ПРИКЛАДНАЯ

ИНФОРМАТИК@

научно-практический журнал

№ 3 (81) 2019

ISSN 1993-8314

СИНЕРГИЯ ПРИНТ

прикладная

ИНФОРМАТИК@

научно-практический журнал

Том 14. №3 (81). 2019

Май – Июнь

ISSN 1993-8314

Университет «Синергия»

Журнал включен в Перечень ведущих периодических изданий, рекомендованных ВАК для публикации результатов диссертационных исследований.

Журнал выходит с 2006 г. Периодичность издания — 6 раз в год.

Журнал индексируется в российских и зарубежных базах научной периодики eLIBRARY (РИНЦ), Russian Science Citation Index (RSCI) на платформе Web of Science, ВИНИТИ, Ulrich's Periodicals Directory

Учредитель и издатель: Негосударственное образовательное частное учреждение высшего образования «Московский финансово-промышленный университет «Синергия»»

Адрес редакции и издателя:

129090, Москва, ул. Мещанская, д. 9/14, стр.1 (юрид.)

125190, Москва, Планетная ул., д. 36, оф. 301, 302

Тел.: +7 (495) 987-43-74 (доб. 33-04); e-mail: appliedinformaticsjournal@gmail.com; www.appliedinformatics.ru

Journal of Applied Informatics

INFORM@TICS

Peer-reviewed scientific journal

Vol. 14. No. 3 (81). 2019

ISSN 1993-8314

May – June

Synergy University

Published since 2006. Periodicity: six times a year.

The journal is indexed in
Russian Science Citation Index (RSCI) on Web of Science platform,
VINITI (Russian Academy of Sciences), Ulrich's Periodicals Directory

Publisher: Moscow University for Industry and Finance «Synergy»

Publisher address: 9/14 s.1, Meshchanskaya str., Moscow, 129090, Russia

Editorial office address: of. 301; 36, Planetnaya st., Moscow, 125319, Russia

Tel: +7 (495) 987-43-74 (ext. 33-04); e-mail: appliedinformaticsjournal@gmail.com; www.appliedinformatics.ru

ИТ-БИЗНЕС

E-commerce

ИТ-МЕНЕДЖМЕНТ

Управление эффективностью

ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА

Эффективные алгоритмы

Информационная инфраструктура

Сетевые технологии

SIMULATION

Акторное моделирование

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Защита информации

ЛАБОРАТОРИЯ

Модели и методики

DOI: 10.24411/1993-8314-2019-10011

А. А. Протасова, *Университет «Синергия», г. Москва, aprotasova@synergy.ru*
О. А. Козлова, *Университет «Синергия», г. Москва, blestoks@yandex.ru*

Мошенничество в онлайн-торговле

Статья посвящена исследованию различных способов мошенничества с платежами в онлайн-торговле, которые наиболее распространены в последнее время. В работе описаны особенности различных видов мошенничества, эффективные и популярные программы по предотвращению мошенничества в онлайн-торговле, и исследованы характеристики работы программ по отслеживанию подозрительных транзакций. Статья предназначена для формирования представления о наиболее распространенных способах мошенничества с платежами в онлайн-торговле и комплекса мер по их предотвращению.

Ключевые слова: мошенничество в онлайн-торговле, фишинг, фарминг, дружественное мошенничество, чистое мошенничество, схема мошенничества, способы борьбы с мошенничеством в онлайн-торговле.

Введение

Развитие современных информационно-компьютерных технологий влияет на все сферы жизни и деятельности человека. И даже традиционная торговля все более и более смещается в сторону онлайн-торговли, что приводит к появлению различных способов мошенничества в онлайн-торговле. Мошенничеством в торговле называется мошенничество с платежами, к которому относится любой вид нелегальной или неправильно осуществленной транзакции. Мошенничество с платежами — это давно существующая проблема. На протяжении достаточно долгого времени излюбленным методом мошенников являлась кража банковской карты и последующее осуществление покупок с помощью данной карты. Это по-прежнему происходит, но более распространенным становится относительно новый вид мошенничества — мошенничество в онлайн-торговле.

