Угрозы онлайн-мошенничества в страховании

Андрей Бусаргин
Директор направления Brand Protection, Group-IB

О компании

Group-IB — одна из ведущих международных компаний по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий

1000+

успешных расследований по всему миру, 150 особо сложных уголовных дел

$300 млн

возвращено клиентам Group-IB благодаря нашей работе

Официальный партнер Europol и Interpol

Рекомендована Организацией по безопасности и сотрудничеству в Европе (ОБСЕ)

Постоянный член Всемирного экономического форума

Threat Intelligence от Group-IB – в числе лучших мировых систем по оценке Forrester и Gartner

Одна из 7 самых влиятельных компаний в области кибербезо-пасности по версии Business Insider

Лидер российского рынка по исследованию киберугроз

О нас говорят:

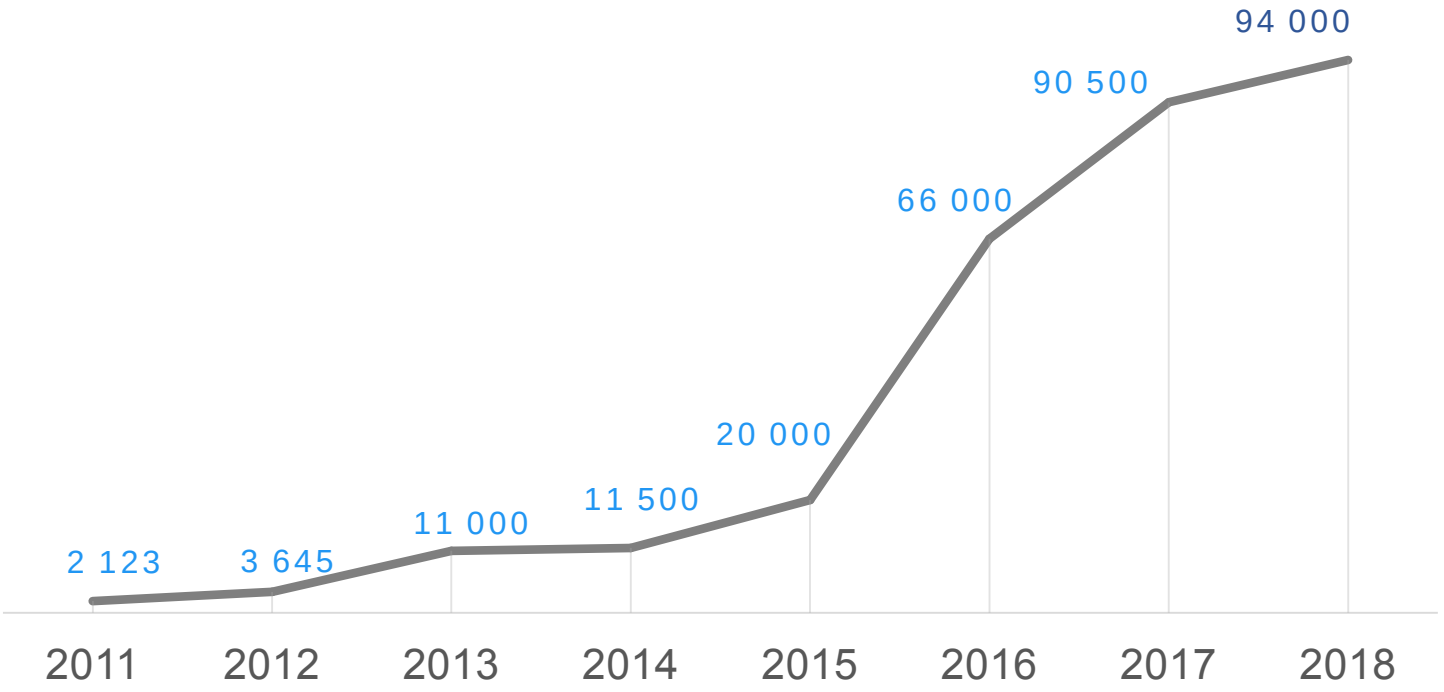
theguardian Bloomberg Forbes REUTERS Esquire

ПЕРВЫЙ КАНАЛ РОССИЙСКАЯ ГАЗЕТА ИЗВЕСТИЯ ВЕДОМОСТИ РОССИЯ 1 Коммерсантъ

Решения Group-IB

Защита бренда – одно из приоритетных направлений технологического развития компании

