Информационное агентство
«WEB-мониторинг»
Свидетельство ИА № ФС7733219 от 19 сентября 2008 года
Научно-практический электронный журнал

ФИНАНСОВЫЕ ПРАВОНАРУШЕНИЯ И ПРЕСТУПЛЕНИЯ

№ 2 (113) 2016
(выходит с октября 2006 г.)

Полиция информирует: как не стать жертвами мошенников
Фото.с сайта
http://static8.depositphotos.com/1005404/1049/i/950/depositphotos_10499957-Money-security.jpg
См. раздел
«Безопасное ведение бизнеса и домохозяйства»

Издатель
ИП **Фединский Ю.И.**

www.webmonitor.ucoz.ru
www.finprest.ucoz.ru
webmonitor@yandex.ru
тел. 8 985 333 87 59

Москва
2016

Подписку на издания ИА «WEB-мониторинг»

с любого календарного месяца

можно оформить

по электронному каталогу
ИД «Экономическая газета»

Финансовые правонарушения и преступления

Для тех, кому важно знать финансовые закон и формы их нарушения

Подписной индекс **80663э**
Информация здесь

Валюта: регулирование и контроль

Для тех, кто хочет быть в курсе валют: вчера, сегодня и завтра

Подписной индекс **42335э**
Инфорция здесь

Налоговые правонарушения и преступления

Для тех, кто стремится грамотно платить налоги

Подписной индекс **41587э**
Информация здесь

ИД "Экономическая газета"
http://www.arpk.org
тел. (499) 152 88 50

Подписка

на 2016 год

на электронный журнал

Финансовые правонарушения и преступления

Для тех, кому важно знать законы и формы их нарушения

Объединенный каталог «Пресса России»
подписной индекс **80663**

Оглавление

Вниманию читателей!

Строки, выделенные цветом и подчеркнутые,
являются активными гиперссылками.

Пользуйтесь ими
для получения в Интернете
оригиналов публикаций.

Безопасное ведение бизнеса и домохозяйства

21.12.2015

Зачем интернет-банку мониторинг контрагентов

Ольга Стаднийчук менеджер по развитию направления компании СКБ Контур

В 2015 году Альфа-Банк внедрил в свой интернет-банк «Альфа-Бизнес Онлайн» сервис проверки контрагентов. Перед отправкой платежа клиенты банка видят необходимую информацию о своих деловых партнерах и могут сберечь свои средства в случае потенциальной угрозы.

Задача: сделать интернет-банк единым функциональным окном

В 2014–2015 годах в банковских кругах витала идея «единого окна», когда в интернет-банке клиенту должны быть доступны все инструменты для ведения бизнеса: бухгалтерские программы, сервисы отправки отчетности и т. д. В результате на сайтах банков появились спецпредложения партнеров на базе агентских договоров. Клиенты не получили каких-то новых полезных возможностей, а партнеры не расширили объемы сбыта.

Следующим шагом стала интеграция ДБО и веб-бухгалтерий. Но несмотря на простоту идеи, реализация выливалась в пул громоздких мероприятий: диалог с вендорами платформ, бюджетирование разработки, согласование безопасности. Одно из самых главных препятствий состояло в том, что на старте было трудно спрогнозировать монетизацию.

Наибольший успех в этой области мог иметь проект, который бы обеспечивал максимальный синергетический эффект с точки зрения нужной пользователю функциональности и приносил бы банку дополнительный доход. Таким проектом стало внедрение 2015 году в интернет-банк «Альфа-Бизнес Онлайн» сервиса проверки контрагентов от СКБ Контур.

Принципы работы

По данным экспертов, в последний год участились случаи, когда компании получали ущерб от фирм-однодневок и «плохой» дебиторской задолженности. Например, поставщику отправляют аванс, а он уже не может выполнить свои обязательства и не возвращает деньги. Причина потерь в том, что бизнес не владеет актуальной информацией о своих контрагентах. Чтобы компании могли регулярно и быстро проверять юрлица и ИП, с которыми работают, СКБ Контур разработал сервис для интернет-банков «Светофор». Он базируется на профессиональном веб-сервисе проверки контрагентов Контур.Фокус.

При загрузке платежных поручений в «Альфа-Бизнес Онлайн» сервис узнает ИНН контрагента и через API-шлюз обращается за данными о контрагенте в Контур.Фокус. В результате перед отправкой платежа клиент видит последние сведения о банкротствах, арбитражных делах, исполнительных производствах и другие важные факты о контрагентах. Сервис имеет понятную визуализацию в виде сигналов светофора, окрашенных в зависимости от важности обнаруженных данных. Кликнув по сигналу, клиент узнает информацию, которая может повлиять на его решение о платеже. Например, данные об арбитражах и сами арбитражные дела.

Также сервис анализирует директора и учредителей контрагентов на предмет «номинальности» и может порекомендовать установить надежный контакт с руководством компании. Так, сервис помогает избежать «плохой дебиторки», проблем с возвратом НДС и повысить информированность о контрагентах.

Результаты внедрения и эффективность

В Альфа-Банке отмечают, что сервис востребован среди клиентов — пользователей интернет-банка «Альфа-Бизнес Онлайн». Полезную опцию уже попробовали несколько тысяч юридических лиц.

Многие из них высоко оценили удобство «Светофора» и реальную пользу их бизнесу. Например, один из предпринимателей планировал перевести своему давнему контрагенту 1,5 млн рублей. Перед отправкой он увидел предупреждающий сигнал и решил не переводить деньги. Оказалось, что предприятие уже не может выполнить свои обязательства.

— Благодаря сервису экспресс-проверки контрагентов, который мы полгода назад внедрили в «Альфа-Бизнес Онлайн», десятки тысяч клиентов Альфа-Банка в онлайн-режиме узнают о последних важных фактах из жизни своих партнеров. Некоторым предпринимателям сервис уже помог предотвратить потерю средств. Вместе с СКБ Контур мы сделали классную и полезную фичу для бизнеса и очень этим довольны,— комментирует Петр Диденко, начальник управления развития электронных продуктов для корпоративных клиентов блока «Электронный бизнес» Альфа-Банка.