В данной статье проанализированы различные способы мошенничества в онлайн-торговле, рассмотрены их основные особенности. Цель этой работы — выявление методов обнаружения мошенничества в онлайн-торговле и разработка комплекса мер, которые могут помочь отследить и предотвратить это мошенничество. Объектом исследования являются процессы мошенничества. Предметом исследования является методы обнаружения мошенничества, и меры, позволяющие отследить и предотвратить мошенничество

Содержание исследования

В связи с активным ростом сектора онлайн-торговли в последние годы происходит существенное увеличение случаев нелегального овладения информацией о банковских картах. Полученную информацию хакеры чаще всего используют сами для осуществления нелегальных транзакций или продают информацию кибертеррористическим организациям для их мошеннической деятельности.

Согласно отчетам компаний из области онлайн-торговли [6], опубликованным в 2017 году, а затем подтвержденным в 2018,

количество нелегальных транзакций по всему миру:

- увеличивалось каждый год с 2004;
- особенно увеличилось в промежуток с 2010 по наши дни;
- сохранит темпы роста на текущей отметке предположительно до 2020 года.

В 2018 сумма совокупных убытков, понесенных компаниями в связи с мошенничеством в онлайн-торговле, в процентном соотношении составила 1,8%, что превысило показатель 2017 года в 1,58%. В среднем 1 доллар, потерянный компанией в результате мошенничества, обходится ей в 2,94 доллара, что также выше прошлогоднего показателя на 17 центов.

По сравнению с 2013 годом, число случаев мошенничества в онлайн-торговле увеличилось на 19%, и уже четвертый год подряд темпы роста количества транзакций, совершенных мошенниками, превышают темпы роста количества транзакций в онлайн-торговле в целом [12]. Из 100 долларов, находящихся в обороте в онлайн-торговле, мошенники в среднем присваивают 5,65 центов.

Мошенничество в онлайн-торговле связано как с оплатой при помощи кредитных карт, так и с использованием вирусного программного обеспечения, дающего доступ к аккаунтам человека в системе онлайн-банкинга через телефоны, планшеты, компьютеры; при этом украденная информация используется для осуществления оплаты.

В связи с вышеизложенным, одной из актуальных задач в настоящее время является обнаружение мошенничества в онлайн-торговле и разработка комплекса мер по отслеживанию и предотвращению мошенничества. Для решения задачи необходимо:

1. изучить причины появления мошенничества в онлайн-торговле;
2. проанализировать наиболее распространенные схемы мошенничества;
3. сравнить способы защиты бизнеса в онлайн-торговле от мошенничества и определить оптимальные методы защиты.

Схемы мошенничества онлайн-торговле

Мошенничество в онлайн-торговле — это нелегальная или неправильная транзакция, осуществляемая через онлайн-магазин. Разница между кражей банковской карты и кражей в онлайн-торговле заключается в том, что при совершении сделок в онлайн-торговле необязательно физическое присутствие банковской карты. Мошеннику всего лишь нужна информация о банковской карте. Хакеры могут нелегально завладеть данной информацией, так как она часто хранится и передается в цифровом формате, а учитывая, что большие объемы информации о банковских картах хранятся и передаются онлайн, хакерам стало проще получить доступ к данной информации.

Каждый раз, когда принимаются меры по предотвращению мошенничества, хакеры адаптируются к ним и находят новые способы обхода установленных барьеров.

Мошенничество в онлайн-торговле является распространенным по двум основным причинам:

1. Хакерам достаточно легко завладеть необходимой информацией. Мошенникам, в свою очередь, легко купить эту информацию на черном рынке.

2. Наблюдается недостаток юридических норм, регламентирующих преследование за данный вид мошенничества.

Отставание законодательной базы обусловлено тремя причинами [10]:

1. Достаточно сложно отследить мошенничество в области онлайн-торговли и с точностью определить преступника, совершившего нелегальную транзакцию. Мошенники постоянно регистрируют искусственные e-mail-аккаунты и используют почтовые ящики (в реальной жизни) под псевдонимом, не раскрывая реальной информации о себе.

2. Расследование дел о мошенничестве в онлайн-торговле не является приоритетным для органов внутренних дел, так как средняя

сумма каждой сделки, в которой замешаны мошенники, относительно низкая.

3.Мошенничество в онлайн-торговле чаще всего выходит за границы одной конкретной страны, что с юридической точки зрения осложняет преследование мошенников и последующее наказание.

