KASPERSKY lab

ИССЛЕДОВАНИЕ РИСКОВ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ В РОССИИ 2014:

МУЛЬТИДЕВАЙСНЫЕ УГРОЗЫ В МУЛЬТИДЕВАЙСНОМ МИРЕ

Июнь, 2014

Содержание

Введение 2
Основные выводы 3
Методология 4
Глава 1. Использование разных устройств для выхода в Интернет 5
Глава 2. Активность пользователей онлайн 8
Глава 3. Данные, хранящиеся на устройствах, и отношение к ним 11
Глава 4. Киберугрозы, с которыми столкнулись пользователи, и их последствия 14
Глава 5. Отношение респондентов к вопросам кибербезопасности 17
Восприятие онлайн-угроз 17
Понимание ландшафта киберугроз 19
Понимание финансовых угроз 20
Отношение к паролям 22
Отношение к угрозам на работе 23
Глава 6. Дети онлайн: отношение родителей, инциденты и решения 25
Заключение 29

Введение

Распространение Интернета даже в самые дальние уголки Земли привело к тому, что сегодня каждый третий житель планеты является пользователем глобальной Сети. Однако, как и в реальном мире, в виртуальном пространстве существуют свои плюсы и минусы. И среди минусов – преступность.

Интернет – это источник киберугроз, которым подвержены как отдельные пользователи, так и крупные корпорации. Одни преступники планомерно атакуют крупные цели, другие предпочитают принцип «ковровой бомбардировки», собирая прибыль понемногу с большого количества жертв. При этом их усилия направлены на разные популярные операционные системы, и чем популярнее платформа, тем большее внимание киберпреступников она привлекает.

Характерно, что злоумышленники тщательно следят за тенденциями в области информационных технологий и оперативно создают новые способы незаконного доступа к чужим данным, учитывая как меняющиеся привычки пользователей, так и новые способы и устройства для выхода в Интернет.

Чтобы оценить отношение и готовность интернет-пользователей к онлайн-угрозам, «Лаборатория Касперского» совместно с международной независимой компанией B2B International регулярно проводит глобальные статистические исследования. В рамках этих исследований пользователи из разных стран, в том числе из России, отвечают на вопросы, касающиеся их знаний о современных киберугрозах и об инцидентах, с которыми им самим довелось столкнуться.

В этом году особое внимание было уделено таким потребностям современных пользователей Интернета, как защита личного онлайн-пространства, ценных финансовых и персональных данных, а также многоплатформенная защита. «Лаборатория Каперского» поставила себе целью выяснить, что более всего волнует интернет-пользователей сегодня и какие действия они предпринимают или планируют предпринять для своей защиты.

Ознакомиться с отчетом по предыдущему исследованию можно по ссылке.

Основные выводы

«Многоплатформенность» становится ведущим трендом:

- 69% опрошенных россиян используют несколько устройств на различных платформах;
- 14% выходят в Интернет с мобильных устройств;
- большинство российских пользователей – 95% – хранят потенциально уязвимую персональную информацию на всех своих устройствах, включая мобильные.

Пользователи доверяют устройствам свою личную жизнь, и это их волнует:

- 45% респондентов в России опасаются, что их персональные данные могут украсть;
- 52% пользователей переживают, что за ними могут незаметно следить на их устройствах через вебкамеру;
- 68% участников опроса хранят на устройствах особо конфиденциальную информацию и боятся, что кто-либо увидит ее.

Финансовые угрозы становятся все более актуальными:

- 79% российских пользователей совершают финансовые операции онлайн, при этом 41% использует для этого мобильные устройства;
- 30% респондентов столкнулись с той или иной финансовой угрозой онлайн;
- 76% опрошенных хотели бы, чтобы банки, платежные системы и онлайн-магазины предоставляли им специальные решения для защиты транзакций на всех устройствах, в том числе мобильных.