В ближайшие полгода СКБ Контур планирует внедрить сервис в нескольких федеральных и региональных банках, а в декабре 2015 г. стартуют первые решения вендоров банковских платформ: BSS (Юниаструмбанк) и iSimpleLab (Крайинвестбанк). Ожидается, в 2016 г. «Светофор» станет всеобщим гигиеническим инструментом при отправке платежей в интернет-банке.

// bankir.ru, 21 декабря 2015 № 1589320

Финансы, банки №1589320

Навигатор

Материалы по защите прав потребителей финансовых услуг

Информационные материалы по защите прав потребителей финансовых услуг были созданы одним из партнеров Проекта по повышению уровня финансовой грамотности жителей, компанией ПАКК, в 2015 году.

Материалы разработаны с учетом специфики восприятия целевых групп Проекта и прошли апробацию.

Брошюры, буклеты и плакаты распространяются с сентября 2015 года. В Калининградской области информационные материалы распространяются региональным управлением Роспотребнадзора, а также в образовательных и других социальных учреждениях. Плакаты добавлены в фотогалерею - в самом подвале страницы.

Список макетов брошюр и буклетов в PDF-формате:

Файлы

Avtokredit_broschura.pdf
Debetovaya karta_broschura..pdf
Dobrovolnye pensionnye nakoplenya_broschura.pdf
Ipotechniy kredit_broschura.pdf
Kreditnaya karta_broschura.pdf
Materialy dlya shkolnikov_broschura.pdf
MFO_broschura.pdf
OSAGO DSAGO avtokasko_broschura.pdf
Plategnye uslugi_broschura.pdf
Potrebitelskiy kredit_broschura.pdf
Vklad i schet_broschura.pdf
Avtokasko_buklet.pdf
Avtokredit_buklet.pdf
Banki_vklady i kredity_buklet shkolniki.pdf
Bankovskaya karta_buklet shkolniki.pdf
Debetovaya karta_buklet.pdf
Dobrovolnye pensionnye nakoplenya_buklet.pdf
Ipotechniy kredit_buklet.pdf
Kreditnanya karta_buklet.pdf
MFO_buklet.pdf
OSAGO DSAGO_buklet.pdf
Pamyatka_zaemschika_buklet.pdf
Plategnye uslugi_buklet.pdf
Potrebitelskiy kredit_buklet.pdf
Strahovanie_buklet shkolniki.pdf
Vklad i schet_buklet.pdf

Источник: http://fingram39.ru/projects/371-materialy-po-zashchite-prav-potrebiteley-finansovykh-uslug.html

22.12.2015

Андрей Заикин: «Структурированные данные — основа информационной безопасности банка»

Андрей Заикин, руководитель направления информационной безопасности компании КРОК

Беседовал: Сергей Вильянов, редактор

Из опубликованного недавно отчета компании Veritas Technologies, получившего название Databerg Report 2015, следует, что IT-специалисты в российских организациях не имеют сведений о 53% данных, хранящихся на внутренних ресурсах, а 30,5% этих данных бесполезны для бизнеса. Это значит, что значительные ресурсы заняты, фактически, хранением цифрового мусора, среди которого могут обнаружиться разнообразные зловреды.

Что еще неприятнее, столь высокая доля неконтролируемого пространства корпоративной сети, которое может содержать конфиденциальные данные, часто становится свидетельством неэффективной работы IT-подразделения. О способах противодействия накапливанию цифрового мусора и повышении безопасности данных в корпоративной сети мы говорили с Андреем Заикиным, руководителем направления информационной безопасности компании КРОК.

— На текущий момент IT-инфраструктуры компаний, особенно работающих долгие годы, очень разрослись. И в ходе этого роста в хранилищах накопились данные, историю появления которых уже никто не помнит. И что в них, собственно, содержится, тоже не всегда очевидно. Даже на уровне личных архивов отдельного сотрудника не всегда наблюдается упорядоченность, и этот сотрудник сам не может объяснить, что, собственно, хранится в файлах, созданных несколько лет назад. И актуальность хранимого под большим вопросом.

На уровне компании эта проблема встает в полный рост. Во-первых, ее хранилище используется неэффективно. В неструктурированных файловых «свалках» лежит очень странный набор информации, включающий музыку, фильмы, какие-то запускаемые файлы с торрентов и т. д. Среди этого может прятаться что-то действительно опасное. Или его там можно надежно спрятать до поры до времени.

Во-вторых, среди этих массивов данных может храниться (и утекать) конфиденциальная информация. Как известно, некоторые вещи с годами могут становиться лишь привлекательнее для третьих лиц.

— Современные Авгиевы конюшни, в общем. С одной стороны, цена гигабайта сейчас такова, что мусор лежит почти бесплатно. С другой — иметь под боком неконтролируемую terra incognita не очень приятно. И как покорить эту целину?

— Необходимо переводить информацию из неструктурированного вида в структурированный. Первый вариант — внедрять системы документооборота, благодаря которым появятся дополнительные метаданные — версионность, владелец, стадия согласования и т. д. Этот процесс движется параллельно развитию информационной индустрии и радикальных перемен не вносит.

Второй вариант — использовать специализированные системы, которые позволяют обеспечить комплексный подход к работе с неструктурированными данными. Такие системы разрабатывают несколько вендоров, например Varonis и Symantec. Класс таких систем называется Data Governance.

Здесь стоит оговориться, что есть системы управления правами доступа — Identity Access Management, Identity Access Governance — они регулируют доступ к корпоративным системам и ресурсам. Data Governance работает именно с неструктурированными данными и обладает особой функциональностью для эффективной работы с ними.

Прежде всего надо классифицировать данные по содержанию. Выяснить, есть в них что-то конфиденциальное или нет. Здесь помогает поиск по ключевым словам, например по номеру заведомо конфиденциального договора, по названиям компаний-партнеров, по автору документа. Также анализируется список пользователей, имеющих доступ к файловым ресурсам. Например, если папка закреплена за топ-менеджером, то в ней с большой вероятностью может храниться что-то важное, даже если к данным давно не обращались.

Исходя из таких эвристик, мы понимаем, что одни данные важны, другие — менее важны, но подлежат хранению (например, бухгалтерская отчетность за прошлые годы), а третьи — важности не имеют вовсе.