Исследование, опубликованное компанией Worldpay, задействовало 274 предприятия из разных отраслей, которым задавались вопросы о случаях мошенничества в онлайн-торговле. 52% участников исследования воспринимают рост транзакций в онлайн-торговле как потенциальную угрозу увеличения активности мошенников. Почти столько же предприятий (51%) имеют трудности в мониторинге транзакций в разных странах и применении технологий, предназначенных для разоблачения мошенников. Это обусловлено языковым барьером и сложностью отслеживания достоверности личных данных покупателей из других стран.

Проанализируем наиболее распространенные схемы мошенничества.

1. Хищение личных данных

Одним из наиболее часто встречающиеся видов мошенничества в онлайн-торговле являются хищение личных данных (71%); «фишинг», трактуемый как попытка получения доступа к банковским счетам путем использования подложных идентификационных данных (66%); присвоение банковского счета (63%). В данных видах мошенничества целью является кредитная карта, так как транзакции, при которых не требуется физическое присутствие банковской карты, осуществляются практически мгновенно, а доступ к информации, необходимой для данной транзакции, получить относительно несложно. При хищении личных данных целью злоумышленника является проведение транзакций от имени другого человека. Мошенники перехватывают информацию о существующем человеке, находящуюся в открытом доступе, например, ФИО, адрес электронной почты, адрес прописки и фактический адрес проживания, а также на информацию о кредитной карте и банковских счетах. Владея подобной информацией можно заказывать товары от чужого имени и оплачивать их, указывая чужую кредитную карту.

«Фишинг» [3] для получения доступа к личным данным подразумевает рассылку сообщений на электронную почту, смс на телефоны.

«Фарминг» направляет пользователя по ложному адресу. Злоумышленник портит навигационную инфраструктуру и овладевает некоторой ее частью (локальная версия, система доменных имен). Для получения доступа к личным данным нужен часто только украденный пароль. Он позволяет завладеть уже существующим аккаунтом пользователя в онлайн-магазине, часто вся платежная информация уже хранится в аккаунте.

К хищению личных данных Относятся относятся и атаки хакеров на предприятия онлайн-торговли, с целью кражи личных данных покупателей, и установки вирусного программного обеспечения на компьютеры для получения доступа к конфиденциальной информации о пользователе [8].

Другим способом мошенничества является атака посредника. Информация о кредитных картах перехватывается при отправке сведений по электронной почте, копировании кредитных карт при пользовании в общественных местах [8] Для овладения аккаунтом пользователя хакер подключается к каналу связи между продавцом и покупателем, либо покупателем и банком.

2. «Дружественное мошенничество»

На четвертом месте по популярности среди видов мошенничества, согласно исследованию, расположилось «дружественное мошенничество». При данном виде мошенничества покупатели обычно заказывают товары или услуги и оплачивают их (предпочитая традиционные способы оплаты, такие как кредитные карты). Затем покупатели специально инициируют ситуацию, при которой им возвращаются деньги, ут-

верждая, что их кредитная карта или информация об их аккаунте была украдена. Соответственно, продавец выплачивает им компенсацию, но при этом товар или услугу покупатель также оставляет себе.

Одним из видов «дружественного мошенничества» является повторная отправка [3]. Мошенники, использующие украденные личные данные для совершения покупок, не указывают свой настоящий адрес, поэтому они привлекают посредников, чьи личные данные используются для совершения транзакции и которые затем перенаправляют товары мошенникам.

3) «Чистое мошенничество»

В данном случае название не отражает сути этого вида мошенничества, потому что на самом деле в нем нет ничего чистого. Основным принципом «чистого мошенничества» является совершение покупки украденной кредитной картой, но транзакция осуществляется таким путем, чтобы обойти технологии обнаружения мошенничества.

Этот вид мошенничества требует гораздо больше ноу-хау от мошенников, так как, в отличие от «дружественного мошенничества», в котором основной целью является получение денежной компенсации, после того как покупка уже совершена, в «чистом мошенничестве» преступники досконально анализируют технологии обнаружения мошенничества, применяемые предприятием, и затем используют максимально возможное количество личных данных о владельце украденной банковской карты. Личные данные полностью вводятся мошенниками правильно, чтобы сделать их обнаружение практически невозможным. Прежде чем совершается «чистое мошенничество», банковскую карту обычно тестируют. Эти тесты проводят в виде дешевых покупок в онлайн-магазинах с целью проверки правильности личных данных владельца украденной карты и ее действительности.

