсудили современные вызовы и угрозы, создаваемые ростом киберпреступности в мире, и сценарии реагирования на них в различных плоскостях: законодательной, технической и информационной.

Синхронизация законов

Преступники подрывают доверие граждан к информационным системам, в том числе к электронным госуслугам, и тем самым наносят ущерб государству – поскольку государство инвестирует значительные средства в создание информационных систем, прежде всего в развитие электронных госуслуг. Разрабатываемая в Совете Федерации стратегия кибербезопасности призвана поставить заслон хакерам, защитить секретную информацию и предотвратить преступления в интернет-пространстве.

«Киберпреступления сложнее заметить, поэтому считать их еще нужно учиться», – сказал Руслан Гаттаров, член Совета Федерации, председатель Комиссии по развитию информационного общества. По данным разных информационных агентств, в мире от действий киберпреступников пострадало от 1 % до 17 % жителей. Разработчики антивирусов называют большие цифры, правоохранители меньшие. Достоверная картина не складывается, потому что киберпреступления сложно обнаружить, а с точки зрения законодательства, которое не поспевает за развитием технологий, не все вторжения в информационные системы можно квалифицировать как преступления.

Сказывается и низкая информированность граждан о рисках при пользовании платежными системами и совершении иных действий в интернете. Например, после опроса, проведенного в Европе, в ходе которого хотели выяснить, что пользователи знают об угрозах в сети, 15 % опрошенных решили отказаться от интернет-банкинга.

Среди проблем, которые препятствуют развертыванию более действенной борьбы с компьютерными преступлениями на государственном уровне, можно упомянуть несовершенство законодательства, отсутствие механизма регистрации жалоб на кибермошенничество и необходимость широкого международного сотрудничества спецслужб – тогда как у мошенников международная кооперация налажена очень хорошо.

Борьба с киберпреступностью только в своих границах малоэффективна. Однако формирование международных механизмов идет очень тяжело: постоянно встает вопрос о предоставлении данных за рубеж. «Нужны не подпольные договоры между спецслужбами, а практика взаимодействия и относительная синхронизация национальных законов», – сказал Руслан Гаттаров.

ЦБ за превентивные меры
Противодействовать сообща
Системы ДБО – основная мишень
Защита за разумные деньги
Начиная с аппаратного уровня
Операторы связи против мошенников
Аналитика как превентивная мера

Мировой опыт показывает, что предсказательная аналитика может с успехом применяться для раннего обнаружения неправомерных действий: с введением единой зоны платежей в евро стала возможной новая мошенническая схема, так называемая «карусель НДС», когда одни и те же товары многократно перемещаются через границу. НДС-разрыв в ЕС оценивается на уровне 70–100 млрд евро в год. Использование аналитических инструментов от компании SAS позволило сократить сроки выявления подозрительных операций с нескольких месяцев или даже лет до 1–2 дней, сообщил Виталий Угольков, руководитель направления по противодействию мошенничеству, SAS Россия/СНГ.

Данные решения построены на основе статистических и прогнозных моделей, которые помогают выявить случаи «нестандартного поведения» и обратить на них внимание оператора системы. Например, если средний размер транзакции для клиента 5000 руб., тогда транзакция на 35 тыс. будет «нестандартной» для клиента. Дальнейший сценарий может настраиваться в зависимости от требований клиента и оценки рисков – можно блокировать подозрительные операции, запросить у клиента дополнительное подтверждение или ограничиться уведомлением.

Недостатками этого метода является риск ложных срабатываний, когда блокируются законные операции, и трудность сбора статистических данных о поведении мошенников для построения прогнозной модели. Здесь на помощь могут прийти технологии Text Mining, применяемые для анализа полей анкетных данных, таких как профессия, должность, сфера деятельности, графа «другое», информация из внешних баз, социальных сетей, комментарии менеджеров по продажам и т. д. Использование неструктурированных данных в составе предикторов может повысить точность моделей на 20 %.

Особо стоит сказать о мошеннических сетях. Киберпреступления часто совершаются организованными группами, которые координируют свою деятельность по интернету. Здесь аналитические инструменты могут оказать помощь в проведении расследований и в предупреждении преступлений. Два человека связаны, если у них есть общие «характеристики»: например они указали один и тот же телефон, живут по одному адресу или рядом, работают в одной компании, переводят деньги друг другу или оба переводят деньги на один и тот же счет. Это часто актуально для страховщиков и интернет-торговли.

Безопасность электронной коммерции
Источник: cnews.ru
http://www.pcidss.ru/articles/134.html

10.07.2013
Джентльмены киберудачи

№10 (405), 10 июля 2013 года
Автор: Константин Геращенко

Львиная доля платежей и расчетов давно перекочевала в Сеть. Каждую секунду в Интернете совершаются сотни тысяч финансовых транзакций. Но, как это часто бывает, новые технологии породили и новые угрозы. Кибермошенничество быстро достигло угрожающих объемов и стало серьезной проблемой.

На западе, где электронные расчеты практически полностью вытеснили наличные деньги, потери банков, компаний и частных лиц от действий кибермошенников весьма значительны. Например, согласно исследованиям компании Javelin, уже в 2007 г. жертвами карточного мошенничества стали 6,8 млн. американцев, а потери составили 30,6 млрд. долл. Как утверждают эксперты ассоциации NHCAA, 3% общих затрат на медицинское обслуживание в США теряется в результате мошенничества в сфере медицинского страхования. В абсолютном выражении это 68 млрд. долл. А по данным ФБР это сумма в несколько раз больше — 226 млрд. долл. в год. В других социальных программах, таких как питание для малоимущих и выплата пособий по безработице, потери составляют 1,7 и 4 млрд. долл. соответственно. В Великобритании в

прошлом году из-за действий кибермошеников, по оценке National Fraud Authority, недосчитались 73 млрд. фунтов. Так называемое производственное мошенничество приносит среднестатистическому предприятию убытки в размере 5% его дохода. Валовый мировой продукт (Gross World Product) в 2011 г. составил 70,28 трлн. долл., а значит, в глобальном масштабе потери от мошенничества превысили 3,5 трлн. долл. Всего же в мире от действий киберпреступников пострадало до 17% жителей.

Несмотря на столь внушительные цифры, по настоящему обеспокоены масштабами кибермошенничества лишь банки и сообщества специалистов по информационной безопасности.

Ситуация в России, на первый взгляд, кажется более благополучной, но причина относительно невысоких абсолютных цифр потерь объясняется менее развитой инфраструктурой дистанционного банковского обслуживания (ДБО) и привычкой населения расплачиваться наличными деньгами. Специалисты прогнозирует, что в ближайшем будущем кибермошенничества станет больше, и уже сейчас уделяют много внимания методам противодействия этому злу, вырабатывают стратегию борьбы с ним. О высокой активности заинтересованных компаний и организаций свидетельствует большое число специализированных конференций и форумов. Одна из таких конференций под названием «Защита от мошенничества: современные подходы», прошла в июне в Москве под эгидой РБК. На этом мероприятии представители банков, властных структур, операторов связи и специализированных ИТ-компаний обсуждали современные угрозы и методы борьбы с ними.

Жертвой может стать каждый

Действительно ли угроза кибермошенничества в нашей стране высока, или страхи по этому поводу сильно преувеличены?

«Кибермошенничество стремительно растет, — утверждает **Дмитрий Кузнецов**, заместитель технического директора компании Positive Technologies. — Объем финансовых средств, которые обращаются в Интернете, не поддается точной оценке, но понятно, что это огромные деньги. Развитие современных технологий, появление смартфонов, интернет-банкинг, личные кабинеты пользователей, перенос туда способов оплаты — все это играет на руку мошенникам, у которых появляется больше возможностей для атаки».

Олег Глебов, эксперт по ИБ компании «Андэк», считает, что для физического лица риск и размер потерь связаны с манипуляциями с банковскими картами, а также интернет-платежами, осуществляемыми с различных гаджетов. Низкая осведомленность большинства людей в вопросах ИБ оборачивается для них пропажей денег, например, если зарплатную карту человек часто использует для оплаты покупок и услуг в Интернете. В данном случае кибермошенничество, как правило, носит разовый характер (например, кража всех денежных средств в момент поступления зарплаты на карту). Нередко физические лица становятся жертвами рассылок спама с вирусным ПО в социальных сетях или на популярных сайтах. Юридические лица также подвергаются целевым атакам все чаще, о чем свидетельствуют отчеты исследовательских агентств.