Дети являются наименее защищенной категорией пользователей Интернета, что представляет опасность и для их родителей:

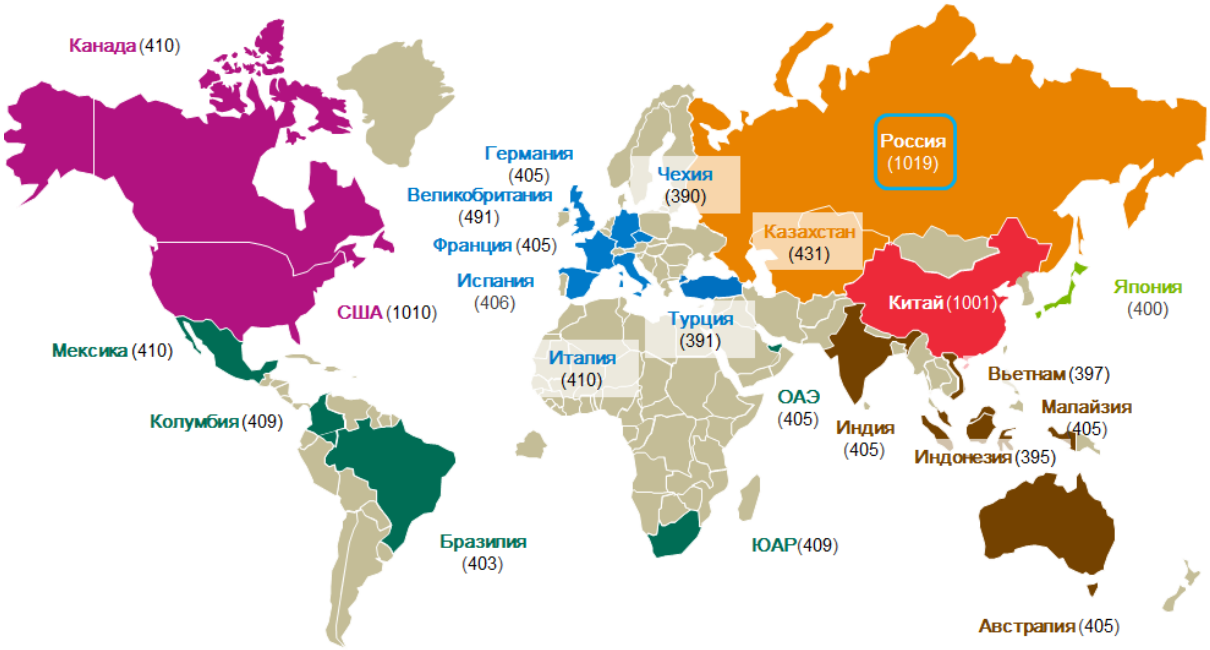
- 35% взрослых россиян считают, что количество онлайн-угроз для их детей растет, при этом 15% чувствуют, что не могут контролировать, что их дети видят или делают онлайн;
- за последние 12 месяцев дети 20% респондентов столкнулись с той или иной киберугрозой в Сети, а 14% потеряли данные или деньги взрослых.

Пользователи беспокоятся о киберугрозах, но мало делают для своей защиты:

- защитными решениями не оснащена почти половина компьютеров на базе Mac OS X и мобильных устройств на платформе Android;
- паролями не защищены более трети настольных компьютеров на базе Windows и более четверти смартфонов Android;
- почти половина респондентов не принимает никакие меры безопасности при пользовании бесплатными публичными Wi-Fi сетями.

Методология

Исследование проводилось посредством онлайн-опроса с мая по июнь 2014 года среди пользователей из 23 стран мира, в том числе из России:



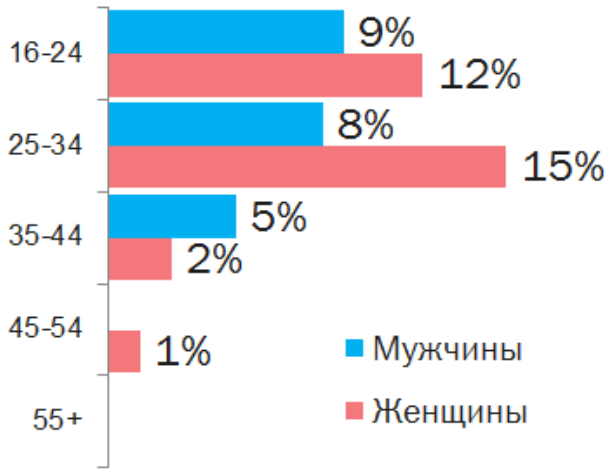
В общей сложности было опрошено 11135 человек в возрасте от 16 лет. В России было опрошено в Сети 1019 пользователей – 52 % из них мужчины и 48 % женщины. Четверть опрошенных в России представлена молодыми людьми до 24 лет, 24% пользователей оказались в возрасте от 25 до 34 лет, 20% – от 35 до 44 лет, и 31% – от 45 и старше.