4. Мошенничество с партнерской программой

Мошенничество с партнерской программой может быть реализовано в виде двух схем, и обе направлены на то, чтобы нелегальным путем заставить партнерскую программу выплачивать больше денег. Это достигается с помощью управления траффиком или статистикой регистрации на сайте онлайн-магазина. В некоторых случаях это полностью автоматизированный процесс, в остальных случаях нанимаются люди, для регистрации большого количества искусственных аккаунтов. Способ оплаты не важен.

5. Мошенничество со схемой в виде треугольника

В данном виде мошенничества задействовано три точки [2]. Первая — искусственный онлайн-магазин, в котором популярные товары товары продаются по низкой цене. Фальсифицированный онлайн-магазин просто собирает адреса и информацию о банковских картах — это его единственная цель.

Второй вершиной данного треугольника является использование похищенной информации о кредитной карте и ФИО реального человека, чтобы заказать товары в настоящем онлайн-магазине и отправить их покупателю.

Третьей вершиной данного треугольника является использование похищенной информации о кредитной карте с целью совершения дополнительных покупок, которые мошенники затем присваивают себе. Информацию о заказе не всегда можно связать с номером кредитной карты, поэтому данная схема может долгое время оставаться нераскрытой, что ведет к большим убыткам для покупателей и онлайн-магазинов.

6. Мошенничество под видом продавца

Мошенники продают товары по низким ценам, но не отправляют их покупателям, вырученные деньги присваивают. Способ оплаты не важен, но в основном используются способы, не предусматривающие возврата денег. Этот вид мошенничества существует и в оптовой торговле [11].

Методы по предотвращению мошенничества в онлайн-торговле

В опросе участвовали предприятия из 14 стран [4]. 58% участников исследования называют главной задачей по предотвращению мошенничества в онлайн-торговле – создание интегрированной системы, которая была бы способна предоставить предприятиям детальный обзор всех их транзакций во всех экономических сегментах, дифференцированный по странам.

Способы мошенничества зависят от каналов сбыта продукции. Согласно опросу 69% участников исследования [4], продажи через сайты-посредники (eBay, AliBaba, Amazon), также частично подвержены мошенничеству. 64% предприятий среди подверженных мошенничеству каналов сбыта выделили продажи через мобильные приложения, а 55% назвали продажи через собственные онлайн-магазины.

В 2018 году, как было упомянуто ранее, количество транзакций с участием мошенников выросло почти на 30%. Согласно прогнозам аналитических агентств в области онлайн-торговли, активность мошенников в 2019 году должна только увеличиться. Однако разрабатываются инструменты, с помощью которых предприятия онлайн-торговли могут бороться с мошенниками. Это специально разработанные программы, которые отслеживают подозрительные транзакции и страхуют предприятия от несения убытков в связи с деятельностью мошенников.

Программы по борьбе с мошенничеством в онлайн-торговле в основном работают по одному и тому же принципу [5] (см. рис. 1). Предприятие автоматически перенаправляет детали заказа программе. Она анализирует факторы риска данной транзакции и присылает ответ либо в форме шкалы риска, либо в форме «отклонить/одобрить транзакцию». Чтобы обнаружить потенциальную