Жертвой кибермошенников, как отмечает **Сергей Кузнецов**, генеральный директор SafeNet в России и СНГ, становятся как частные лица, так и предприятия. Преступники ищут «слабое» место в защите периметра компании. «На данный момент уже нет той защиты, которую невозможно взломать», — подчеркнул он. По мнению Олега Глебова, чаще всего атакам мошенников подвергаются физические лица, так как они менее защищены, как технически, так и юридически. При этом средний размер кражи можно оценить примерно в 5–10 тыс. рублей. Что касается юридических лиц, то здесь успешных мошенничеств меньше, но средний размер потерь может исчисляться сотнями тысяч и миллионами рублей.

«Помимо банков, в поле зрения хакеров попали компании нефтегазовой индустрии, добывающие и перерабатывающие предприятия, — говорит **Алексей Лукацкий**, бизнес-консультант по безопасности компании Cisco. — Взламывая систему, они меняют работу бизнес-логики, чтобы украсть реальные продукты, например нефть. В случае воровства объем нефти на входе в трубу и на выходе будет разным, и задача мошенников — сделать так, чтобы эта разница как можно дольше оставалась незамеченной. А для этого надо перенастроить логику работы системы таким образом, чтобы она не реагировала на расхождение в данных. Похожий алгоритм используется и при хищении нефтепродуктов в цистернах, или руды в вагонах». Компании СМБ реже подвергаются атакам, поскольку не располагают большими суммами на счетах, а исчезновение даже небольшого количества денег сразу же будет замечено.

Как отмечет **Даниил Пустовой**, менеджер по развитию DNA Distribution, в прошлом году почти 20% киберпреступлений в мире совершены в России. Наиболее привлекательной для мошенников является слабо защищенная информация, что позволяет ее тем или иным способом украсть, и возможность быстро превратить эту информацию в деньги. «Кибермошенничество — наиболее распространенных преступление, — говорит **Олег Шабуров**, руководитель группы ИБ российского представительства Symantec. — Причина понятна: это самый быстрый и при этом самый легко маскируемый способ украсть деньги». **Александр Цыкунов**, руководитель Дирекции

маркетинга и продаж «Астерос Информационная безопасность», также считает, что развитие ИТ, рост потребностей бизнеса и частных лиц в информационных сервисах открывают для мошенников новые горизонты. В реализации любого сервиса заложен бизнес-процесс, в котором участвуют ИТ-системы и люди, работающие по определенному регламенту. «ИТ-системы, регламент и люди — вот три основных „мишени“ для атаки мошенников», — подчеркнул Цыкунов.

«Глобальный объем киберпреступлений растет с каждым днем: в соответствии с отчетом „Norton cybercrime report“, жертвами киберпреступников за год стали 556 млн. человек, это около 18 пострадавших ежесекундно, — говорит **Алексей Сизов**, руководитель группы противодействия мошенничеству компании „Инфосистемы Джет“. — Статистика в России не менее показательна. Все больше продаж товаров и услуг осуществляется с использованием электронных денежных средств или дистанционных сервисов оплаты. А это означает рост связанных с ними мошеннических действий. В среднем, каждый третий сталкивается с различными попытками мошенничества, включая дистанционные финансовые операции или банальные просьбы о пополнении баланса телефонного счета».

Жертвами мошенников по словам **Виктории Балюк**, заместителя председателя правления «Ренессанс Кредит», становятся все без исключения — от частных лиц до крупных компаний. Причем, атаки происходят непрерывно, и в этом на своем опыте убеждаются более полутора миллиона человек в день. **Николай Федотов**, главный аналитик компании InfoWatch, называет жертв кибермошенничества в порядке частоты инцидентов:

- пользователи платежных систем и систем ДБО;
- игроки популярных многопользовательских игр;
- предприятия здравоохранения и компании медицинского страхования;
- налоговые органы;
- лица, желающие приобрести нелегальный товар/услугу;
- торговцы интернет-магазинов и интернет-аукционов;
- граждане с повышенной доверчивостью;
- покупатели интернет-магазинов и интернет-аукционов;
- операторы персональных данных (только котируемых);
- нарушители авторских прав;
- игроки фондового рынка.

По словам **Федора Горловского**, старшего инженера Центра компетенций ИБ компании «АйТи», к кибермошенничеству можно отнести следующие виды противоправных действий:

- кардинг — операции с использованием платежных карт или их реквизитов, не инициированные или не подтвержденные их держателями;
- фишинг — получение доступа к конфиденциальным данным пользователей путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов или социальных сетей;
- вишинг — аналог фишинга с использованием телефона;
- фарминг — процедура скрытного перенаправления пользователя на ложный IP-адрес;
- мобильное мошенничество — связано с услугами мобильной связи, в частности, с короткими номерами для отправки SMS.

Так сколько же мы теряем?

«Суммы потерь компаний и доходов мошенников сильно разнятся, — говорит **Наталия Тесакова**, директор по маркетингу компании „Андэк“. — Одни считают возможные утраты, другие — реально украденные деньги. Каждая исследовательская компания дает результаты, основываясь на своем понимании темы мошенничества и киберпреступлений». По мнению Тесаковой, сегодня отсутствует единая общепринятая классификация кибермошенничества, или, на языке специалистов, «фрода» (от английского слова fraud — мошенничество, жульничество, обман). «Типов мошенничества очень много, и далеко не все они связаны с использованием ИС, — продолжает она. — Возьмем для примера один из видов фрода — мошеннические операции с банковскими картами. Обратимся к трем источникам цифр, связанным с карточным фродом, и удивимся, насколько сильно они разнятся. Согласно статистике компании Euromonitor International, на Россию в 2012 г. пришлось 91,4 млн. евро потерь от мошеннических операций с банковскими картами. По словам же **Анатолия Аксакова**, президента Ассоциации региональных банков „Россия“, который ссылается на данные Ассоциации российских членов Europay (АРЧЕ), ежегодная сумма потерь от преступных махинаций с банковскими картами составляет 2,5 млрд. долл.».

Продукт особого свойства

Системы для противодействия кибермошенникам — это не обычные продукты. Имея много общих черт и схожих функциональных возможностей по сравнению с другими решениями для ИБ, антифрод-системы, тем не менее, стоят особняком. Их главные особенности — сложность и

комплексность. Антивирусные программы, межсетевые экраны, DLP-системы, спам-фильтры — все они рассчитаны на выполнение одной задачи. ПО для противодействия мошенникам решает одновременно множество задач, анализирует большое число параметров и обрабатывает статистические данные.

Потенциальный объем — сотни миллионов

Системы противодействия кибермошенничеству получили на Западе большое распространение, поэтому объем рынка там весьма велик. По данным Gartner, в прошлом году он достигал 450 млн. долл. Показательна и его динамика. В 2010 г. рынок оценивался в 200 млн. долл., а в 2011 г. — в 270 млн. долл. Однако, по словам Андрея Комарова, в этих оценках не учтены объемы продаж ряда компаний, следовательно, их можно считать заниженными. Некоторые эксперты называют более высокие показатели — 270 и 304 млн. долл. соответственно.

Обречен на рост и развитие

Говоря о перспективах рынка систем противодействия кибермошенничеству, специалисты единодушны в своих оценках: он обречен на рост и развитие. Понятно, что будут появляться новые угрозы, и это потребует разработки и внедрения соответствующих средств защиты. А кроме того, серьезной движущей силой данного сегмента рынка стал принятый два года назад Федеральный закон № 161 «О национальной платежной системе», устанавливающий правовые и организационные основы национальной платежной системы, и регулирующий порядок оказания платежных услуг. В рамках данного закона определяются деятельность субъектов национальной платежной системы, требования к организации и функционированию платежных систем, порядок осуществления надзора и наблюдения в национальной системе.

http://www.crn.ru/numbers/reg-numbers/detail.php?ID=80658

10.07.2013

Безопасность онлайн-платежей

Автоматизация розницы

Автор: Наталья Жилкина 10 июля 2013

Вопрос о безопасности объектов электронной коммерции стоит очень остро. Сейчас не составляет проблемы с помощью «профессионалов» за небольшие деньги организовать DDoS-атаку на онлайн-ресурс конкурента. (Причем DDoS — это только одна из возможных угроз.) А построение системы защиты, которая сможет эффективно противостоять таким атакам, обойдется в десятки раз дороже. Нередки случаи воровства клиентских баз или мошенничества в отношении онлайн-сервисов банков.