Преступления с использованием компьютерных и телекоммуникационных технологий



по данным Генеральной прокуратуры и МВД РФ

Необходимость защиты присутствия страховых компаний в интернете. Предпосылки

При выборе страховки пользователи анализируют онлайн ресурсы

71%

Опрошенных потребителей используют **онлайн инструменты** для выбора страховки

Мобильные приложения набирают популярность среди ваших клиентов

68%

Опрошенных хотели бы использовать **мобильное приложение своего страховщика**

Обманутые пользователи с легкостью отдадут свои данные мошенникам

50%

Опрошенных готовы **делиться информацией о своей жизни**, если это позволит подобрать лучшие страховые предложения

Пользователи приобретают страховку в интернете

26%

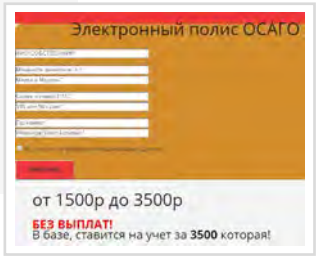
Опрошенных потребителей **купили полис через интернет или мобильное приложение**

Источник: PWC, Риски онлайн бизнеса в страховании

Типы монетизации онлайн-мошенничества в страховой индустрии

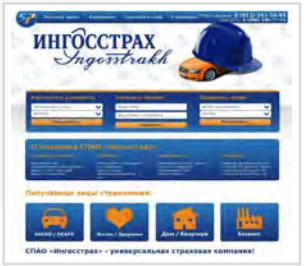
Приём платежей на мошеннические счета

Обманутый потребитель переводит денежные средства мошенникам. Далее он получает настоящий страховой полис, который однако будет недействительным, так как в страховую компанию деньги не поступали.



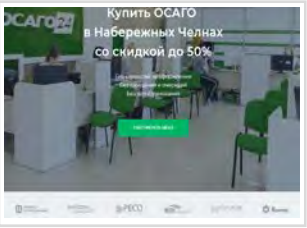
Приём платежей за продажу поддельных полисов

Мошеннические сайты собирают заказы и просят предоплату. В итоге потребитель получает фальшивый страховой полис.



Раскрутка собственных сторонних сервисов

Многие злоумышленники используют бренды страховых компаний для раскрутки собственных сайтов, привлечения на них трафика и платежей пользователей.



Захват связки логинов и паролей, данных банковских карт

Фишинговые сайты создаются, чтобы невнимательные пользователи оставили связку ключей злоумышленнику.

Атаки могут происходить массово или таргетированно.

Последствия онлайн-мошенничества для страховых компаний

Упущенная прибыль

Клиенты переводят мошенникам денежные средства, которые собирались потратить на сервис вашей компании.

Потеря клиентов

Потенциальные клиенты покупают поддельные полисы, а негатив и жалобы обращают в сторону компании, чей бренд был незаконно использован. Как следствие, возникает риск необходимости выплат компенсаций и отработки жалоб.

Репутационные потери

Сервисы, полученные пользователями от «ложного партнёра», с большой вероятностью могут оказаться ненадлежащего качества. Что может нанести репутационный ущерб компании, чей бренд был использован мошенниками.

Утечки

Фишинговые сайты становятся причиной утечки персональных данных сотрудников и клиентов/потенциальных клиентов компании в Сеть.

Это также негативно сказывается и на репутации компании.

Все действия злоумышленников являются финансово мотивированными.

После столкновения с мошенничеством 64% пользователей больше не вернутся к бренду.