Глава 1. Использование разных устройств для выхода в Интернет

В первую очередь участники опроса ответили, с каких устройств они выходят в Интернет. Выяснилось, что **69% респондентов используют одновременно несколько устройств на различных платформах**. При этом, если выяснять, с каких устройств они выходят в онлайн *большую часть времени*, оказывается, что 85% предпочитают традиционные компьютеры и ноутбуки, 7% – смартфоны, и 7% – планшеты.

Любопытно, что больше всего участников опроса, выбравших смартфон в качестве основного «окна» в Сеть, проживают на территории Ближнего Востока, Латинской Америки и Азии (до 27% респондентов из этих стран чаще всего выходят онлайн именно со смартфонов). На этом фоне Россия с показателем 7% занимает одну из самых последних строчек в рейтинге стран, попавших в выборку исследования.

Если же взглянуть на демографический аспект, то большинство россиян, выбравших «мобильный» формат, окажется среди молодых женщин в возрасте от 16 до 34 лет:

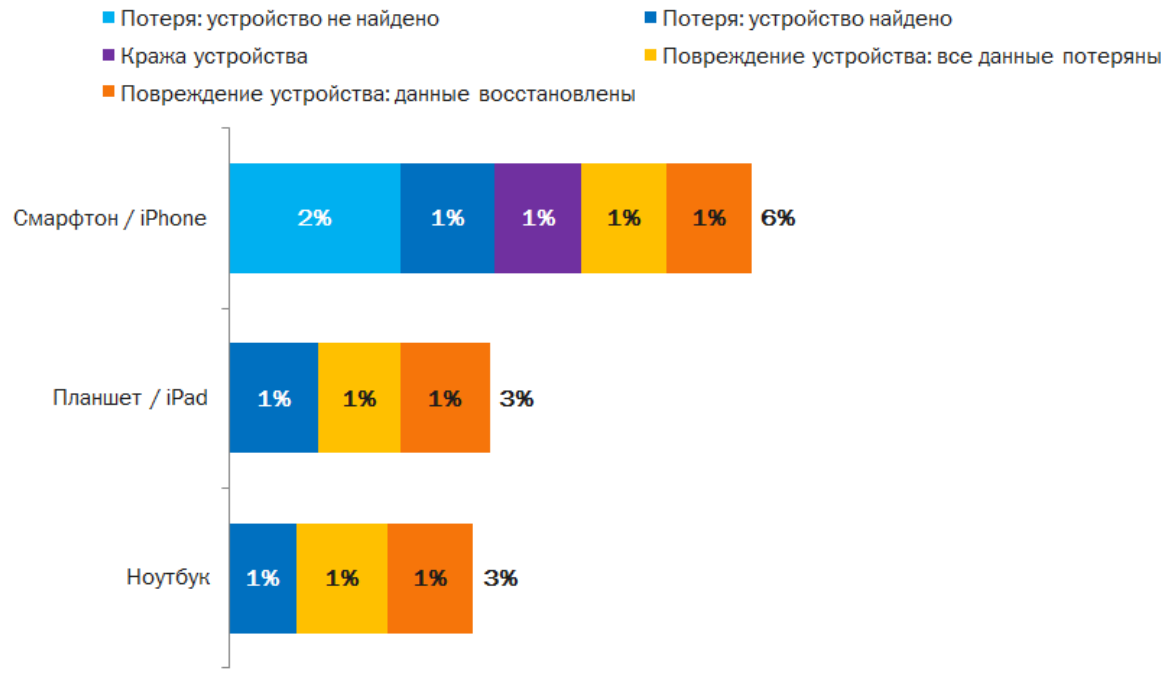


Исследование также показало, что, хотя пользователи выбирают различные устройства для доступа в Интернет, заботятся об обеспечении защиты от онлайн-угроз они далеко не для всех из них. Так, если 93% российских пользователей признают, что поставили защитное решение на свой компьютер на базе ОС Windows, то доля защищенных настольных компьютеров на базе Mac OS X составляет всего 41%, и лишь 56% респондентов отметили, что поставили защиту на свой Mac book. Не менее беспечны оказались и пользователи мобильных устройств – **только 59% планшетов и 54% смартфонов на платформе Android ограждены от киберугроз с помощью специального защитного решения**.