В настоящее время в России сложился целый рынок мошеннических операций, оборот которого соперничает с оборотом крупных ИТ-компаний. Средний банк теряет со счётов клиентов около 100 млн рублей в год. По данным Group-IB, в сфере дистанционного банковского обслуживания (ДБО) за 2011 год в России мошенники «заработали» более 900 млн долларов. В 2012-м страна вышла на первое место в Европе по росту мошенничества с банковскими картами — таковы недавние данные исследования компании FICO. Согласно статистике Euromonitor International, на Россию пришлось 6% потерь от мошеннических операций с банковскими картами, что в абсолютных величинах означает сумму в 91,4 млн евро. За прошлый год рост составил 35% по сравнению с 2011-м. При этом в 2006 году потери российских банкиров составляли не более 2% от общеевропейских (12,6 млн евро), а теперь, как сообщается в отчёте, они больше, чем в Германии, и приблизились к испанским.

По словам Ольги Корнеевой, директора по маркетингу процессингового центра PayOnline, Россия — одна из двух наиболее активно развивающихся зон мира по приросту количества платежей по банковским картам в интернете. «А за ростом популярности карт среди населения следует рост объема мошеннических операций по ним, — отмечает Ольга Корнеева. — С 2006 по 2011 год их доля в общем объеме платежей по картам в интернете увеличилась на 50% и приблизилась к общемировому однопроцентному уровню».

За ростом популярности карт среди населения следует рост объема мошеннических операций по ним

Россия далеко не единственная страна, в которой заметно активизируется мошенничество, связанное с банковскими транзакциями и персональной информацией. Так, в Великобритании в 2011 году оно увеличилось на 35 и 58% соответственно (UK's Fraud Prevention Service report). По мере роста технической оснащенности и подготовленности хакеров финансовым организациям необходимо постоянно улучшать свои стратегии защиты данных. «Для компаний, которые пренебрегают аспектами безопасности и в результате подвергают своих клиентов неоправданным рискам, трудно найти оправдание, тем более что сейчас есть известные стратегии и решения, которые доказали свою эффективность в этой области», — считает Сергей Кузнецов, генеральный директор SafeNet в России и СНГ.

Новый сегмент «бизнеса»

Это самый настоящий бизнес, с чёткой иерархией: как и на любом обычном предприятии, здесь имеются отделы кадров, должностные обязанности, план продаж и даже «первый отдел», обеспечивающий строгую конфиденциальность. У этой экосистемы есть свои дилеры, своя партнерская сеть… Такая иерархия строится на ясном разделении ответственности и обязанностей. Благодаря научной организации труда теневые компании работают чрезвычайно эффективно.

Четкое разделение ответственности и позволяет построить весьма действенную экосистему, бороться с которой чрезвычайно сложно. Поэтому банку необходимо не только уметь устанавливать факт мошенничества, но также своевременно и правильно реагировать на инцидент: например, перекрыть доступ к сетям, которые были поражены, заблокировать карточки с украденными номерами и т. д. Эта процедурная часть имеет большое значение.

Безопасность приема онлайн-платежей по банковским картам в России обеспечивается профессиональными организациями: банками, IPSP и агрегаторами платежей

Мошенничество в банках возникло не столь давно, и связано оно с тем, что кредитные учреждения начали использовать технологии для создания новых сервисов. А последние оказались уязвимы для мошенничества: ведь обычно сначала запускается сервис, а его безопасность в полной мере обеспечивается уже потом.

«Безопасность приема онлайн-платежей по банковским картам в России обеспечивается профессиональными организациями: банками, IPSP и агрегаторами платежей, — комментирует Ольга Корнеева. — Они проходят сертификации на соответствие требованиям международных платежных систем — и только после этого получают право на обработку платежных данных владельцев карт. Используемые ими технологии соответствуют мировым стандартам, однако одними технологиями рост мошенничества в рунете не остановить».

http://www.computerra.ru/74214/bezopasnost-onlayn-platezhey/

11.07.2013

Россияне все чаще становятся жертвами киберпреступников

Чем больше население пользуется различного рода финансовыми инструментами, тем активнее мошенники пытаются воспользоваться этим в своих целях. Особенно наглядно такая тенденция проявляется в секторе пластиковых карт, где с каждым годом положение становится все тревожнее.

Реальной объективной статистики количества киберпреступлений, в том числе связанных с платежными картами, нет. Правда, в последнее время Центральный банк, который занимается регулированием этого рынка, понял необходимость мониторинга ситуации. Принято решение о начале формирования такой статистики. Существует также Ассоциация российских членов Европей (АРЧЕ), которая в различных формах дает информацию о киберпреступлениях, в том числе в сфере платежных карт. По данным организации, объем мошеннических операций в России в 2012 году составил примерно 2,5 млрд. долларов, а в целом по миру – примерно 13 млрд. долл. Таким образом, доля России довольно значительна – около 20 %.

Как считает депутат Госдумы, президент Ассоциации региональных банков России Анатолий Аксаков, это не может не внушать обеспокоенность. Равно как и то, что в 2012 г. число преступлений в этой сфере, по данным АРЧЕ, возросло в России примерно на 60 %. Хотя, возможно, и больше, так как банки, как правило, стараются об этом не говорить.

Между тем, можно прогнозировать дальнейшие рост мошенничества в этой сфере, так как растет число карт. При общем росте рынка розничных кредитований в 2012 году на 40 %, количество кредитов, выданных с помощью карт, составило 75 %. То есть основным драйвером розничного кредитования явился именно этот продукт.

Преступления, связанные с использованием пластиковых карт, квалифицируются как кражи. Чтобы совершать их, преступникам в первую очередь необходимо получить данные пластиковых карт. На Западе это достигается путем взлома крупных платежных систем, баз данных банков или страховых компаний. После этого сведения поступают на «черный» рынок, где их приобретают злоумышленники.

В нашей стране ситуация обстоит немного по-другому, уточняет начальник отдела главного управления экономической безопасности и противодействия коррупции МВД РФ Роман Романов.

Получение информации о картах клиентов в основном происходит путем установки на банкоматы так называемых скиминговых устройств. Далее изготавливаются поддельные банковские карты и уже по ним похищаются деньги.

В МВД преступления учитываются в соответствии со статьями Уголовного кодекса РФ. Те, что связаны с банковскими картами, проходят как мошенничество или кража, в зависимости от ситуации. Как самостоятельные преступления они в полицейской статистике не отражаются. Раскрытие подобных дел требует широкого спектра оперативно-розыскных мероприятий и, как следствие, много времени.

Владимир ГУРВИЧ

Источник: novopol.ru

http://www.ecolife.ru/infos/news3/16085/

11.07.2013

В Адыгее полицией раскрыто мошенничество, совершенное с использованием сети Интернет

Полицией Майкопского района возбуждено уголовное дело в отношении 27-летнего местного жителя по факту мошеннических действий.

В органы внутренних дел обратилась 61-летняя жительница Майкопа. По словам женщины, неустановленное лицо оформило на ее имя кредит в сумме 60 тысяч рублей. Она также пояснила, что получила уведомление о том, что просрочена оплата кредитного платежа.

В ходе специальных оперативных и технических мероприятий сотрудники полиции установили, что данный кредит был оформлен посредством сети Интернет.

В дальнейшем выяснилось, что на территории района располагается магазин климатического оборудования. Для удобства клиентов, предоставив необходимый комплект документов, на месте можно приобрести товар в кредит.

У хозяина торговой точки был заключен договор с одним из банков в Москве. Через сеть Интернет он направлял заявку в службу безопасности банка. После необходимой проверки документов оформлялся кредитный договор.

Оперативники также выяснили, что хозяину торговой точки часто помогает его сын. Молодой человек имеет доступ и к офисной технике.

Оказалось, что ранее он работал в нескольких торговых центрах. С прошлого места работы у него осталась ксерокопия паспорта заявительницы.

Используя эти данные, он составил фиктивный договор и оформил кредит на ее имя. Злоумышленник даже внес первый взнос, чтобы скрыть данный факт.

Мошенничество выявилось только после того, как женщина получила уведомление.

У полицейских есть основания полагать, что это ни единственный факт преступной деятельности подозреваемого.

Пресс-служба МВД по Республике Адыгея

http://mvd.ru/news/item/1095911/

12.07.2013

ГИБДД по Мурманской области предостерегает от использования неофициальных сервисов проверки и уплаты штрафов

Госавтоинспекция еще раз предостерегает граждан от использования неофициальных Интернет-сайтов, предоставляющих сервисы по проверке и уплате административных штрафов за нарушения ПДД, и настоятельно рекомендует использовать только официальные ресурсы.