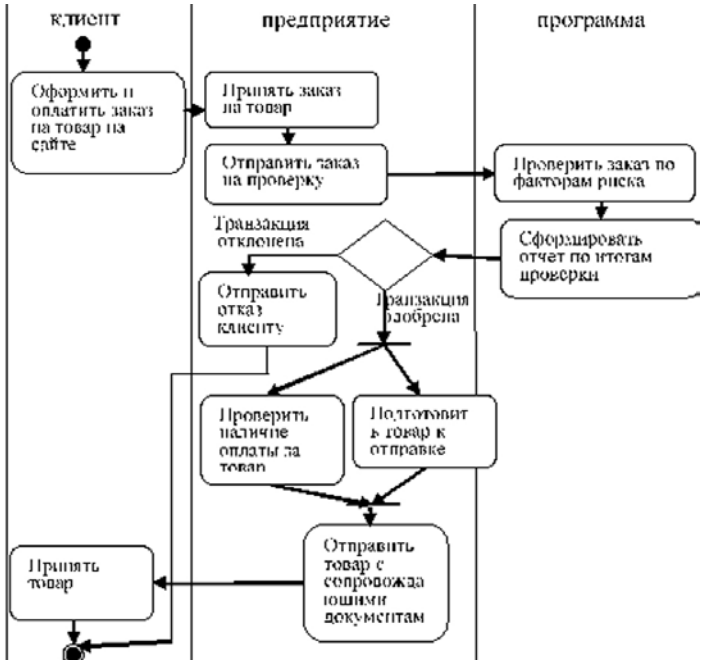

Рис. 1. Диаграмма деятельности «Проверка заказов на мошенничество»
Fig. 1. Activity diagram of the «Check orders for fraud»

финансовую махинацию, анализируется несколько предостерегающих факторов, например, несовпадение адреса доставки и платежного адреса, повторные заказы одного и того же товара, заказы на большую сумму из других стран.

Проанализируем несколько основных технических характеристик работы программ по отслеживанию подозрительных транзакций.

1. Самообучаемость — в режиме реального времени программа получает информацию о нелегальных транзакциях, что позволяет благодаря самообучающейся модели мгновенно распознать мошенничество. По сравнению с проверкой транзакций вручную, программа работает быстрее и охватывает более широкий диапазон предупреждающих о потенциальном мошенничестве сигналов.

2. Автоматизированный рабочий поток — для ускорения рабочего потока предприятие может автоматизировать отслеживание транзакций с нелегальной оплатой, отправку деталей заказа, блокировку подозрительных устройств, отмену подозрительных заказов и т. д.

3. 3. равило, отчеты о подозрительной активности предоставляются единым информационным блоком, это означает, что предприятию не нужно переключаться с одного приложения на другое. Это существенно упрощает процесс мониторинга подозрительной активности.

4. Гарантия денежной компенсации — в случае одобрения нелегального заказа данной программой, ее создатели обязуются покрыть все убытки, понесенные предприятием по нелегальному заказу. Это делает инвестицию в программу практически лишенной риска для предприятия.

5. Система аутентификации по устройству позволяет предотвратить мошенничество, так как анализирует массивы данных, включающие в себя браузер, операционную систему, язык и местоположение заказчика. С помощью этих данных система определяет отношение устройства, с которого сделан заказ, к преступной деятельности. Если обнаруживается подозрительная активность, система автоматически блокирует данный заказ.

6. Кастомизация — программы по борьбе с мошенничеством позволяют подобрать индивидуальные для каждого предприятия критерии мониторинга способов оплаты и личных данных пользователей.

7. Поддерживаемые платформы — инструменты по предотвращению нелегальных транзакций создают собственные шаблоны, которые позволяют отслеживать подозрительную активность при регистрации в онлайн-магазинах.

Программы по предотвращению мошенничества в онлайн-торговле

Существует достаточно большое количество программ по предотвращению мошенничества в онлайн-торговле, среди них Simility, Subuno, Riskified, Signifyd, Forter, FraudLabs Pro, Trustev, DupZapper, Kount. Наиболее эффективными и популярными в настоящее время являются Signifyd и Simility. Рассмотрим работу этих программ.

Каждое решение, которое принимает программа Signifyd, представлено в виде счета, указывающего на качество заказа, и выражено в специальной числовой шкале. Программа позволяет автоматизировать техническую поддержку в том, что касается выполнения и отмены заказов. Таким образом, вместо ручного мониторинга подозрительной активности сотрудниками предприятия программа мгновенно распознает такую активность. Также программа гарантирует полную денежную компенсацию в течение 48 часов в случае одобрения нелегальной транзакции. При установке не вносит изменений в уже установленное программное обеспечение.