Отбор «неважных» данных — довольно кропотливое дело, потому, используя вроде бы очевидные признаки, можно легко ошибиться. Например, что делают видеофайлы большого объема в корпоративной сети? Можно ли их удалять? В большинстве случаев можно, но если видеоматериалы обнаруживаются, к примеру, в общей папке отдела маркетинга, то это нормальная ситуация. Скорее всего, они предназначены для решения рабочих задач. Но если в открытой папке лежат терабайты фильмов, церемониться не стоит.

Анализируется статистика доступа к файлам. Собираются все логи, по которым видно, какой пользователь и когда записал файлы, когда прочитал, в каких группах он находится, какие у него права. Исходя из этого, можно делать определенные выводы. Если человек записал некие данные и больше ни он сам, ни другие к ним не обращались, то, вероятнее всего, они неважны, особенно если прошло несколько лет. Можно обратиться к сотруднику и уточнить, что это. Или просто удалить сразу, если речь идет об avi-файле на 4 гигабайта.

— И как это делать, вручную?

— Такие системы есть в автоматизированном варианте, например Varonis Data Transport Engine, позволяющий переносить данные по определенным признакам на внешние накопители или просто удалять. Или можно делать это вручную, что, конечно, надежнее, но дольше.

Данные, которые вроде бы нужны, но крайне редко используются, лучше архивировать. Например, если к неким папкам больше года никто не обращался, их можно упаковать в архив. Всех сотрудников, имеющих к ним доступ, заранее предупреждают: если данные все же нужны, переместите их в актуальные папки или в личный архив.

Наконец, самые необходимые и востребованные данные необходимо тщательно структурировать и защищать. Мы особенно тщательно отслеживаем, кто к ним обращается и из каких отделов. Например, когда бухгалтерия имеет доступ к своей папке, это нормально. Но если права доступа к ней есть у рядового сотрудника IT-отдела, здесь уже нужно разбираться. Чтобы

расследовать этот потенциальный инцидент, мы смотрим статистику доступа: когда он последний раз обращался и что делал. Если он обращается каждый день напрямую в NTFS и читает все появляющиеся файлы, подозрения усиливаются. Если же обращение было единоразовым и случилось год назад, то, возможно, речь идет о случае техподдержки или восстановления данных из бэкапа. И права доступа уже не нужны.

Есть возможность автоматически отбирать потенциально лишние привилегии. Это может происходить как по причине долгого отсутствия обращений, так и из-за «непохожести» конкретного пользователя на тех, кто обычно имеет доступ к папке. Также можно установить системы, предоставляющие доступ к данным. И вместо того чтобы каждый раз писать заявку в IT-отдел, у нас будет один бизнес-пользователь, который понимает, какие данные хранятся и кому нужен к ним доступ. И он сам будет через специальный портал эти данные предоставлять. Конкретным людям и на заранее определенный срок. Это радикально снижает нагрузку IT-отдела. Но чтобы добиться этого, необходимо провести структурирование данных, о котором мы говорили в самом начале.

— А какую банковскую специфику стоит отметить?

— В банках доля ценных данных особенно высока. Их структуризация позволяет распределить информацию по накопителям различной скорости, самое важное — на самые быстрые и защищенные, остальные — на более объемные и дешевые. Также появляется возможность разместить определенные массивы данных ближе к их непосредственным потребителям, что особенно актуально при разветвленной филиальной сети. В частности, сейчас как раз ведем похожий проект для территориально распределенного банка, который пожелал навести порядок и усилить информационный контроль за региональными филиалами.

— Хорошо, допустим, мы структурировали информацию, как нам теперь контролировать ее перемещение? Расскажите, пожалуйста, о подходах DLP и IRM. Какой из них более эффективен на практике?

— Не секрет, что есть два подхода к борьбе с утечками. Первый — это решения класса Data Loss Prevention (DLP), и второй — Information Rights Management (IRM).

DLP изначально нацелено на защиту от непреднамеренных угроз, когда пользователь хочет отправить информацию наружу без злого умысла. Однако подкованный злоумышленник может, как правило, обойти такую систему.

IRM-система заточена против преднамеренных утечек. Информация, считающаяся конфиденциальной, упаковывается в контейнер, и доступ к ней есть только у проверенных пользователей, обладающих всеми правами. Но права доступа в IRM-системах, как правило, не регулируются, потому что их определяет владелец данных. И чем больше масштабы организации, тем больше времени требуется на настройку IRM. Поэтому есть смысл использовать DLP-системы для защиты всего массива данных от непреднамеренных утечек и IRM — только для конфиденциальной информации.

Но, еще раз повторюсь, внедрение различных систем информационной безопасности практически невозможно, пока данные не структурированы. Нельзя просто купить некое решение, и оно все само как-то заработает. Нет, начинать надо именно со структурирования. Когда данные упорядочены, мы вольны выбирать между различными системами защиты.

— В наступающем году у значительной части банков стоит задача не потратить деньги на что-то новое, а, скорее, сократить затраты. Как в это вписывается тема нашей беседы?

— Много лет подряд банки могли себе позволить быстрое и дорогостоящее развитие систем. Теперь возможностей для этого поменьше. Но когда быстро растешь, не всегда есть время и средства уделять внимание мелким деталям. Сейчас мы видим, что клиенты из банковской сферы стали делать акцент не столько на покупку новых систем, сколько на систематизацию данных и выстраивание внутренних процессов. Да и уже купленные продукты можно настроить более вдумчиво.

Выгода от погружения в оптимизацию зависит от каждого конкретного случая. Но то, что хорошо отлаженные процессы и эффективно работающая система безопасности берегут деньги и снижают риски, это очевидно.

Мы предлагаем услуги по аудиту и описанию бизнес-процессов, связанных с управлением доступом к данным, даем рекомендации по изменениям и готовим соответствующие методики.

Также мы помогаем банкам внедрять соответствующие инструменты для работы с неструктурированными данными, с правами доступа, DLP и IRM-системы.

2016 год будет годом оптимизации затрат в сфере ИБ и IT. Навести порядок в данных необходимо. Это не только расчистит хранилище, но и снизит риски…

// bankir.ru, 22 декабря 2015 № 1592388

Финансы, банки №1592388

04.01.2016

Острожно, мошенники! Как уберечь себя от обмана

Практически ежедневно граждане обращаются с заявлениями о мошенничестве. Особенность данного вида преступлений в том, что люди сами добровольно передают преступникам денежные средства, ценности, сообщают в полиции.