Это связано с тем, что в последнее время гражданам все чаще поступают предложения проверить и уплатить свои административные штрафы на иных Интернет-ресурсах, не являющихся официальными. Так, некоторые мошеннические сайты под видом сервисов проверки штрафов предлагают узнать с их помощью информацию о якобы неуплаченных штрафах за нарушения ПДД и сразу же уплатить их через Интернет. При этом сведения о совершенных гражданином нарушениях, публикуемые в таких сервисах, являются, как правило, вымышленными, а в случае уплаты через подобный сайт штрафа деньги и данные кредитных карт граждан попадают в руки злоумышленников.

Официальными ресурсами, предоставляющими возможность как проверить, так и уплатить административные штрафы за нарушения ПДД, являются Интернет-сайт Госавтоинспекции МВД России (http://www.gibdd.ru), Единый портал государственных и муниципальных услуг (http://www.gosuslugi.ru).

http://www.hibiny.com/news/archive/45538/

15.07.2013

В Санкт-Петербурге направлено в суд уголовное дело о кражах денежных средств с банковских карт

Прокуратура г. Санкт-Петербурга утвердила обвинительное заключение по уголовному делу в отношении Кирилла Жбанова и Дмитрия Ивлева. Они обвиняются в совершении преступлений, предусмотренных п.п. «а», «в», ч. 2 ст. 158 УК РФ (кража группой лиц по предварительному сговору с причинением значительного ущерба гражданину). Кроме того, Жбанову инкриминируется п. «в» ч. 3 ст. 158 УК РФ (кража, совершенная в крупном размере).

По версии следствия, обвиняемые приобрели устройства, предназначенные для списания денежных средств с электронных карточных счетов в банковских учреждениях (POS-терминалы). В их конструкцию они внесли изменения, после которых совершать такие операции стало невозможным.

Эти устройства злоумышленники устанавливали в различных местах торговли в Санкт-Петербурге – в магазинах, ресторанах быстрого обслуживания и АЗС. После провода банковских карт через данные терминалы они накапливали в себе информацию о номерах и ПИН-кодах, которая передавалась на мобильные телефоны обвиняемых. Получив эти сведения, сообщники изготавливали дубликаты банковских карт, которые использовали в банкоматах различных банков города, снимая денежные средства с карточных счетов без ведома их владельцев.

Всего с 3 по 27 февраля 2012 года Жбанов и Ивлев похитили 849 тыс. рублей, принадлежащих 13 потерпевшим.

http://genproc.gov.ru/smi/news/archive/news-83636/

22.07.2013

Карты, деньги, отпечатки пальцев

Жертвой мошенников, промышляющих незаконным выводом денег с карт, сегодня может стать любой владелец банковской кредитки

Михаил Хмелев
shutterstock.com
НОМЕР: Профиль 822

Несмотря на все новые средства защиты банковских карточек, мошенники по-прежнему похищают миллиарды рублей ежегодно.

«Я едва полностью не поседел за тот месяц, пока банк решал, кто виноват в том, что пропали все деньги с моей «пенсионной» карты, и возвращать ли мне накопленные за полгода сбережения», — рассказывает один из пострадавших от действий карточных мошенников, человек пенсионного возраста, ни разу за последние годы не бывавший за границей и даже не подозревающий о возможности оплачивать картой покупки в Интернете. Жертвой мошенников, промышляющих незаконным выводом денег с карт, сегодня может стать любой владелец банковской кредитки. Это только кажется, что ваша зарплатная карта в полной безопасности, если вы лишь снимаете с нее наличные в ближайшем банкомате. Вы можете не ездить за границу, соблюдать все возможные меры предосторожности, совершая покупки в интернет-магазинах, но риск компрометации вашей банковской карты и пропажи хранящихся на ней денежных средств остается.

Никаких высоких технологий для кражи денег с карты не требуется. Карта нашего собеседника была «скомпрометирована» в результате снятия наличных в обычном банкомате. И не где-нибудь в экзотической стране, а в одном из спальных районов столицы. Злоумышленники действовали по старинке, давно известным способом.

Именно «старый добрый» скимминг Александр Кузнецов, руководитель блока «Риски и безопасность» компании UCS, считает главной угрозой для обладателей пластиковых карт. «Снимаете ли вы наличные в банкомате или расплачиваетесь кредиткой в супермаркете, вы проделываете одно и то же: прокатываете свою карту через специальное считывающее устройство, — рассказывает эксперт. — В каждом банкомате и платежном терминале есть устройство для чтения данных с магнитной полосы на обратной стороне кредитки. Ровно такой же считыватель преступники размещают снаружи банкомата — в компактной накладке из пластика. На языке мошенников он называется «скиммер». Его почти не отличить от «родных» деталей банкомата». Считав данные с карты, как в случае с нашим пенсионером, мошенникам остается лишь узнать ПИН-код к вашей карте. Сделать это можно с помощью накладки на клавиатуру, портативной видеокамеры или банального подглядывания. После того как мошенникам стали известны секретный код и данные карты, им не составит труда изготовить ее копию на «белом» пластике и снять с нее деньги в любом банкомате.

Технология скимминга, бывшая для нашей страны экзотикой еще несколько лет назад, сегодня в России очень распространена. По данным компании FICO, наша страна вышла на первое место в Европе по темпам роста объемов «фрода» (мошенничество с банковскими картами и платежными сервисами) — в 2012 году прирост составил более 35%. На Россию теперь приходится более 6% от его общего объема, что в абсолютных показателях в прошлом году превысило $91 млн. Впору бить тревогу, но представители банковского сообщества призывают не драматизировать ситуацию. «Уровень фрода остается в традиционных рамках по отношению к общему объему транзакций с банковскими картами на протяжении многих лет, — уверяет Тимур Аитов, вице-президент НП НПС. — Объемы «карточных» потерь в результате действий мошенников составляют порядка 10 б.п. (0,1%) от объема транзакций в сети торгово-сервисных предприятий и 1—2 б.п. (0,01—0,02%) — в банкоматах. При этом в России уровень фрода по-прежнему ниже, чем в большинстве развитых стран, поскольку карты россиян не так привлекательны для мошенников, как «пластик» западных потребителей». По данным процессинговой компании UCS, по уровню проникновения мошенничества в банковской сфере Россия все еще недотягивает до остального мира — отношение потерь к общему объему операций по картам у нас в 4 раза ниже. Но по мере роста числа банковских карт в России и увеличения числа операций по ним мы уверенно догоняем развитые страны.

http://www.profile.ru/article/karty-dengi-otpechatki-paltsev-76686

25.07.2013

В Чувашии задержаны подозреваемые в совершении мошенничества с использованием электронно-считывающего устройства

В июле в Чебоксарах в терминале одного из банков двое мужчин установили считывающий аппарат - скиммер. С помощью устройства они получили информацию о персональных данных и пин-кодах электронных карт оплаты граждан. Об этом стало известно службе безопасности банка, сотрудники которой обратились в полицию. Камера видеонаблюдения, установленная в помещении банкомата, четко зафиксировала лица злоумышленников.

Пресс-служба МВД по Чувашской Республике

http://mvd.ru/news/item/1117517/

26.07.2013

Новый выпуск проекта «Финансовая грамотность» банка УРАЛСИБ посвящен кредитным картам

Представлены новые выпуски совместного проекта Банка УРАЛСИБ и ИД «Комсомольская правда» «Финансовая грамотность», направленного на экспертную поддержку и финансовое просвещение граждан.

Вопросы читателей о применении различных банковских продуктов и услуг в газете «Комсомольская правда» комментируют эксперты Банка УРАЛСИБ.

Карточные продукты, которым посвящена тема очередного выпуска, являются важной составляющей розничного сегмента Банка УРАЛСИБ. По просьбам читателей начальник управления маркетинга Банка УРАЛСИБ Сергей Бреусенков объяснил, в каком случае лучше получить потребительский кредит, а в каком – кредитную карту. Также эксперт рассказал о дополнительных возможностях погашения задолженности по кредитной карте: дистанционно через систему УРАЛСИБ | Интернет-банк, или при наличии зарплатного счета в другом банке – безналичным переводом в УРАЛСИБ через интернет-банк другого банка. Интерес читателей вызвала и совместная программа с авиакомпанией «Аэрофлот» «Аэрофлот-бонус», позволяющая при расчетах по дебетовой или кредитной карте получать мили, которые можно выгодно обменять на авиабилеты «Аэрофлота» и авиакомпаний альянса Sky Team (Скай Тим), а также на услуги компаний–партнеров программы.