Simility — это программа, которая оценивает риск транзакции по характеристикам устройства, с которого был выполнен заказ. Эти характеристики включают в себя браузер, язык, геолокацию, операционную систему, имя пользователя, уровень заряда

Таблица 1. Сравнение программ по предотвращению мошенничества в онлайн-торговле.
Table 1. Comparison of fraud prevention programs in online trading

	Signifyd	**Simility**	**Subuno**	*Riskified*	*Forter*	**Trustev**
Машинное обучение	да	да	да	да	да	да
Автоматизированный рабочий процесс	да	да	да	да	да	да
Панель инструментов Insights	да	да	да	да	да	да
Гарантия возврата платежа	да	нет	да	да	да	нет
Кастомизация	да	да	да	да	да	да
Отпечатки устройства	да	да	нет	да	да	да
Поддерживаемые платформы	Shopify, Magento	любые (через API, но приложения недоступны)	Magento, PrestaShop, Shopify, WooCommerce, ZenCart	Magento, Shopify	Magento	любые
Цена	начиная с 1% от заказов	зависит от объема транзакции	от 19 долларов в месяц	зависит от объема транзакции	доступны по запросу	65.4
Бесплатный план	да	нет	нет	нет	нет	нет
Бесплатная пробная версия	да (14 дней)	да	да (30 дней)	нет	нет	нет

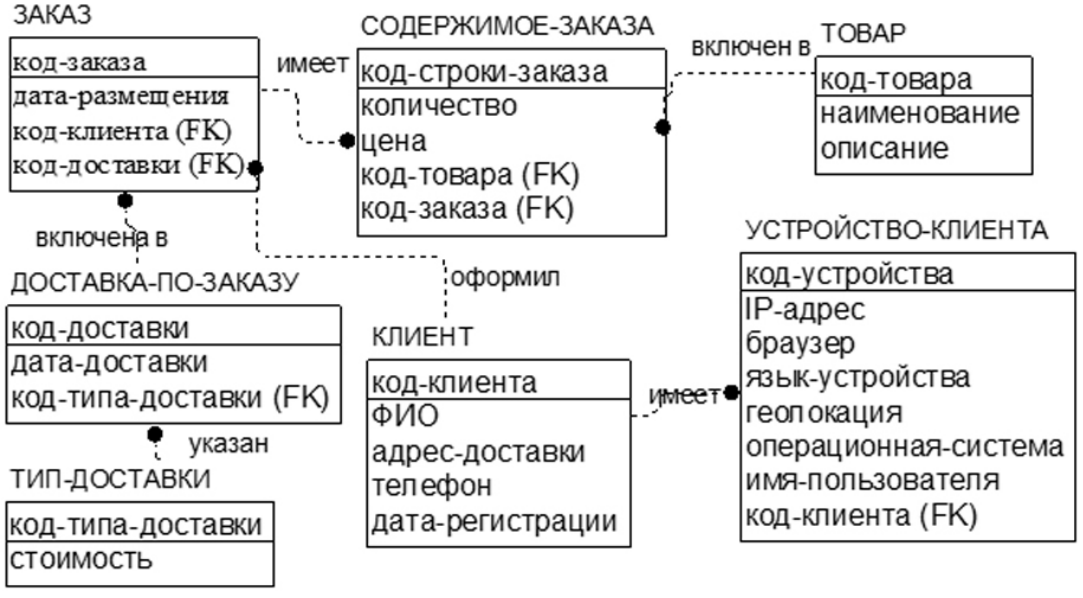

Рис. 2. Обобщенная структура базы данных
Fig. 2. Generalized structure of the database

аккумулятора и т. д. Даже если устройство не было занесено в черный список или является новым для данного канала сбыта продукции, программа вычислит мошенника благодаря самообучающемуся алгоритму. Когда характеристики устройства меняются, например, используется другой браузер или обновляется операционная система, программа может определить, принадлежат эти характеристики одному и тому же устройству или нет.

На рисунке 2 отражены сведения, которые должны накапливаться в программах по борьбе с мошенничеством [7].

Транзакции в онлайн-торговле могут содержать в себе сигналы, указывающие на потенциальную причастность мошенников к данным транзакциям. Ниже перечислено 10 сигналов с кратким описанием [1].

Если в транзакции присутствует всего пара таких признаков, то ее нельзя наверняка отнести к транзакции с повышенным риском, если же она объединяет в себе сразу несколько (от 5-6) таких признаков, то с очень высокой долей вероятности в этой транзакции замешаны мошенники.

1. Впервые заказывающие покупатели. Мошенники в онлайн-торговле обычно нацеливаются на сайты, на которых они до этого ничего не заказывали. Как только они совершают преступление, они сразу же переключаются на другой онлайн-магазин.