Но операционная система Windows, защите которой российские пользователи уделяют такое большое внимание, уже давно не является единственной целью злоумышленников. По данным облачной инфраструктуры Kaspersky Security Network, в

2014 году ежемесячно детектируется около 20 тысяч новых образцов вредоносного программного обеспечения под ОС Android, а обезвреженная некоторое время назад сеть ботов Flashback состояла более чем из 700 тысяч компьютеров под управлением Mac OS X. Кроме того, не стоит забывать и о кроссплатформенных угрозах, таких как условно законная сеть кибершпионажа компании Hacking Team, использовавшая шпионские модули для iOS и Android.

Однако не только киберзлоумышленники могут представлять опасность для данных, хранящихся на устройствах пользователя. Согласно опросу, устройства 12% респондентов в России за последний год были потеряны, украдены или сломаны.



Чаще всего неприятности такого рода случаются со смартфонами (6%), реже – с планшетами и ноутбуками (по 3%). При этом потеря или кража устройства, как правило, сопровождаются полной или частичной потерей данных, на них хранившихся.

45% российских пользователей, участвовавших в исследовании, признались, что ценят данные на устройстве больше, чем само устройство. А еще **68% опрошенных россиян сообщили, что некоторая хранящаяся на их устройстве информация настолько конфиденциальна, что они боятся, что кто-нибудь может увидеть ее**.

В связи с этим респондентов в России спросили, защищают ли они доступ к своим гаджетам, например, с помощью пароля (включая графический). 99% участников опроса, использующих компьютеры на платформе Mac OS X, применяют эту элементарную меру защиты. А вот **среди пользователей настольных ПК на базе Windows применение паролей встречается заметно реже – об этом сообщили всего 63% опрошенных**. Что касается российских пользователей смартфонов и планшетов Android, то «паролят» свои устройства 74% и 82% респондентов соответственно.

Вдобавок, согласно опросу, почти каждый третий россиян (а точнее 29%) делится своим личным устройством с другими членами семьи, еще 5% пользователей

доверяют свои устройства детям. При этом 37% таких респондентов не предпринимают никаких дополнительных действий для защиты устройства и/или данных на нем, так как не видят риска. Кстати, больше всего таких доверчивых пользователей в Японии – 44%, меньше всего – в Китае и странах Азиатско-Тихоокеанского региона (22%).

Однако совместное использование устройства таит в себе дополнительные опасности – владелец не может быть на 100% уверен в уровне компьютерной грамотности своих детей, домочадцев или друзей. То, что одному человеку кажется элементарной мерой предосторожности, другому может просто не прийти в голову. В итоге, общее устройство может сделать уязвимыми сразу нескольких пользователей.

Таким образом, опрос показывает, что подавляющее большинство россиян предпочитают для выхода в Интернет различные устройства на различных операционных системах, но мало заботятся об их защите. Такая беспечность ставит сохранность их данных и денег под угрозу, поскольку – как станет ясно из дальнейших глав – пользователи доверяют своим устройствам очень многое.