Одно из наиболее динамично развивающихся направлений розничного бизнеса Банка УРАЛСИБ – автокредитование. Комментируя вопросы читателей, главный эксперт дирекции поддержки банковского бизнеса Банка УРАЛСИБ Дмитрий Семенов рассказал, что УРАЛСИБ предлагает на выбор несколько программ автокредитования с максимальной суммой кредита 3 млн рублей, на срок до 5 лет. Ставка по кредиту зависит от срока кредита, размера первоначального взноса и от выбранной кредитной программы. На приобретение автомобилей марок: Audi, Volkswagen, Skoda, Hyundai, Lifan, Chery, Lada предусмотрены специальные программы кредитования со сниженными процентными ставками в рублях РФ. В случае выбора автомобиля другого производителя можно воспользоваться кредитом на автомобиль по стандартной программе Банка. Читатели также узнали об услуге «Trade-in», в рамках которой стоимость взятого в кредит автомобиля зачитывается при покупке нового автомобиля в автосалоне.

Источник: ОАО «УРАЛСИБ»

http://bankir.ru/novosti/s/novyi-vypusk-proekta-finansovaya-gramotnost-banka-uralsib-posvyashchen-kreditnym-kartam-10051050/#ixzz2asnZ4juv

26.07.2013

«Щит и меч» для карты

Уровень мошенничества в области безналичных платежей в России невысок, но система безопасности компании Visa продолжит совершенствоваться.

// Наталия Трушина, Bankir.Ru

Вопрос безопасности платежей по пластиковым картам является актуальным не только для банков, но и для российского общества в целом. Стимулирование безналичных расчетов со стороны государства и все большее проникновение возможностей дистанционного банковского обслуживания (ДБО) в регионы усиливает интерес к проблеме. О ситуации с уровнем интеллектуальной преступности в России, успехами платежных систем в борьбе на «невидимом фронте» и важности личной бдительности пользователей «пластика» шла речь на тематическом пресс-завтраке компании Visa, который состоялся 24 июля 2013 года.

Защищенная безналичной невинностью

На мероприятии присутствовали глава департамента управления рисками Visa по России, странам СНГ и Юго-Восточной Европы **Олег Скородумов** и директор по управлению рисками Visa в России **Дмитрий Дмитриев**. Однако представил журналистам результаты исследований и давал ответы на вопросы только Олег Скородумов. Он поделился сразу несколькими хорошими новостями, касающимися безопасности безналичных платежей. Первая из них заключалась в том, что мошенничество по картам Visa в мире стабильно снижается. Сейчас показатели находятся в области исторического минимума. Компания Visa очень много инвестирует в инновационные решения для усиления безопасности платежей. Речь идет и об использовании чиповых карт, и применении технологии «Verified by Visa» на платформе 3D Secure, и внедрении некоторых новых систем обнаружения мошеннических транзакций и т.д. Благодаря всесторонним усилиям в компании Visa фрод (от английского «fraud**»** — мошенничество в области информационных технологий) был снижен на две трети за последние двадцать лет.

Вторая хорошая новость заключалась в том, что уровень мошенничества в России в 10 раз ниже, чем в мире. Воровство по безналичным платежам сегодня в нашей стране равно 5 копейкам на каждую 1 тыс. рублей. Чтобы понять, много это или мало, Олег Скородумов обратился к результатам исследования объема «потерянных» или «забытых» денег в России на одного гражданина страны. В данной работе, проведенной специально по заказу компании Visa, было определенно количество денег, которое течение года забывается, разбрасывается в виде мелочи при наличном обороте и т.д. Как оказалось, один россиянин теряет, таким образом, в среднем $137 в год, что равно 4 тыс. рублей. Если сопоставить с 5 копейками «уеденными» мошенниками с карты на каждую 1 тыс. рублей, то выйдет, что на каждые 50 тыс. рублей потраченных ежемесячно по карте Visa приходится в год только 30 рублей преступных транзакций в России. Даже при всех погрешностях вычислений выходит, что теряет или забывает при наличном обороте в год среднестатистический россиянин более чем в десять раз больше денег.

Но несмотря на то, что проблема кибермошенничества с пластиковыми картами по масштабу гораздо меньше, чем «проблема забытых денег», эксперты компании Visa считают, что она все равно требует решения, и не оставляют данную область без своего внимания. Специалисты компании Visa выделяют четыре основных типа мошенничества с пластиковыми картами. Первый из них – скимминг. Это вид мошенничества, при котором данные карты считываются любым способом: через банкомат или в торговой точке и т.д. Далее изготовляется поддельная карта – точная копия оригинальной, по которой уже проводятся мошеннические транзакции. Вторым видом является мошенничество через Интернет, когда через всемирную сеть похищаются данные карты, необходимые для проведения транзакций, мошенники покупают по этим данным какие-либо ценности или выводят деньги любым другим способом. Следующий тип мошенничества предполагает работу с украденными или найденными пластиковыми картами. Он отличается от первого вида тем, что дубликат карты не изготавливается, а мошеннические транзакции происходят с оригинала. А последний, четвертый тип мошенничества – это так называемая социальная инженерия. Злоумышленники напрямую воздействуют на держателя карты, побуждая его самостоятельно произвести транзакции в его пользу.

Слоеный пирог безопасности

Предупрежден – значит вооружен

Непростые ответы

Биометрия всем поможет

История с географией

Регулятор возьмет под контроль

Начальник отдела безопасности банковских карт ОТП Банка **Андрей Леонтьев** напомнил, что данные об уровне мошенничества с пластиковыми картами по России в скором времени появятся в ЦБ РФ. Как известно, все российские банки будут обязаны предоставлять регулятору информацию о случаях мошенничества по картам своих клиентов с разбивкой по типам фрода. Если говорить о показателях ОТП Банка, то параметр «fraud/turnover», который используется платежными системами как показатель уровня карточного фрода, во 2-м квартале этого года составил 0,02%, в то время как по Европе за тот же период он был в среднем 0,055%, а по миру 0,073%. «Предположу, что общий уровень фрода в нашей стране ниже, чем в мире, – заявил Андрей Леонтьев. – Конечно, это в какой-то степени связано с недостаточным уровнем развития сети обслуживания карт».

Количество мошеннических операций с картами будет увеличиваться, уверен банкир. Это связано, во-первых, с увеличением объема карт, эмитируемых банками. Во-вторых, с ростом количества различных интернет-сервисов и мобильных приложений, позволяющих выводить денежные средства с карточных счетов. В-третьих, с повышением уровня технической грамотности мошенников и, параллельно с этим, довольно низкой финансовой грамотностью (в части использования карт) населения.

http://bankir.ru/novosti/s/shchit-i-mech-dlya-karty-10051120/#ixzz2asnFYRLn

29.07.2013

Банковские карты в России стали "золотым дном" для мошенников

"Коммерсантъ FM", 29.07.2013

По итогам 2012 года число махинаций с банковскими картами увеличилось на треть и продолжает расти, говорится в отчете компании FICO. Подавляющее большинство мошеннических операций происходит при участии сотрудников банков, уверены эксперты.

Число преступлений с банковскими картами в России за год выросло на треть. Об этом свидетельствуют результаты исследования американской компании FICO. По их данным, убытки от мошеннических операций с банковскими картами выросли в прошлом году на 35% и продолжают увеличиваться. Ежегодный прирост рынка банковских карт, по данным Центробанка, составляет 40%.

По прогнозам специалистов Центробанка, объем операций, совершенных в России с использованием платежных карт, достигнет в 2013 году 30 трлн руб., что на 25% больше уровня 2012 года.

Сейчас доля безналичных операций более 22%, и она растет. Российский карточный рынок развивается колоссальными темпами. По данным Центробанка, на 1 января 2013 года количество карт, открытых в российских банках, составило 240 млн штук, из них активны 75%.

Несмотря на участившиеся случаи мошенничества с банковскими картами клиенты банков защищены законом в достаточной степени, пояснил председатель совета директоров компании QIWI Борис Ким.

"Закон о национальной платежной системе, который был принят в прошлом году и вступил в действие, предполагает так называемый принцип нулевой ответственности потребителя. Это означает, что если с вашей картой была произведена какая-то мошенническая операция, то не вы должны доказывать ее мошеннический характер. Вам достаточно для этого подать заявление в банк, который эмитировал вашу карту, а банк должен доказывать, что эта операция была немошеннической, поэтому тут смело нужно отстаивать свои права", — уверен Ким.

Зачастую в мошеннических схемах с картами задействованы сотрудники банков, считает лидер незарегистрированной партии защиты заемщиков "Кредитная амнистия" Михаил Козлов.