2. Заказы на суммы значительно выше среднего. Украденные банковские карты действительны короткий период времени, поэтому задачей мошенников является максимизация потраченной за одну транзакцию суммы.

3. Быстрая доставка. Большинство покупателей выбирает наиболее дешевые виды доставки. Но так как для мошенников деньги за доставку не являются предметом для беспокойства, они часто выбирают наиболее быстрый вид доставки, например, срочная доставка на следующий день после размещения заказа.

4. Необычное местоположение. Персоналу онлайн-магазинов следует особенно тщательно проверять заказы, которые приходят из стран, из которых ранее заказов не поступало. У таких заказов риск потенциальной связи с мошенниками значительно выше.

5. Большое количество одного определенного товара в заказе. Как и в случае с заказами на большую сумму, описанными выше, покупка большой партии какого-то определенного товара — это способ извлечь максимальную выгоду из похищенной банковской карты за короткий срок.

6. Совпадение адресов доставки. Совпадение адресов доставки у нескольких заказов, размещенных за небольшой промежуток времени, может служить индикатором того, что мошенники используют несколько похищенных банковских карт, каждая из которых оформлена на разных владельцев.

7. Адрес доставки / платежный адрес не совпадают с IP-адресом. Онлайн-магазинам необходимо проверять соответствие IP-адреса адресу доставки и платежному адресу. Если обнаруживается несоответствие, риск, что транзакция проводится мошенниками, выше.

8. Несколько банковских карт, проходящих по одному и тому же IP-адресу. Такие транзакции указывают на то, что сразу несколько заказов было размещено с одного и того же компьютера. При этом у таких заказов могут не совпадать личные данные и адреса доставки.

9. Странная орфография и пунктуация. Иногда мошенники полностью пишут заглавными буквами или ставят пробелы вместо запятых в целях экономии времени. Статистически подтверждено, что странно оформленные сообщения чаще имеют отношение к мошенничеству в онлайн-торговле.

10. Большое количество транзакций с одной и той же карты за короткий период времени. Это знак того, что преступник пытается потратить как можно больше денег с похи-

щенной банковской карты, пока ее владелец не заблокировал счет.

К сожалению, простого пути предотвращения мошенничества в онлайн-торговле не существует. Поэтому ответственность по отслеживанию мошенников также лежит и на персонале онлайн-магазинов.

Способы борьбы с мошенничеством в онлайн-торговле

Проанализируем несколько возможных способов борьбы с мошенничеством в онлайн-торговле [10].

1. Денежные потоки должны быть защищены на всех стадиях осуществления транзакции. Наиболее важными элементами являются счет-фактура и квитанция об оплате, содержащая личные данные покупателя. Защитой в данном случае выступает специальный криптографический код, написанный для предприятия и применяемый при обработке и передаче данных на его веб-сайте. Это создает дополнительный слой защиты от потенциальной атаки хакеров, тем самым гарантируя покупателям неприкосновенность личных данных.

2. Онлайн-магазинам помогают проверки интенсивности транзакций с целью анализа поведения покупателей. Если интенсивность транзакций существенно превышает норму, то это может указывать на хакерскую атаку посредством похищенных банковских карт. Иногда проверки интенсивности транзакций сопряжены с проверкой соответствия личных данных владельца карты, предоставленных во время оформления заказа, с личными данными, указанными в его социальных сетях, а также сопряжены с установлением лимита на одну транзакцию с определенной банковской карты в рамках заказа в онлайн-магазине. Проверки интенсивности транзакций сортируют транзакции по географическому признаку, что автоматически делает заказы из стран, из которых ранее заказов не поступало, более подозрительными. Обычно в таких случаях заказы блокируются для дальнейшей проверки вручную сотрудниками онлайн-магазина. При проверке вручную сотрудник может связаться по электронной почте или по телефону с заказчиком и попросить его подтвердить личные данные или проверить, была ли ошибка в несовпадении платежного адреса и адреса доставки. Онлайн-магазинам важно уточнять такие детали, поскольку для покупателей такая дополнительная проверка не займет много времени и лишь повысит доверие к онлайн-магазину.