Инструменты действий злоумышленников

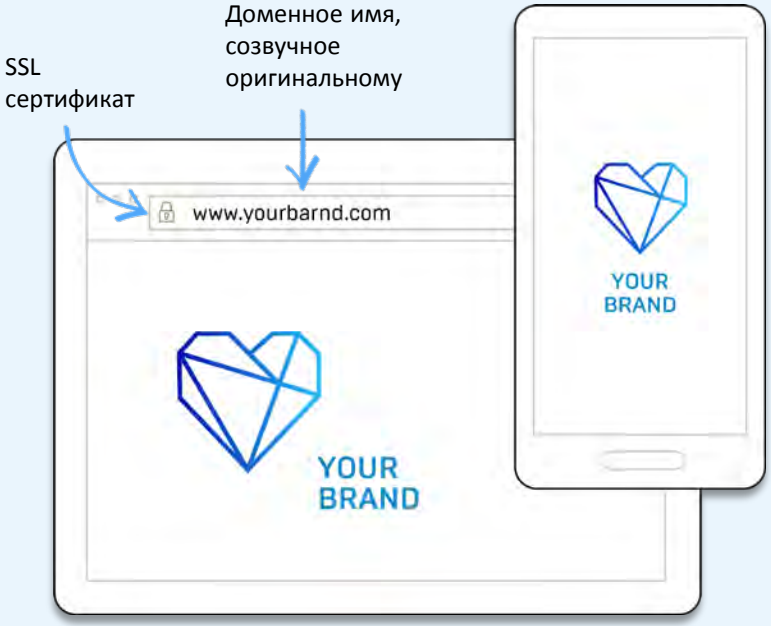
Риски
Потеря выручки
Потеря клиентов и сотрудников
Репутационные потери
Утечки

Тип монетизации	Инструменты
Прием платежей на поддельные реквизиты с помощью сайтов-клонов	Поддельные сайты, мобильные приложения, аккаунты в социальных сетях
Рассылки клиентам и сотрудникам с поддельных e-mail адресов	Мошеннические сайты, мобильные приложения фальшивые промо-акции
Захват связки логинов и паролей	Фишинг
Раскрутка собственных сторонних сервисов	Ложное партнерство, неправомерное использование товарного знака

Как преступники монетизируют ваш бренд

СОЗДАНИЕ ПЛОЩАДКИ

- Логотип, товарные знаки
- Название
- Фирменные цвета



ПРИВЛЕЧЕНИЕ ТРАФИКА

Поисковая оптимизация (SEO)

Спам
- по e-mail
- в мессенджерах

Реклама
- контекстная
- баннерная
- в соцсетях
- через Adware

Продвижение в соцсетях
- с помощью поддельных аккаунтов бренда
- разгон ботами
- через лидеров мнений

Секреты эффективного реагирования

МОДЕРАТОРСКИЕ АККАУНТЫ И ВЫСТРОЕННЫЕ ОТНОШЕНИЯ С КРУПНЫМИ ПЛОЩАДКАМИ

Мгновенное устранение нарушений через интерфейс / ускоренное рассмотрение запросов администраторами крупных площадок.

Растущая сеть партнеров, заинтересованных в борьбе с мошенниками

САМАЯ БЫСТРАЯ БЛОКИРОВКА В .РУ/.РФ И НАЦДОМЕНАХ

Компетентная организация КЦ RU / РФ в блокировке фишинговых и вредоносных ресурсов – снятие доменов с делегирования по обращениям Group-IB происходит в приоритетном порядке.

Компетентная организация КЦ РУ/РФ, партнер Фонда развития Интернет

РЕПУТАЦИЯ СРЕДИ ПРЕСТУПНИКОВ

Многие мошенники знают о Group-IB и понимают, что мы можем привести их на скамью подсудимых. Осознание неизбежности наказания существенно повышает эффективность всех мер реагирования.

Официальный партнер Interpol и Europol

ОПЕРАТИВНОЕ РЕАГИРОВАНИЕ В 1000+ ДОМЕННЫХ ЗОН

Прямые контакты с регистраторами доменных имен и хостинг-провайдерами, взаимодействие с Центрами реагирования по всему миру.