Анастасия Кузнецова

http://www.kommersant.ru/doc/2243869

29.07.2013

У мошенников много фокусов с банковскими картами

Россиянам советуют быть бдительными и финансово грамотными

Анастасия Башкатова

Банкомат может таить в себе много опасностей для владельцев пластиковых карт. Фото Айгуль Юсуповой

Платежи с использованием банковских карт набирают в России оборот. Ежегодный прирост рынка, по данным Центробанка, составляет 40%. Представители платежных систем добавляют, что уровень мошенничества с карточками в РФ в 10 раз ниже, чем в мире. Хотя, по

данным иностранных аналитиков, убытки России от мошеннических операций с банковскими картами растут самыми быстрыми в мире темпами – на 35% в 2012 году. Банкиры советуют гражданам быть более бдительными, ведь в России распространены самые разные виды мошенничества.

За одну только прошлую неделю в Подмосковье и Чувашии были задержаны несколько правонарушителей, которые пытались снять с чужих карт деньги с помощью специального считывающего устройства, устанавливаемого на банкомат. Также из регионов поступали новости о незаконном снятии крупных сумм с украденных карт, о вымогательстве с граждан денег за разблокировку якобы заблокированных карт и т.д. Мошенничество с банковскими картами в России очень распространено.

Одновременно с этим Центробанк хвалится растущей популярностью банковских карт. По прогнозам начальника управления департамента регулирования расчетов ЦБ Вадима Кузнецова, объем операций, совершенных в РФ с использованием платежных карт, достигнет в 2013 году 30 трлн. руб., что на 25% больше уровня 2012-го. «Сейчас доля безналичных операций более 22%, и она растет. Российский карточный рынок развивается колоссальными темпами: почти 40% ежегодного прироста», – добавляет Кузнецов. По данным ЦБ на 1 января 2013 года, количество карт, эмитированных российскими банками, составило 240 млн. шт., из них активны 75%.

Представители платежных систем тоже рапортуют об успехах. По данным компании Visa, уровень мошенничества в России в 10 раз ниже, чем в мире. Как пояснил глава департамента управления рисками Visa по России, странам СНГ и Юго-Восточной Европы Олег Скородумов, на каждые 50 тыс. руб., потраченных ежемесячно по карте Visa, в год приходится 30 руб. мошеннических транзакций в России.

Согласно проведенным весной этого года опросам Национального агентства финансовых исследований, 74% россиян – держателей карт никогда не сталкивались с мошенничеством с банковскими картами, 26% соответственно сталкивались. Тот же показатель распространенности мошенничества демонстрируют Канада и Сингапур. Один из самых низких показателей в Швеции – 12%, а высоких – в США: более 40%. Между тем, по данным американской компании FICO, ситуация в России не так уж благополучна: убытки РФ от мошеннических операций с банковскими картами растут самыми быстрыми в мире темпами. В 2012 году рост на 35% к 2011-му.

http://www.ng.ru/economics/2013-07-29/5_platezhi.html

На тему:

30.07.2013

Мошенники придумали новые фокусы с банковскими картами

"Коммерсантъ FM", 29.07.2013

http://www.19rus.info/news/108972.html

30.07.2013

Хакеры против банков

Насколько безопасно пользоваться банковскими карточками?

Евгения Кузнецова

Участившиеся в последнее время хакерские атаки на банки по всему миру заставляют особо мнительных пользователей банковских карт хранить свои сбережения в наличных. Последней каплей для многих из них стала громкая история с похищением 160 миллионов номеров кредитных и дебетовых карт российскими и украинскими хакерами.

Федеральная прокуратура Южного округа Нью-Йорка представила обвинения двум россиянам – 26-летнему Александру Калинину и 31-летнему Николаю Насенкову, которым, в случае признания виновными, грозит до 30 лет заключения. Федеральный прокурор штата Нью-Джерси Пол Фишман назвал мошенничество, совершенное россиянами, крупнейшей раскрытой схемой по взлому и воровству данных, которое когда-либо случалось в США.

Никто не защищен?

«Полная безопасность в этом деле практически недостижима, – заявил в беседе с корреспондентом «Голоса Америки» российский хакер, пожелавший остаться неизвестным. – Вспомните случаи с воровством 45 миллионов долларов в мае этого года, или историю с Group-IB. Систему можно обновлять бесконечно, но “дырочки” в ней всегда найдутся».

По словам анонима, методики хакерских взломов развиваются быстрее «неуклюжего и неповоротливого зверя информационной безопасности», благодаря чему компьютерным преступникам со всего мира и удается регулярно «чистить» банки и финансовые корпорации.

Отвечая на вопрос корреспондента «Голоса Америки», аноним также отметил, что сам бы не посоветовал пользователям банковских карт хранить на них деньги и совершать безналичные расчеты, так как именно тогда средства «наиболее уязвимы». «Лучше уж старые проверенные стеклянные банки», – в шутку добавил он.

Абсолютная безопасность

Среди специалистов по информационной безопасности – бытует мнение о том, что создать абсолютную информационную защиту можно, однако это будет чрезвычайно затратно. Об этом в комментарии «Голосу Америки» рассказал ведущий эксперт по информационной безопасности компании InfoWatch Андрей Прозоров.

«Говоря о защите информации, стоит понимать необходимость баланса: удобство использования информации, стоимость средств защиты и надежность системы защиты, – констатировал он. – Абсолютная защита будет стоить дорого, да и удобство пользователя информационных систем и информации при этом будет минимальным».

По словам эксперта, обычно специалисты по информационной безопасности говорят о рисках и управляют ими путем принятия риска, снижения риска, передачи риска или избегания угроз.Как и анонимный хакер, Прозоров отметил опасность безналичных расчетов и заявил, что в последнее время из-за их возросшей популярность опасность кибератак также повысилась.

Аналогичные преступления не редкость в последнее время. «С учетом роста популярности безналичного расчета (в частности, использования пластиковых карт), мы можем с уверенностью утверждать, что количество преступлений и размер ущерба будет только расти», – пессимистично отметил он.

Другой проблемой борьбы с киберпреступлениями эксперт назвал сложности с задержанием хакеров. «В современную эпоху открытых цифровых границ сложно не только выявить преступников, доказать их причастность, но и физически задержать их, – пояснил он. – Государствам следует договариваться о сотрудничестве и помогать друг другу в расследовании инцидентов и преследовании злоумышленников».

Статьи по теме

Российские хакеры обвиняются в «одном из крупнейших хищений информации»
Хакеры США намерены обдумать отношения с властями
США и Китай обсуждают вопросы кибербезопасности
Украинские хакеры обвиняются в хищении 15 миллионов долларов в США
Кибератаки, торговля, Северная Корея станут главными темами китайско-американского саммита
Китай проведет военные кибер-учения
«Электронный Робин Гуд» сознался во взломе компьютеров «Стратфор»
Китай подозревают в хищении военных секретов США
Взрыв на полигоне с 18 миллионами снарядов
http://www.golos-ameriki.ru/content/hacker-comp/1713055.html

За рубежом

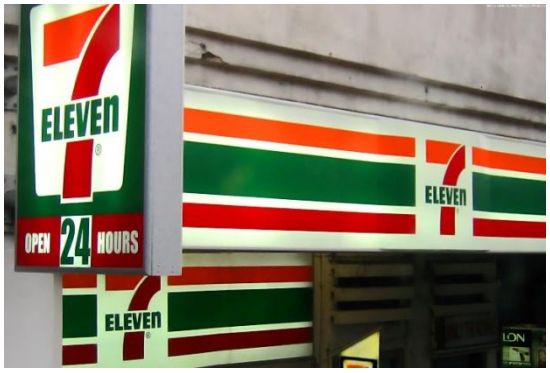
30.07.2013

Хакер и рынок: как вполне уже «обыденное» похищение реквизитов кредитных карт может повлиять на глобальные финансы

Автор: Михаил Ваннах

Русский хакер — это бренд. Почти такой же, как русская водка. Но если с прозрачной очищенной борются нынче по миру активисты ЛГБТ-сообщества, недовольные течением отечественного законодательного процесса (и с удивлением выясняющие в этой борьбе, что самые известные сорта популярного напитка принадлежат отнюдь не русским), то хакерам противостоят федеральные правоохранители США, поддержанные полицией стран Европы. Которая также выясняет вещи, новые для неё, но куда более интересные и важные для всех. Об одном из таких «открытий чудных» поведала The Christian Science Monitor.

От русских хакеров не уберегли даже глобальные самураи из «7-Одиннадцать».



О том, как компания на редкость терпеливых «русских хакеров» влезла аж в системы NASDAQ, «Компьютерра» уже рассказала. Но это — «элитная» часть работы. А команда эта — как минимум по одному члену — пересекается с интернациональным, русско-украинским коллективом, который с августа 2005 по июль 2012 года совершил крупнейшее хакерское хищение в истории. Он похитил номера 160 миллионов кредитных карт! Четыре русских и один украинец утащили кредиток больше, чем составляет численность взрослого населения России и Украины.