Мошенники, как правило, отличаются способностями психологического воздействия на жертву, красноречивостью, умением убедить в выгодности своих предложений. Часто им на руку оказывается жадность людей, желание без особого труда получить материальную выгоду (приобрести товар по выгодной цене, вложить средства под высокие проценты), либо наивность, малограмотность, отсутствие бдительности, осторожности и мягкосердечность. Во многих случаях в сети мошенников попадают пожилые люди.

Наиболее распространенными видами таких преступлений являются телефонные звонки с информацией о том, что родственник совершил ДТП, совершил преступление по неосторожности и во избежание привлечения его к уголовной ответственности необходима большая сумма денег, якобы для передачи сотрудникам полиции, прокуратуры, пострадавшему или его родственникам. При таких обращениях преступник стремится действовать быстро, напористо, не давая опомниться своей жертве, объясняя это нехваткой времени и тем, что спасти родственника через считанные минуты будет уже невозможно.

Рекомендуемые действия:

Ни в коем случае не сообщать о наличии наличных денег и никому не передавать их. Объяснить преступнику, что необходимо время для сбора, снятия с карты (счета) требуемой суммы. Можно пообещать перезвонить на его номер через несколько минут. Отключившись, немедленно сообщить о звонке в полицию. Для собственного успокоения сделать звонок своим родственникам, которые якобы попали в сложную ситуацию. При этом необходимо помнить, что если телефон родственника недоступен или не отвечает, то это не подтверждает правдивость и достоверность поступившего звонка. Дальнейшие действия согласовывать с полицией.

Часто граждане обращаются с заявлениями о том, что внесли крупные суммы в кредитно-потребительские кооперативы, где обещали высокую доходность, а на деле не возвращают даже внесенные средства. Об этом уже много говорили и писали, было множество примеров, но граждане продолжают верить в чудо и доверяют свои сбережения сомнительным предпринимателям. Чей-то пример о получении прибыли в этой организации не дает никакой гарантии выполнения обязательств перед вами. Сам принцип финансовых пирамид заключается в привлечении максимальных средств от вкладчиков, благодаря рекламе определенного круга лиц, которые реально получили доход. Это сродни игровому бизнесу, и каждый должен понимать, что жертвуя своими деньгами, он не получает никаких гарантий дохода, а шанс стать счастливчиком очень призрачный. Это доказали тысячи обращений в полицию пострадавших от мошенников, но и по сей день люди ждут чуда и сами ищут кому доверить свои сбережения, чтоб быстро разбогатеть. Остается напомнить, что чудеса бывают только в сказке, а в реалии от граждан продолжают поступать десятки заявлений о потерянных деньгах и несбывшихся мечтах.

В последнее время жулики активно используют интернет-ресурсы. Один из способов получения легких денег – введение в заблуждение пользователей одного из распространенных сайтов бесплатных объявлений. Очень удобный ресурс для тех, кто хочет что-то продать или купить, но и тут нельзя терять бдительность. Для примера один из распространенных способов, которыми пользуются мошенники. Совершают телефонный звонок гражданину о том, что планируют купить вещь, представленную в объявлении на сайте. Для гарантии серьезности своих намерений предлагают внести на банковскую карту продавца предоплату, для чего просят продиктовать номер и другие данные карты. Продавец в соблазне быстрой продажи и получения денег с удовольствием предоставляет требуемые данные. В последующем, пользуясь этими данными, мошенники снимают с карты все денежные средства, либо оплачивают товары или услуги с карты потерпевшего. Такие преступления заявляются практически ежедневно.

Так, 1 ноября текущего года в дежурную часть отдела поступило заявление гражданки, 1987 г.р., которую заинтересовало объявление о продаже автомобиля. Цена казалась заманчивой и авто подходящим. Созвонившись с продавцом, она согласилась сделать предоплату в сумме 10 тысяч рублей на указанный номер карты, чтоб забронировать покупку. Продавец обещал в ближайшее время пригнать машину и оформить сделку. Но после перечисления задатка номер телефона оказался заблокирован, а несостоявшаяся покупательница осталась один на один с нажитой проблемой.

2 ноября лишилась денежных средств в сумме 450 тысяч рублей еще одна гражданка, которая сообщила «покупателю» данные своей карты, по ранее поданному ею объявлению на Интернет-сайте о продаже козы. Коза вместо дохода принесла большой убыток, а деньги, как было установлено, «ушли» в Ульяновскую область.

Вывод: никогда никому не передавайте данные своей банковской карты, так как они могут быть использованы преступниками. Даже если вы пользуетесь услугами известных интернет магазинов с использованием банковской карты, то целесообразно иметь запасную карту, на которой размещен минимум средств, для проведения покупки.

Не обошли стороной наших горожан и мошенники, действующие через социальные сети. Взломав страничку пользователя и обнаружив там множество его друзей, всем им были разосланы письма с просьбой, в связи с возникшими проблемами, перечислить взаймы денежные суммы на указанный номер телефона либо интернет-кошелек. Естественно, нашлись друзья, готовые помочь материально в трудную минуту, и направившие свои кровные мошенникам.
В последнее время участились случаи, когда потерпевшие, желая трудоустроиться, перечисляют денежные средства по объявлению с предложением работы. Практически все такие случаи заканчиваются визитом в полицию и утраченными крупными денежными суммами. Мнимый работодатель красочно описывает возможность трудоустройства в госучреждение (варианты - объект энергетики, предприятие на Севере), обещая высокую зарплату, полный соцпакет и т.д. Для осуществления мечты нужно всего лишь взять коньячка, колбаски и придти в учреждение, где его встретит работодатель. Название учреждения выбирается таким образом, что оно есть в любом городе или райцентре. Через пару минут следует звонок, что для решения вопроса надо срочно «забросить» денег на интернет (сотовый телефон), которые потом вернут. Иногда следует предложение через час перечислить затраченную сумму на карточку, для чего нужны реквизиты карты. В результате соискатель работы обнаруживает, что его в учреждении никто не ждет, номер «работодателя» не доступен, деньги пропали. Потерпевшему ничего не остается как обратиться в полицию и снять полученный стресс не востребованным коньячком с закуской. Как правило, оказывается, что звонки с предложением работы были сделаны из другого, отдаленного региона.