Авторизованный член международных сообществ команд реагирования

Зачем нужно защищать свой бренд в Интернете

Возвращение трафика

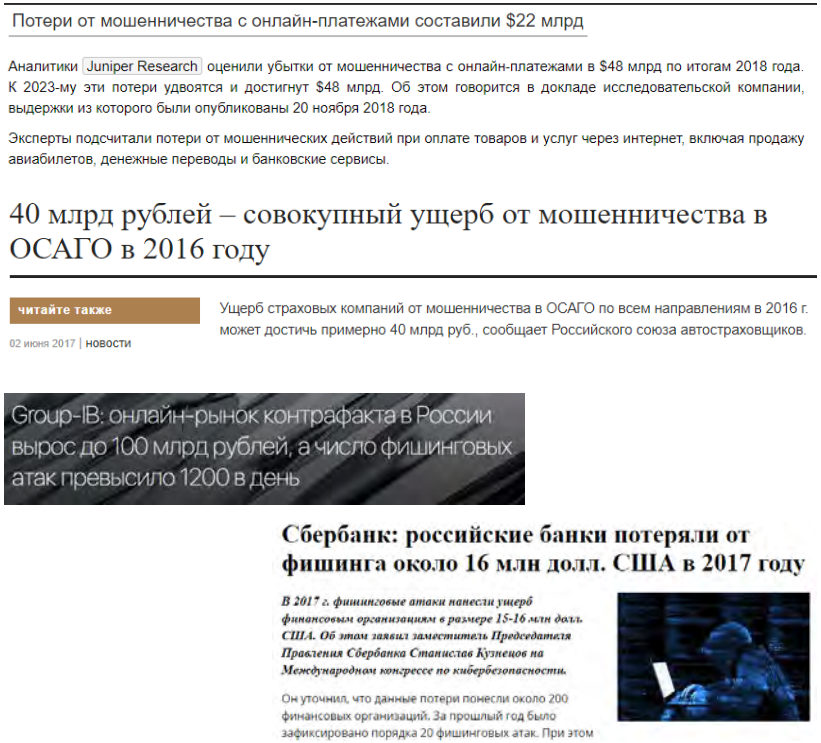
на официальные ресурсы после блокировки ресурсов злоумышленников, которые перехватывают до 50% аудитории.

Увеличение выручки

в результате блокировки ресурсов злоумышленников, собирающих с обманутых пользователей платежи.

Предотвращение потерь

минимизация рисков возврата денежных средств, юридических и судебных издержек, а также репутационных потерь.



Потери от мошенничества с онлайн-платежами составили $22 млрд

Аналитики Juniper Research оценили убытки от мошенничества с онлайн-платежами в $48 млрд по итогам 2018 года. К 2023-му эти потери удвоятся и достигнут $48 млрд. Об этом говорится в докладе исследовательской компании, выдержки из которого были опубликованы 20 ноября 2018 года.

Эксперты подсчитали потери от мошеннических действий при оплате товаров и услуг через интернет, включая продажу авиабилетов, денежные переводы и банковские сервисы.

40 млрд рублей – совокупный ущерб от мошенничества в ОСАГО в 2016 году

читайте также

02 июня 2017 | новости

Ущерб страховых компаний от мошенничества в ОСАГО по всем направлениям в 2016 г. может достичь примерно 40 млрд руб., сообщает Российского союза автостраховщиков.

Group-IB: онлайн-рынок контрафакта в России вырос до 100 млрд рублей, а число фишинговых атак превысило 1200 в день

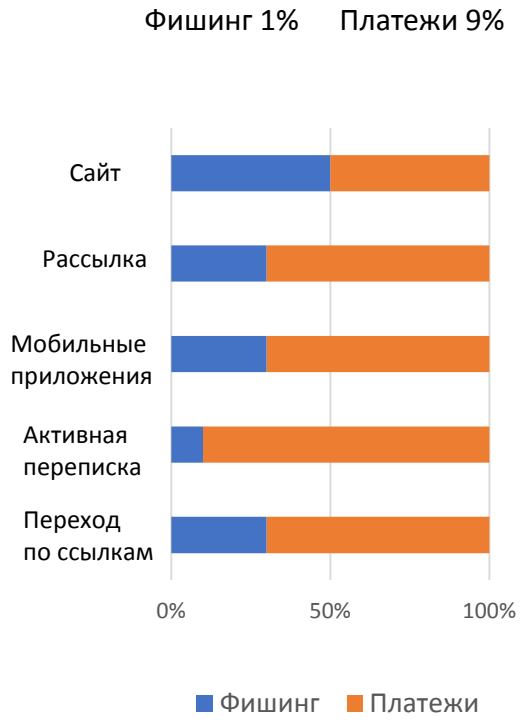
Сбербанк: российские банки потеряли от фишинга около 16 млн долл. США в 2017 году

В 2017 г. фишинговые атаки нанесли ущерб финансовым организациям в размере 15-16 млн долл. США. Об этом заявил заместитель Председателя Правления Сбербанка Станислав Кузнецов на Международном конгрессе по кибербезопасности.

Он уточнил, что данные потери понесли около 200 финансовых организаций. За прошлый год было зафиксировано порядка 20 фишинговых атак. При этом

Сколько зарабатывают злоумышленники в год. Страхование. Аудитория.