Прокурор штата Нью-Джерси Пол Фишман поражен масштабом деятельности хакеров.

Приводятся только потери финансовых учреждений — таких известных, как 7-Eleven, JCPenney, JetBlue и Dow Jones: они составляют 300

миллионов долларов. Суммы, потерянные держателями украденных карт, не называются. Схема хищения была «проста, как Колумбово яйцо». Украденные данные оптом сбывались преступникам по всему миру. Те наносили их на чистые карты и воровали уже непосредственно, снимая наличность в банкоматах. Примитивно и действенно.

Федеральный прокурор Манхэттена Прита Бхарар всегда интересовался сложными экономическими схемами.

Но какое воздействие может оказать деятельность хакеров на рынок? Рынок в целом. Именно таким вопросом задался федеральный прокурор Манхэттена Прита Бхарар, традиционно специализирующийся на раскрытии финансовых преступлений, которые совершаются с использованием сложных экономических схем. Он считает, что представленные обвинения говорят о возможностях киберпреступников наживаться уже не на кражах с отдельных банковских счетов, а на финансовой системе в целом… Разберемся же в том, как такие потенции возникают.

Итак, первое, на что стоит обратить внимание, — это отсутствие данных о суммах денег, пропавших у держателей кредитных карт. Тут может быть несколько версий. Первая — оптимистическая. То, что всем-всем пострадавшим сети розничной торговли ущерб полностью компенсировали, и тогда вред от хакерской деятельности укладывается в приведённые 300 миллионов долларов. В пересчёте на одну кредитку — менее двух зелёных. Совокупно суммы весьма внушительные, но в среднем — эквиваленты стоимости нескольких электронных транзакций. Или мелочи, которую вы или не взяли со сдачи либо потеряли из-за отсутствия отделения для неё в кошельке. Если так, то речь идёт лишь о некотором увеличении суммы издержек денежного обращения.

Но, может быть, дела обстоят много хуже. И тогда поименованные 300 миллионов долларов — всего лишь видимая часть айсберга. А потери конкретных людей не учтены или учтены в незначительной степени.

http://www.computerra.ru/77226/haker-i-ryinok-kak-vpolne-uzhe-obyidennoe-pohishhenie-rekvizitov-kreditnyih-kart-mozhet-povliyat-na-globalnyie-finansyi/

Беларусь

12.07.2013

Проверка штрафов в интернет: как не попасть в руки мошенников

Павлюк Быковский, Deutsche Welle

МВД Беларуси запустило сетевой сервис для проверки наличия штрафов за превышение скорости. DW выяснила, какие опасности для махинаций таит в себе этот сервис, и как можно оградить себя от посягательств мошенников.

С 9 июля начал работать онлайн-сервис белорусского МВД, с помощью которого автолюбители могут проверить, есть ли у них штраф за превышение скорости. Речь идет об автоматическом фотографировании нарушений правил дорожного движения (ПДД). Оно применяется в Беларуси с июля 2012 года. По действующим правилам МВД должно заказным письмом уведомлять провинившегося владельца автомобиля о наложении на него штрафа (от 50 до 300 тысяч белорусских рублей или от 4 до 25 евро в пересчете). Владелец машины может оспорить наложение штрафа, заявив, что за рулем был кто-то другой.

Мошенники интересуются чужими штрафами

Теперь у МВД появился еще и соответствующий онлайн-сервис. Для получения информации о неуплаченных штрафах на сайте министерства нужно указать фамилию, имя и отчество владельца автомобиля, серию и номер свидетельства о его регистрации. Очевидно, что этот сервис могут взять на вооружение и злоумышленники, если воспользуются базой данных белорусской ГАИ.

Как отмечают наблюдатели, к базе, в которой содержится информация обо всех зарегистрированных в стране автомобилях, помимо сотрудников правоохранительных органов имеет доступ сегодня достаточно широкий круг лиц. Завладев реальной информацией о наличии штрафов за нарушение ПДД владельцами автомобилей, мошенники могут заманить жертву на фальшивый сайт, якобы предназначенный для оплаты штрафов.

В итоге мошенники могут получить либо просто деньги в размере штрафа, либо номера банковских карточек. О том, что такая опасность вполне реальна, свидетельствует опыт России. Российская Госавтоинспекция 10 июля выступила с предостережением граждан от использования неофициальных онлайн-сервисов проверки и оплаты штрафов из-за участившихся случаев мошенничества.

Как определить подлинность сайта

Безопасность при онлайн-платежах

http://udf.by/news/society/83006-proverka-shtrafov-v-internet-kak-ne-popast-v-ruki-moshennikov.html

США

05.07.2013

Российские хакеры обвиняются в «одном из крупнейших хищений информации»

Михаил Гуткин

Кибер-мошенники украли данные о 160 миллионах кредитных карт, взломали биржу Nasdaq

В четверг федеральные прокуроры в Нью-Йорке и Нью-Джерси предъявили обвинения в мошенничестве и взломах компьютерных систем четверым гражданам России и одному украинцу. Жертвами кибермошенников стали более десятка западных компаний, включая торговые сети 7-Eleven, Carrefour SA, JC Penney, авиакомпанию JetBlue, Visa Inc., Citibank, бельгийский банк Dexia. По данным обвинения, потери этих компаний составили в общей сложности сотни миллионов долларов. Один из подозреваемых, Александр Калинин из Санкт-Петербурга, обвиняется также во взломе серверов электронной биржи Nasdaq.

Помимо Калинина, обвинения были предъявлены гражданам России Николаю Насенкову, Роману Котову и Дмитрию Смилянцу из Москвы, а также бизнесмену из Москвы и Сыктывкара Владимиру Динкману и подданому Украины Михаилу Рытикову из Одессы. Как сообщает российское агентство Life News, «Смилянец с 2011 года является основным владельцем киберспортивного проекта “Moscow Five”, команды которого дважды завоевывали бронзовые награды на мировых первенствах Counter-Strike 1.6, League of Legends и DOTA 2».

Первые обвинения были предъявлены еще в 2009 году, но были обнародованы лишь сейчас. Двое обвиняемых – Динкман и Смилянец – были арестованы в июне прошлого года в Нидерландах по запросу США. Смилянец был экстрадирован в США в сентябре прошлого года и должен предстать перед судом в Нью-Джерси на следующей неделе. Решение об экстрадиции Динкмана еще не принято.

Трое других обвиняемых находятся в розыске.

Каждому из обвиняемых в США грозит до 30 лет тюрьмы.

http://sartraccc.ru/i.php?oper=read_file&filename=Press/rushack.htm

15.07.2013

Криптовалютчики под колпаком

Журнал "Коммерсантъ Деньги", №27 (935), 15.07.2013

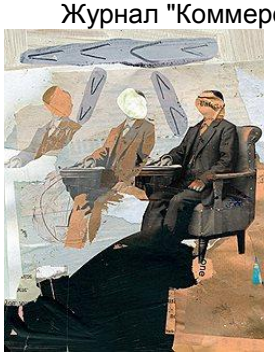


Фото: Леонид Фирсов

В США по обвинению в финансовом мошенничестве и отмывании денег судят создателей Liberty Reserve, одной из крупнейших в мире анонимных платежных систем. Похоже, на очереди — криптовалюта Bitcoin. Борьба с анонимностью в интернете, особенно после разоблачений Эдварда Сноудена, выходит на новый уровень.

Олег Хохлов, Анастасия Демидова

Король Артур

Более 55 млн нелегальных трансакций на сумму $6 млрд — таков впечатляющий итог семи лет работы анонимной платежной системы Liberty Reserve. Ее владелец Артур Будовский с партнерами обвиняются в создании крупнейшего в истории предприятия для отмывания денег. Для сравнения, межправительственная организация FATF (Financial Action Task Force on Money Laundering) оценивает общий объем отмывания денег всеми способами в 2-5% мирового ВВП в год, что составляет примерно $1,38-3,45 трлн (впрочем, ввиду распространенности проблемы FATF не берется оценить, сколько денег на самом деле отмывается через легальные и нелегальные финансовые системы).