Часто обращаются граждане внесшие предоплату за поставку товаров и услуг (поставка сруба, стройматериалов, проведение монтажных и ремонтных работ и т.д.). В последующем товар не поставляется, услуги не оказываются и после месяцев ожидания и попыток самостоятельно вернуть перечисленные средства, неизбежно обращение за помощью в полицию. Вернуть деньги бывает сложно и не всегда возможно, тем более что часто заявитель передает деньги без оформления каких-либо расписок, лишь по устной договоренности. Вывод: не передавайте и не перечисляйте деньги за не оказанные услуги. Планируемые сделки оформляйте документально.

Достаточно часто значительные денежные суммы с банковских карт похищаются с использованием современных технологий, посредством распространения вирусных программ, которые позволяют мошенникам снимать средства со счетов абонентов, пользующихся мобильным банком. При этом по факту перечисления сумм с карты извещение мобильного банка об операции блокируется и не производится. Более уязвимы для таких вирусов устройства с операционными системами, которые установлены на большинстве сотовых телефонов. Имеющееся антивирусное обеспечение для средств мобильной связи далеко не всегда способно предотвратить такое вмешательство. Самый надежный выход – не пользоваться приложением «Мобильный банк», так как шансы возврата утраченных сумм практически близки к нулю.

Остается добавить, что большинство денежных средств, утраченных по халатности потерпевших, так и не удается вернуть. Преступные схемы связанные с интернетом, телефонными звонками, банковскими картами, как правило, реализуются из других регионов России. Для получения средств используются утраченные паспорта граждан и телефонные номера, а порой и банковские карты оформленные с их помощью. Это, к слову, должно стать предостережением от утерь своих документов и бережное к ним отношение.

Наивно было бы полагать, что при выборе жертвы преступники пожалеют одинокую пожилую больную женщину или побоятся обокрасть состоятельного чиновника с большими полномочиями. Потерпевшим может стать каждый из вас или ваших родственников.
Наш город – наш дом. Мы хотим, чтоб жить в нем было спокойно, удобно и комфортно, а значит и безопасно. Мы призываем всех граждан содействовать нам в этом, проявляя бдительность, разъясняя своим родственникам, знакомым, соседям какие угрозы существуют, как от них защититься, противостоять. Не оставайтесь безучастными в вопросах профилактики правонарушений и преступлений. Любую информацию о совершенных или готовящихся преступлениях незамедлительно предоставляйте в дежурную часть территориального отдела внутренних дел.

http://www.magcity74.ru/news/28958-ostrozhno-moshenniki-kak-uberech-sebja-ot-obmana.html

28.01.2016

В МВД по Чувашской Республике прошла пресс-конференция по теме: «Киберпреступления и телефонные мошенничества»

28 января в МВД по Чувашской Республике прошла пресс-конференция по теме: «Киберпреступления и телефонные мошенничества». С представителями республиканских и районных СМИ встретились руководители управления уголовного розыска, отдела «К» и

Чувашского отделения ПАО «Сбербанк». Заместитель начальника отдела управления уголовного розыска МВД по Чувашской Республике подполковник полиции Евгений Андреев рассказал о мошенничествах, совершаемых на территории республики. «В 2015 году на территории Чувашии совершено 1058 фактов мошенничеств, из них 102 факта в сельской местности. Чаще всего жертвами обмана становились жители Чебоксар, Новочебоксарска, Канаша, Алатырского и Чебоксарского районов», - рассказал Евгений Анатольевич. Об основных видах совершаемых мошенничеств рассказал начальник отделения по раскрытию мошенничеств общеуголовной направленности УУР МВД по Чувашской Республике старший лейтенант полиции Андрей Яблоков. По его словам, чаще всего жители республики становятся жертвами так называемых «социальных» мошенничеств (совершаются под видом социальных работников, снятия порчи, продажи меда) и хищений с использованием средств сотовой связи и сети Интернет. О преступлениях, связанных с хищением денежных средств с банковских карт, рассказал начальник отдела «К» МВД по Чувашской Республике подполковник полиции Александр Смирнов. «С начала года зарегистрировано 49 фактов списаний денежных средств с банковских карт граждан, из них 7 случаев с использованием вредоносного программного обеспечения, скачанного при открытии смс-сообщений с незнакомых номеров», - уточнил Александр Владимирович. Об основах безопасного пользования банковскими картами и мерах по противодействию мошенничеству рассказал начальник управления прямых продаж Чувашского отделения ПАО «Сбербанк» Евгений Слепенко. В завершении мероприятия выступающие ответили на вопросы журналистов.

Пресс-служба МВД по Чувашской Республике

Несколько правил работы с банковскими платежными картами:

Нельзя никому и никогда сообщать пин-код карты и реквизиты карты (номер карты, секретный код, срок действия карты и на кого она зарегистрирована);

Необходимо выучить пин-код либо хранить его отдельно от карты;

Нельзя передавать карту другим лицам – все операции с картой должны проводиться на Ваших глазах или вами лично;

Не разрешайте операторам принимающим платежи или кассирам в магазинах разглядывать вашу карту и после ее возвращения убирайте ее немедленно с глаз;

При снятии денежных средств нужно стараться использовать только те банкоматы, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной. Такие банкоматы устанавливаются в государственных учреждениях, банках, крупных торговых центрах и т.д. в которых затруднен доступ к банкоматам (пропускная система) или находяться под круглосуточным наблюдением охраны;

Не выкидывайте чеки от банкомата у самого банкомата, по возможности старайтесь уничтожить чек;

Совершая операции с пластиковой картой в банкомате следите, чтобы рядом не было посторонних людей, обращайте внимание на картоприемник, клавиатуру и сам банкомат. Если они оборудованы какими-либо дополнительными устройствами и на них приклеены коробочки с рекламой, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на банкомате телефону;

При осуществлении покупок в сети Интернет не вводите дважды информацию с карты. В случае сбоя, после ввода первого раза обязательно проверяйте адрес сайта в строке браузера. В случае неуверенности правомочности сайта немедленно заблокируйте карту;