Ресурс	Трафик	Конверсия	Аудитория мошеннического ресурса
Сайт	614 496 среднее количество поисковых запросов связанных с компанией	14%	86 029 человек попадут на сайт злоумышленника
Рассылка	100 000 человек состоит в списках рассылок злоумышленников	20%	20 000 человек откроют сообщения злоумышленников
Мобильные приложения	1 000 количество скачиваний неофициальных мобильных приложений	100%	1 000 количество скачиваний неофициальных мобильных приложений
Активная переписка	7 920 состоит в неофициальных ресурсах социальных сетей	150 в день	54 750 начнут переписываться со злоумышленником
Переход по ссылкам		5%	396 перейдут по ссылкам в постах и комментариях



Сколько зарабатывают злоумышленники в год. Страхование. Заработок.

Потенциальные пострадавшие	Фишинг 1% от:		Платежи 9% от:	
86 029 попадут на сайт злоумышленника	50%	43 015	50%	43 015
20 000 откроют сообщения злоумышленников	30%	6 000	70%	14 000
54 750 начнут переписку со злоумышленниками	30%	16 425	70%	38 325
396 перейдут по ссылкам в постах и комментариях	10%	40	90%	356
1 000 количество скачиваний неофициальных мобильных приложений	30%	300	70%	700

Средний чек

Фишинг: 70 000 ₽
Платежи: 10 000 ₽

Потери

Фишинг: 46 045 524,00 ₽
Платежи: 86 756 508,00 ₽

65 779

Доверчивых:

658

96 396

Доверчивых:

8 676

Итоговые потери для страховых компаний

Прямые потери: 86 756 508,00 ₽

РАБОТА С ОБРАЩЕНИЯМИ:		
Чистые затраты	75 000 ₽/мес	900 000,00 ₽

Суммарные прямые потери:

87 656 508,00 ₽

Косвенные потери: 46 045 524,00 ₽

Стоимость компании	70 000 000 000
Гудвил	3 900 000 000
Вероятность попадания инцидента в СМИ	5%
Падение Гудвил	5%

Потеря капитализации:

9 750 000,00 ₽

УНИКАЛЬНАЯ ЭКСПЕРТИЗА

Передовые технологии мониторинга и анализа активности киберпреступников

Собственная система сбора данных о киберугрозах (threat intelligence) позволяет нам видеть IT-инфраструктуру злоумышленников, использующих ваш бренд

Одна из самых высокотехнологичных threat intelligence систем в мире

Forrester
Vendor Landscape:
External Threat Intelligence
2017

Один из ведущих поставщиков threat intelligence в мире

Cyber Defence
Magazine
Vendor Landscape:
Global Threat
Intelligence

ОЩУТИМЫЙ ROI

Быстро достигаем значимого результата, прицельно блокируя инфраструктуру преступников, приносящих максимальный ущерб

16 лет опыта расследования киберпреступлений

Собственный Центр реагирования 24/7/365

Репутация и контакты Центра реагирования CERT-GIB обеспечивают высокую эффективность устранения нарушений в досудебном порядке

85% нарушений устраняется в досудебном порядке

НАМ ДОВЕРЯЮТ

СБЕРБАНК

Microsoft

sochi.ru 2014

Group-IB защищала символику и билетную продукцию XXII Зимних Олимпийских игр в Сочи

АЭРОФЛОТ Российские авиалинии

Глобальная блокчейн-платформа Waves (рыночная капитализация $870 000 000+), выбрала Group-IB для защиты пользователей от фишинга

К НАМ ПРИСЛУШИВАЮТСЯ

GROUP-IB

ТАСС

Резидент "Сколково" защитил пассажиров "Аэрофлота" от действий мошенников

РИА НОВОСТИ

Выявлены новые уловки теневых сайтов по продаже алкоголя в России

banki.ru

Group-IB: мошенники заработали на сбое Telegram не менее $59 тыс

vc.ru

«Опасные» подарки к 8 марта: как определить мошеннический сайт и сохранить свои деньги

НАМ БЛАГОДАРНЫ


Microsoft


Тинькофф Кредитные Системы


AVITO.ru


Rostelecom


ecco


ПЕРВЫЙ КАНАЛ

Андрей Бусаргин
busargin@group-ib.com
+7 915 350 76 42

Предотвращаем и расследуем киберпреступления с 2003 года

www.group-ib.ru
blog.group-ib.ru

bp@group-ib.ru
+7 495 984 33 64

twitter.com/groupib
facebook.com/group-ib

t.me/group_ib
instagram.com/group_ib