3. Проверка на предыдущие отказы в совершении платежа с банковской карты. Бывают случаи, когда карта использовалась несколько раз и неизменно поступал отказ в совершении платежа. При этом карта может использоваться в конце своего срока действия и может быть авторизована/одобрена. В любом случае большое количество отказов по операциям с банковской карты может указывать на потенциальную хакерскую атаку. Поэтому онлайн-магазину необходимо проанализировать транзакции, по которым владельцу банковской карты поступил отказ в осуществлении.

4. 3-D защита, например, код безопасности MasterCard или VbV (Verified by Visa), является наиболее эффективным способом предотвращения мошенничества в онлайн-торговле. Двухуровневая система аутентификации при совершении каждой транзакции служит барьером для мошенников. При двухуровневой системе аутентификации магазин не несет ответственности в случае одобрения транзакции, проведенной мошенниками, и соответственно не выплачивает покупателю компенсацию.

5. Анализ данных, предоставляемых ежедневно программами SAFE и TC40. Эти данные помогают отслеживать любые подозрительные паттерны, связанные с банковскими операциями. При этом они не нарушают политику конфиденциальности компаний Visa и MasterCard.

6. Обратная связь от покупателей. Опыт столкновения с мошенниками может оказаться полезным. Если покупатель предупреждает онлайн-магазин о потенциальной атаке хакеров/транзакции с участием мошенников, он делает это, чтобы помочь, поэтому онлайн-магазинам не стоит игнорировать такие заявления.

Методы защиты от мошенничества в онлайн-торговле

Рассмотрим несколько способов защитить бизнес в онлайн-торговле от мошенничества [9].

1. Задержка заказов. Онлайн-магазин может создать специальный отдел, который будет вручную заниматься задержкой заказов. Критерием задержки может являться сумма заказа, например, дополнительной проверке будут подвергаться заказы на сумму, превышающую 250 долларов, в праздники, если бизнес сезонный, сумму, при которой заказы будут подвергаться дополнительной проверке, можно повысить до 500 долларов.

2. База данных с заказами, в которых были задействованы мошенники, внутри онлайн-магазина. Такие заказы можно сортировать по адресу доставки, номеру банковской карты или личным данным заказчиков. Прежде чем подтвердить заказ, онлайн-магазин сможет пробить его по уже существующей базе данных.

3. Совместная база данных с заказами, в которых были задействованы мошенники. Подразумевается объединение нескольких онлайн-магазинов, представленных в одном и том же экономическом сегменте, с целью создания единой базы данных, в которую будут помещены все заказы, сделанные мошенниками. Проверка заказа через такую базу данных существенно снизит риск для онлайн-магазина быть обманутым мошенниками.

4. Телефонная база данных. Использовать телефонные справочники, чтобы сверять данные, предоставленные заказчиком, с данными, указанными в справочниках. Такой сервис предоставляется многими веб-сайтами.

5. Банк-эмитент. Онлайн-магазин может напрямую связаться с банком, который производит транзакцию по банковской карте заказчика, чтобы сверить личные данные и адрес доставки, указанный заказчиком. При этом онлайн-магазину необходимо будет назвать все данные о бизнесе (регистрационный номер, ИНН, историю операций), которые потребует банк.

6. Связаться с покупателем напрямую. Если при заполнении формы заказа покупатель указал действительный телефонный номер, для подтверждения личных данных и адреса доставки онлайн-магазину достаточно позвонить покупателю и сверить информацию по заказу.

7. Запись всех разговоров с клиентами. Если продукция будет утеряна вследствие деятельности мошенников, запись телефонного разговора с покупателем, оформившим заказ, может оказаться полезной. Онлайн-магазинам рекомендуется документировать разговоры (отдельно выписывать все личные данные заказчика) и записывать все входящие звонки.

8. Законодательные акты, преследующие мошенничество в онлайн-торговле. Онлайн-магазинам рекомендуется помещать на своих сайтах вырезки из законодательных актов, в которых будет прописано наказание за те или иные виды мошенничества, чтобы это служило предостережением. Формулировка может отличаться в зависимости от страны, в которой зарегистрирован онлайн-магазин.

Чем больше характеристик охватывает система защиты и чем сложнее система аутентификации, тем больше вероятность предотвратить мошенничество в онлайн-торговле. Использование ранее упомянутой 3-D защиты может снизить вероятность совершения транзакции, в которой будут замешаны мошенники, на 90%.