При осуществлении оплаты услуг через сеть Интернет обращайте внимание на начало адреса в адресной строке браузера в которой должен быть указан нарисованный замочек и символы https:// обозначающий зашифрованный протокол обмена данными;

10. При поступлении звонков на телефон от имени сотрудников банка, которые просят вас сообщить им сведения о вас и реквизиты банковской карты не разговаривайте с ними и по возможности сообщите в правоохранительные органы о номере телефона с которого поступил звонок;

11. Если у Вас возникли вопросы по работе с картой, советуйтесь только с сотрудниками банка, никогда не прибегайте к помощи или советам третьих лиц при проведении операций с банковской картой;

12. В случае смены номера телефона, на который приходят уведомления о совершаемых банковских операциях, замените и номер уведомления в отделении банка;

13. Банковскую платежную карту, являющуюся «зарплатной» и имеющей овердрафт (кредитный лимит) старайтесь не использовать при покупках в магазинах и в сети Интернет, так как в случае кражи с нее денежных средств снимут всю сумму хранимых денег и весь лимит кредита;

14. В случае обладания банковской платежной картой и имея привязанный номер сотового телефона, исключите возможность использования сотового телефона для работы в сети Интернет и посещения различных сайтов, так как велика возможность получения на сотовый телефон

вредоносных программ, осуществляющих кражи денежных средств с банковских карт, по возможности пользуйтесь не бесплатными антивирусными программами;

15. Храните пароли для работы с услугой «Интернет-банкинга» в недоступном месте для посторонних лиц, в случае их утери немедленно сообщите в банк о блокировке доступа к личному кабинету услуги «Интернет-банкинга» и примите меры к смене всех ранее выданных или полученных паролей.

Памятка владельцам банковских карт

Банковская карта – это очень удобный способ хранения денежных средств и безналичной оплаты покупок в магазинах, кафе и в сети Интернет. Эти карты были придуманы и созданы для удобства населения в обращении с деньгами и для исключения использования наличных средств. И вместе с тем, владельцы банковских карт из-за своей невнимательности или незнания элементарных правил безопасности подвергают себя опасности и могут лишиться своих денежных средств. В последнее время увеличилось количество преступных посягательств на «содержимое кошельков» граждан, хранимое на банковских счетах и обслуживаемых посредством банковской платежной карты (карточный счет). В силу того, что банковская карта для банковского счета является неким ключом, позволяющим совершать практически все банковские операции со счетом (с денежными средствами), при этом, требуется только наличие самой карты и знание ее ПИН-кода, то это обстоятельство явилось причиной резкого возросшего внимания со стороны преступных элементов в отношении лиц, владеющих такими платежными картами и средств, хранимых на счетах, обслуживаемых с помощью них.

По информации отдела «К» МВД по Чувашской Республике

https://21.mvd.ru/news/item/7137684/

28.01.2016

МВД России по Тверской области советует, как уберечь себя от мошенничества в интернете

tverlife_news_

В настоящее время все более распространенным способом хищений денежных средств граждан становятся хищения с банковских пластиковых карт при помощи услуги «Мобильный банк».

Данному виду преступлений в основном подвергнуты клиенты крупных банков. При открытии счета гражданам предлагается услуга «Мобильный банк», а для ее отключения необходимо написать заявление, о чем не всегда предупреждают клиентов.

В настоящее время можно выделить три основных способа, при помощи, которых совершаются хищения денежных средств.

1. Способ «Классический». Данный способ можно назвать самым распространенным.

Потерпевшим при заключении договора указывается абонентский номер, который и подключается к «Мобильному банку». По различным причинам, многие владельцы пластиковых карт банков перестают в дальнейшем пользоваться абонентскими номерами (потерял, переехал, сменил оператора и т.д.), в связи, с чем оператор сотовой связи через шесть месяцев перевыпускает СИМ-карту с данным абонентским номером и выставляет ее на продажу.

После приобретения данной СИМ-карты новому абоненту продолжают поступать СМС-сообщения о движении денежных средств по карте предыдущего владельца СИМ-карты и, соответственно, остается возможность управлять данной картой через «Мобильный банк».

Возможностью перевести денежные средства на свой новый абонентский номер могут как лица, которые приобрели СИМ-карту для себя, предоставив для этого необходимый пакет документов, так и лица, которые скупают оптом СИМ-карты у недобросовестных представителей операторов сотовой связи, не оформляя их надлежащим образом, в том числе в различных регионах России.

2. Способ «Вредоносные программы»

2.1. Используется вредоносная программа, которая самостоятельно рассылает СМС - сообщения с телефона потерпевшего.

Данная программа устанавливается (попадает) на телефон при получении СМС или ММС сообщений, а так же при посещении различных Интернет сайтов.

Одним из признаков наличия вредоносной программы на мобильном телефоне может являться направление «пустых» СМС или ММС сообщений на номера телефонов, имеющихся в разделе «Контакты» мобильного телефона. При открытии такого СМС или ММС происходит заражение телефона, который получил данное сообщение. Возможно получение потерпевшим СМС с номера «900» с различной информацией, которую он не запрашивал.

Выявить, что на телефоне установлена вредоносная программа, так же можно при помощи получения детализации телефонных звонков и СМС. В данном случае, при наличии вредоносной

программы в распечатке звонков, в разделе «Исходящие СМС» будут сообщения на номер «900», которые владелец телефона не направлял.

2.2. Используется платный сайт или платная программа в интернете

При помощи данной программы злоумышленником отправляется СМС с подменой (клонированием) номера на сервисный номер «900», т.е. при направлении сообщения указывается номер потерпевшего, и как в вышеуказанном способе, денежные средства переводятся на абонентский номер или на расчетный счет.

Отличие от вышеперечисленного способа в п.2.1. является отсутствие в распечатке детализации телефонных звонков и СМС, т.е. в разделе «исходящие СМС» с абонентского номера потерпевшего не будет сообщений на номер «900», а будут только ответные (входящие) СМС с данного номера.