В общем, эта история заслуживает экранизации, и фильм должен получиться более динамичным, чем байопик "Социальная сеть", рассказывающий о Марке Цукерберге. Итак, Нью-Йорк, 2006 год. Уроженцы Украины Артур Будовский и его бизнес-партнер Владимир Кац избегают тюремного заключения — власти штата обвиняли их в незаконных денежных операциях и пособничестве отмыванию денег при помощи интернет-сервиса Gold Age, которым они управляли с 2002 года. Зарегистрированный в Панаме Gold Age был одним из крупнейших обменников, который позволял выводить деньги из популярных в начале 2000-х полулегальных платежных систем, таких как E-gold и e-Bullion (комиссия обменника достигала 4%). В обвинительном заключении говорилось, что к моменту разгрома системы Gold Age успел отмыть около $30 млн. Будовского и Каца признали виновными, но за решетку не отправили — оба получили по пять лет условного срока.

Оказавшись на свободе, Будовский отправился в Коста-Рику, где основал новую интернет-компанию — Liberty Reserve. Принцип тот же: полная анонимность (при открытии счета можно было указывать вымышленные данные) и пятипроцентная комиссия за вывод денег из системы.

Американские власти утверждают, что целевой аудиторией Liberty Reserve были главным образом наркодельцы, нелегальные порнографы, кардеры, хакеры, создатели финансовых пирамид, замаскированных под инвестфонды, и их клиенты, а также террористы. В начале июня ФБР сообщило о задержании участников международной преступной группы, лидером которой был вьетнамец Дэй Хэй Труонг. Преступники воровали данные кредитных карт, владельцы которых осуществляли покупки онлайн. Как утверждается в пресс-релизе ФБР, около $200 млн мошенники провели в том числе через Liberty Reserve.

Помимо Liberty Reserve в деле Будовского фигурирует еще ряд организаций, в частности печально известная охранная структура G.E.E.S., фактически личная гвардия владельца системы. Всего в деле семеро обвиняемых: пятеро уже арестованы, двое в бегах. Всем им грозит 25 лет тюрьмы по совокупности обвинений.

http://www.kommersant.ru/doc/2224967

США

26.07.2013

Русские хакеры похитили номера 160 млн кредитных карт, но это еще не самое страшное

Марк Клейтон | The Christian Science Monitor

Группа хакеров, в которую входили четверо россиян и один украинец, с 2005 по 2012 год взламывала компьютеры финансовых учреждений и за 7 лет похитила номера 160 млн кредитных карт и сотни миллионов долларов, передает корреспондент The Christian Science Monitor Марк Клейтон.

От действий киберпреступников пострадали такие компании, как 7-Eleven, JCPenney, JetBlue и Dow Jones, говорится в статье. Один из хакеров также обвиняется в проникновении на серверы биржи NASDAQ. Общие потери финансовых учреждений составили 300 млн долларов, не считая потерь держателей карт, чьи данные были украдены.

Двое участников преступной группы, Владимир Дринкман и Дмитрий Смилянец, были арестованы в Нидерландах в 2012 году, после чего Дринкман был передан властям США. Смилянец в настоящее время ожидает суда об экстрадиции. Трое их подельников остаются на свободе, сообщает автор статьи.

Украденные данные о кредитных картах подельники продавали злоумышленникам со всего мира, которые затем наносили их на чистые пластиковые карты и незаконно снимали средства со счетов потерпевших через банкоматы.

Один из хакеров, Александр Калинин, отдельно обвиняется федеральными властями США в том, что в 2008-2010 годах взламывал серверы биржи NASDAQ и тайно устанавливал на некоторые из них вредоносное программное обеспечение, продолжает журналист. Эти программы затем позволяли Калинину отдавать инфицированным серверам различные команды, "в том числе удалить, изменить или похитить информацию".

Эксперты в области компьютерной безопасности предупреждают, что кража номеров кредиток - это еще не самое худшее, чего можно ожидать от киберпреступников. Вместо простого похищения информации хакеры будущего будут пытаться изменить или использовать ее для влияния на рынки.

Источник: The Christian Science Monitor
http://inopressa.ru/article/26Jul2013/csmonitor/hacker.html

24.07.2013

Киберпреступность наносит ущерб экономике США в $ 140 млрд

Источник: Cybersafetyunit.com

McAfee опубликовал новый доклад в котором озвучены новые данные о годовых потерях экономики США от кибератак.

В докладе говорится, что потери США от киберпреступности составляют от $ 20 млрд до $ 140 млрд, или около 1% от ВВП страны, в результате чего средний бизнес теряет и рабочие места.

Совместные исследование некоммерческого Центра " Center for Strategic and International Studies"(CSIS) и компании McAfee отражают пересмотр более ранней оценки ущерба от киберпреступности компании McAfee в $ 1 трлн, озвученной президентом США Обамой в 2009 году.

http://www.crime-research.ru/news/24.07.2013/7641/

Украина

27.07.2013

О чем умалчивают украинские операторы сотовой связи

То, что продемонстрируют и обсудят на конференции Black Hat, открывающейся в Лас Вегасе 31 июля, как именно хакеры удаленно могли бы использовать сим-карты для совершения финансовых преступлений или электронного шпионажа - заставляет задуматься о недалеком будущем безопасности средств связи миллиардов людей.

На протяжении последних лет на страницах ИА SECURITY публиковались те или иные материалы об уязвимостях сотовых сетей и их компонентов. Пришло время не просто задуматься, все очень серьезно.

Подавляющее число абонентов сотовых сетей уверены, что прослушать их мобильный телефон невозможно. И действительно, если говорить о государственных структурах, то они не имеют права без юридически обоснованной веской причины и без разрешения суда заниматься прослушкой. С этой точки зрения законопослушным гражданам беспокоиться и правда не о чем. Другое дело, когда на сцене появляются до зубов вооруженные «короли криминальной прослушки» или «оборотни в погонах, - поясняет **Анатолий Клепов**, российский ученый, один из ведущих мировых экспертов в области информационной безопасности.

Со стороны разработчиков и поставщиков мобильной связи, а так же операторов сотовых сетей - технологии не стоят на месте, однако, это только визуальных технологический прогресс, обусловленный сменой корпусов, красотой иконок, работой маркетинговых и рекламных корпоративных служб.

Для глобального и качественного перехода к более прогрессивным технологиям, с гарантированной степенью защиты мобильных сетей - это весьма затратный и трудоемкий процесс. Более мобильны, как бы это не тривиально звучало - специалисты противоположного лагеря. Мы не будем углубляться в вопросы, чем именно они "вооружаются" и откуда черпают знания, но участившиеся факты предвещают серьезную угрозу.

Дело в том, что специалисты, называйте их как угодно - хакеры или подпольные кулибины, обладающие определенными знаниями и досконально понимающие суть следующих вопросов:

как создавать акустическую помеху и подавлять сигнал мобильных устройств в любых стандартах GSM, в том числе Wi-Fi и Bluetooth,

как снимать речевую и текстовую информацию с любых мобильных устройств,

как определять местонахождение мобильного устройства в любой точке мира,

как удаленно управлять сим-картой для совершения финансовых преступлений или электронного шпионажа

и так далее...

Специалисты подобного уровня не будут использовать перечисленные возможности для личного промысла. Это не только накладно, но и уголовно наказуемо. Подобные вопросы уязвимостей становились поводом в непосредственном обращении к самим производителям мобильных устройств и к операторам сотовой связи. Но что-то нам подсказывает, что до конца вопросы не только не закрываются, но и увеличиваются с каждым днем.

Технологии устаревают гораздо быстрее, чем происходит амортизация технологических процессов, как следствие, кто-то должен понести убытки и если это не сам производитель, то потребителю ничего не остается, как надеяться на удачу. А как известно, надеяться на удачу глупо. К чему же приводит подобные глупости, изучали наши коллеги.

Виды потерь, в результате нарушения информационной безопасности, соответствую такому вот распределению:

35% крупные финансовые потери;
30% кража интеллектуальной собственности;
30% компрометация бренда и руководства компании;
15% противозаконные операции с данными кредитных карт;
12% судебные разбирательства и возбуждения уголовных дел;
10% существенное падение стоимости акций;
7% раскрытие коммерческих секретов компании.

Но речь сегодня не о том, что эти потери есть и будут находить все новые сегменты уязвимости в информационной безопасности корпоративной ли или частной жизни. Проблема в том, что те самые кулибины уже сейчас становятся вполне легальными коммерсантами. Так же, как на азиатском рынке доступна, на первый взгляд, любительская техника для шпионажа, то почему бы ее не дополнить и иным, не менее востребованным спросом. А спрос есть и он колоссален хотя бы потому, что в мире разные системы шифрования, разные стандарты мобильной телефонии как и сама архитектура построения сетей в целом.

Автор: Александр Коваленко
Источник: http://security.ua
http://security.ua/news/press_centre/index.php?ELEMENT_ID=8641

Номер подписан в свет 08.07.2013