3. Способ «Фишинговый сайт»

Данный способ возможен, когда потерпевший пользуется «Личным кабинетом» на интернет-сайте банка. Злоумышленниками создается (используется) сайт, адрес, которого и внешнее оформление идентичны официальному сайту банка. Если потерпевший при входе на сайт банка не использует сохраненную ссылку, а просто набирает название банка в поисковике, то ему обычно предлагается несколько вариантов. Если потерпевшим будет осуществлен вход на такой фишинговый сайт, и будут использованы свои данные для входа в личный кабинет банка (логин и пароль), то данной информацией и могут воспользоваться злоумышленники для входа в «Личный кабинет» на настоящем сайте банка от имени потерпевшего. Далее возможен перевод денег из «Личного кабинета» или подключение карты потерпевшего к услуге «Мобильный банк» на любой абонентский номер.

Основным признаком, что клиент зашел на фишинговый сайт является то, что после ввода логина и пароля на странице появляется надпись о техническом обслуживании сайта или любая иная информация, в которой будет указано о том, что обратиться на сайт можно позднее.

В настоящее время мошенники активно применяют способ, связанный с получением от потерпевшего информации о реквизитах карты, таких как номер, срок действия, CVC/CVV-код (трехзначный код на обратной стороне карты), а так же кодов для осуществления операции по получению логина и пароля системы Интернет-банкинга (например, «Сбербанк Онлайн», «Телебанк» и др.) под предлогом осуществления перевода денежных средств на счет потерпевшего в качестве предоплаты за приобретение продаваемого им товара, недвижимости, автотранспорта, услуг и т.д.

Получив данную информацию, злоумышленник получает доступ к системе интернет-банкинга, в которой, как правило, отражены все имеющиеся пластиковые карты и счета потерпевшего, далее через неё дополнительно подключает услугу мобильного банкинга на свой абонентский номер, а затем беспрепятственно осуществляет перевод денежных средств со всех данных счетов.

Чтобы не стать жертвой мошенников соблюдайте простые правила безопасности:

- не осуществляйте операций по переводу денежных средств на счета и телефонные номера неизвестных Вам лиц;
- не сообщайте незнакомым людям банковские реквизиты принадлежащих Вам пластиковых карт и счетов, свои паспортные данные, любые пароли, пин-коды и иную конфиденциальную информацию;
- перед подключением и использованием услуг интернет-банкинга и мобильного банкинга внимательно ознакомьтесь с условиями, правилами и особенностями предоставления данных услуг, а так же механизмом их действия.
- при блокировке своего абонентского номера у сотового оператора, в случае наличия подключенной услуги мобильного банкинга, обязательно отключите её через оператора горячей линии банка.
- не распространяйте в сети Интернет личную информацию о себе и своих близких.
- используйте для совершения покупок в сети Интернет только проверенные магазины и ресурсы.

http://www.tverlife.ru/short-news/105247.html

29.01.2016

Никогда не сообщайте посторонним лицам номер своей банковской карты!

В 2015 году в ОМВД России по г. Ельцу по-прежнему было зарегистрировано большое количество сообщений о преступлениях так называемых » в сфере телефонного мошенничества и компьютерной связи». В настоящее время мошенники прибегают к новым способам завладения денежными средствами, а именно совершения телефонных звонков по объявлениям размещенных на сайтах «Авито.ру, Авто.ру». Так, в ходе телефонного разговора мошенники сообщают, что готовы приобрести ту или иную вещь, которая соответственно размещена на сайте продаж. В ходе диалога недобросовестный покупатель просит прислать продавца номер

банковской карты на которую он желает перевести задаток в качестве оплаты товара, чтобы последний не передумал продать товар другому лицу. После этого лицо введенное в заблуждение с радостью сообщает мошенникам данные своей банковской карты и денежные средства уже через считанные минуты поступают в пользование мошенникам. Такие лица могут позвонить даже по самым невостребованным товарам только с одним умыслом — это хищение денежных средств. Не становится меньше сообщений о преступлениях, когда мошенники наоборот сами размещают товар и просят добросовестных покупателей перевести на их банковский счет или абонентский номер денежные средства. Поэтому просим жителей г. Ельца быть более бдительными в разговорах при продажи и покупки товаров через Интернет, сообщает прокуратура Ельца.

http://trkelets.ru/news-51128.html

29.01.2016

Надежно, как в Сбербанке: в Верхневолжье осудили специалиста по работе с клиентами

Ржевский городской суд вынес приговор сотруднице Сбербанка.

За хищение чужого имущества в крупном размере она получила наказание в виде лишения свободы на срок два года без штрафа и без ограничения свободы, условно с испытательным сроком в три года

В ходе рассмотрения уголовного дела установлено, что не позднее 25 сентября 2014 года у специалиста по обслуживанию частных лиц дополнительного офиса 8607/0202 Тверского отделения №8607 ОАО «Сбербанк России» возник и сформировался корыстный умысел, направленный на незаконное личное обогащение посредством систематического хищения вверенных ей денежных средств ОАО «Сбербанк России» путем их присвоения.

- С 25.09.2014 года до 09.12.2014 года гражданка Г., исполняя свои функциональные обязанности специалиста по обслуживанию частных лиц на своем рабочем месте в дополнительном офисе 8607/0202 Ржевского отделения Тверского отделения №8607 ОАО «Сбербанк России» в Ржеве, имея умысел на хищение вверенного ей имущества, руководствуясь корыстными побуждениями, незаконно систематически совершала хищение денежных средств ОАО «Сбербанк России», которые безвозмездно против воли собственника обращала в свою пользу, — сообщили в пресс-службе Ржевского городского суда.

За этот период сотрудница Сбербанка присвоила и потратила по своему усмотрению 303 826,43 руб., принадлежащие ОАО «Сбербанк России». Отказавшись от дачи показаний против себя в силу ст. 51 Конституции РФ, в судебном заседании вину она все же признала.

ОАО «Сбербанк России» по уголовному делу заявлен гражданский иск на сумму 303 826 рублей 43 копейки, подсудимая Г. согласилась с указанным гражданским иском. Иск был удовлетворен в полном объеме.

http://www.glavny.tv/news/12657

30.01.2016

В Ульяновске полиция разыскивает женщину, похитившую в банке 5 млн рублей

В Ульяновске неизвестная женщина подозревается в хищении денежных средств, общая сумма которых составила пять миллионов рублей. Информацию об этом предоставили сотрудники управления МВД Российской Федерации по Ульяновской области.

Как известно из сообщений УМВД по Ульяновской области, данный инцидент произошел еще в середине октября прошлого 2015 года. В отделении "Сбербанка" на улице Хрустальной женщина, которой на вид не более 50 лет, предоставила сотрудникам финансового института подложные документы, в том числе и удостоверение личности. После этого неизвестная сняла со счета 57-летней женщины, не проживающей в настоящее время на территории Ульяновска, денежную сумму в размере пять миллионов рублей. Затем нарушительница скрылась, но ее лицо успело попасть на камеры видеонаблюдения, установленные в банке.

Подозреваемая имеет худощавое телосложение, светлые волосы и выглядит не старше 40-50 лет. На момент совершения преступления женщина была одета в яркий шарф, покрывающий голову, темную дубленку, имела очки в черной оправе. Всех, кто осведомлен о местонахождении нарушительницы, просят сообщать в соответствующие структуры.

Лиза Морская

http://www.vladtime.ru/proish/468181-v-ulyanovske-policiya-razyskivaet-zhenschinu-pohitivshuyu-v-banke-5-mln-rubley.html

31.01.2016

Памятка для граждан: Подозрительно низкая цена товара в Интернете

Один из популярных способов мошенничеств, основанных на доверии, связан с размещением объявлений о продаже товаров на электронных досках объявлений и интернет-аукционах. Как правило, мошенники привлекают своих жертв заниженными ценами, выгодными предложениями и требуют перечисления предоплаты путем перевода денежных средств на электронный кошелек.

Внимательно изучите объявление, посмотрите информацию о лице, разместившем его. Если торговая площадка имеет систему рейтингов продавцов, изучите отзывы, оставленные другими покупателями, не забывая о том, что преступники могут оставлять положительные отзывы о себе, используя дополнительные учетные записи.

Воспользуйтесь Интернет-поиском. Иногда достаточно ввести в форму поиска телефонный номер или сетевой псевдоним продавца для того, чтобы обнаружить, что эти данные уже использовались в целях хищения денежных средств и обмана покупателей.

Посмотрите среднюю стоимость аналогичных товаров. Слишком низкая стоимость должна вызвать у вас подозрение.

Если продавец требует перечислить ему на электронный счет полную или частичную предоплату за приобретаемый товар, подумайте, насколько вы готовы доверять незнакомому человеку.

Помните, что, перечисляя деньги незнакомым лицам посредством анонимных платежных систем, вы не имеете гарантий их возврата в случае, если сделка не состоится.

Пресс-служба МВД по Республике Тыва

https://17.mvd.ru/news/item/7147941/

31.01.2016

Полиция информирует граждан о том, как не стать жертвами мошенников

Нередко в полицию поступают сообщения от пожилых граждан о том, что путем обмана и злоупотребления доверием их деньгами завладели неизвестные преступники. Как правило, мошеннические схемы всегда одинаковы: это звонок по телефону с сообщением о происшествии с родственником, которого необходимо «откупить» от уголовной ответственности, или же преступники под видом работников социальных служб проникают в дом к пенсионерам и похищают денежные средства. Мошенники в корыстных целях пользуются доверчивостью пожилых граждан, обещая пенсионерам, ветеранам войны и труда произвести социальные выплаты, получить подарки, предлагают провести в их домах и квартирах льготный ремонт. Это один из наиболее распространенных способов обмана, конечной целью которого является хищение или получение денежных средств от потерпевших.

Полицейские в очередной раз напоминают жителям Ростовской области о бдительности и осторожности. Если незнакомцы представляются сотрудниками горгаза, ЖКХ, Министерства здравоохранения – попросите их предъявить документы, лучше всего – удостоверение. Прежде, чем запустить кого-то в дом, сделайте звонок в организацию, представителями которой назвались пришедшие, и уточните, отправляли ли к вам сотрудников.

Не оставляйте незнакомцев без присмотра, ни в коем случае не уходите в другую комнату. Не рассказывайте гостям о своих сбережениях, тем более не демонстрируйте их перед пришедшими. И обязательно закрывайте за нежданными посетителями дверь.

Если Вам звонят с сообщением, что ваш родственник или знакомый попал в аварию, в полицию, в больницу, и теперь за него нужно внести залог, штраф, взятку – одним словом, откупиться, это мошенники! Обязательно свяжитесь с родственниками или знакомыми! Не предпринимайте поспешных решений. О данных мерах предосторожности также необходимо регулярно напоминать своим пожилым родственникам во время семейных бесед.

Если вас или вашего пожилого родственника все же обманули – сразу же звоните по телефону дежурной части «02» или в отдел полиции вашего района. Чем быстрее вы это сделаете, тем выше возможность задержать злоумышленников и раскрыть преступление по «горячим следам».

Пресс-служба ГУ МВД России по Ростовской области

https://61.mvd.ru/news/item/7148791/

31.01.2016

Заражение телефона вирусом грозит потерей денежных средств с банковской карты

Вирусная программа попадает в смартфон через спам-рассылку смс-сообщений, содержащих различные ссылки. Если пользователь кликает на нее, то скачивается вредоносная программа, которая способна без участия абонента совершать операции с банковской картой. Пользователь даже не догадывается о том, что его телефон заражен, и с его счета списываются средства, так как вирусная программа полностью удаляет входящие SMS-уведомления от банка. В итоге деньги переходят на электронные кошельки злоумышленников.

Сотрудники полиции рекомендуют владельцам телефонов избирательно относиться к получаемой информации и не открывать незнакомые ссылки во входящих смс-сообщениях, будь то даже известные приложения. Также не следует скачивать приложения из непроверенных источников.

В целях профилактики заражения смартфонов необходимо регулярно обновлять антивирусы на своих телефонах. В противном случае вы рискуете занести в свой аппарат вирус и лишиться денежных средств с банковской карты.

В случае обнаружения факта хищения денежных средств необходимо обратиться в кредитную организацию для получения подробной выписки о движении ваших средств (с указанием адресата получения переводов) и заблокировать карту. У сотового оператора нужно получить детализацию соединений по номеру, на который подключена услуга «Мобильный банк», и с этими документами обращаться в полицию.

Пресс-служба МВД по Чувашской Республике

https://21.mvd.ru/news/item/7148895/

Номер подписан в свет 08.02.2016