Глава 2. Активность пользователей онлайн

Российским респондентам предложили указать, чем они чаще всего занимаются онлайн и с каких устройств – в этом году список опций был расширен, чтобы охватить максимальное количество интересов пользователей. В связи с этим процент по некоторым активностям снизился по сравнению с прошлогодним опросом: это не означает, что пользователи стали выполнять указанные действия реже, но говорит о том, какие активности выполняются ими чаще и потому приходят на ум первыми. В целом, ответы получились следующими:

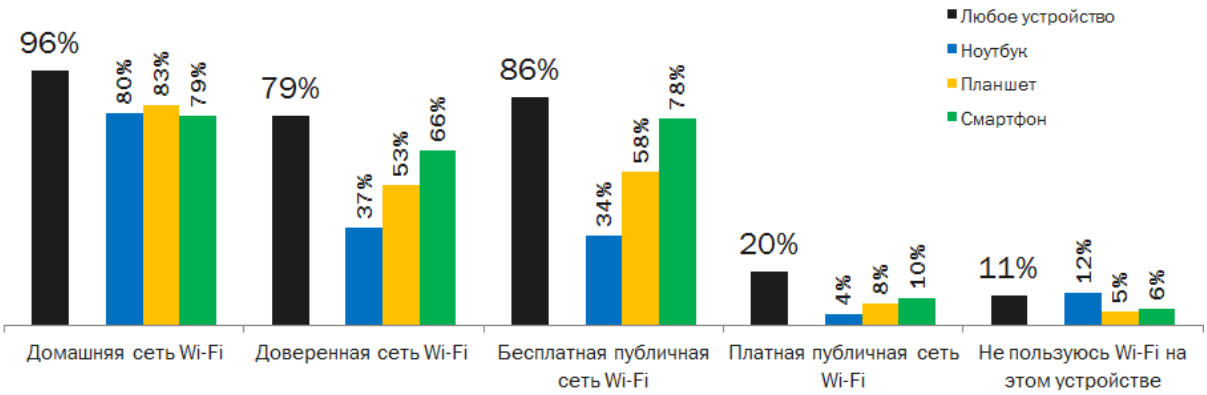
Активность	Любое устройство	Настольный ПК/Ноутбук	Планшет	Смартфон	Любое моб. устройство
Онлайн-шопинг	58%	56%	23%	12%	19%
Онлайн-банкинг	56%	53%	23%	22%	26%
Онлайн-игры	43%	38%	26%	14%	22%
Онлайн-казино / ставки	11%	9%	7%	4%	6%
Социальные сети	80%	75%	67%	67%	71%
Загрузка ПО / приложений	58%	51%	35%	32%	38%
Загрузка медиаконтента	70%	67%	27%	21%	27%
Онлайн-хранилища данных	24%	20%	13%	10%	13%
Выгрузка контента/данных для обмена	56%	52%	27%	26%	30%
Мессенджеры / видеозвонки	67%	60%	42%	45%	48%
Сайты для взрослых	19%	18%	10%	6%	8%
Платежные системы / электронные кошельки	44%	42%	17%	16%	19%
Сайты знакомств	14%	12%	7%	6%	7%
Просмотр фильмов / видео	70%	66%	49%	19%	38%
Прослушивание музыки / радио	68%	61%	49%	42%	50%
Электронная почта	84%	81%	57%	47%	56%
Обучение	39%	36%	22%	18%	23%
Работа	56%	53%	27%	21%	27%
Чтение новостей, статей, книг и т.д.	81%	74%	64%	56%	65%
Любая финансовая активность	**79%**	**77%**	**39%**	**35%**	**41%**
Любая активность	**100%**	**98%**	**99%**	**98%**	**99%**

Как видно из таблицы, электронная почта не теряет популярности у российских пользователей – 84% регулярно проверяют и отправляют письма со своих устройств. Второе место занимает чтение (81%), а третье место досталось социальным сетям (80%). Причем активность в социальных сетях с мобильных устройств оказалась выше – на первом месте, опередив и чтение, и электронную почту.

Те или иные финансовые операции со своих устройств (электронные платежи, покупки онлайн и т.д.) совершает 79% российских пользователей, при этом 41% выбирает для этого мобильные девайсы. Не меньше внимания мобильным платформам уделяют и киберпреступники: по данным облачной инфраструктуры Kaspersky Security Network, в которую поступает информация о киберугрозах со всего мира, количество вредоносных программ, созданных для кражи финансовых данных с устройств Android, за последний год выросло в 14 раз.

В связи с тем, что большинство современных устройств оснащены модулями беспроводной связи, и только в 2013 году, по данным ABI Research, в мире появилось более 4 миллионов свободных Wi-Fi зон, интересно было также узнать отношение

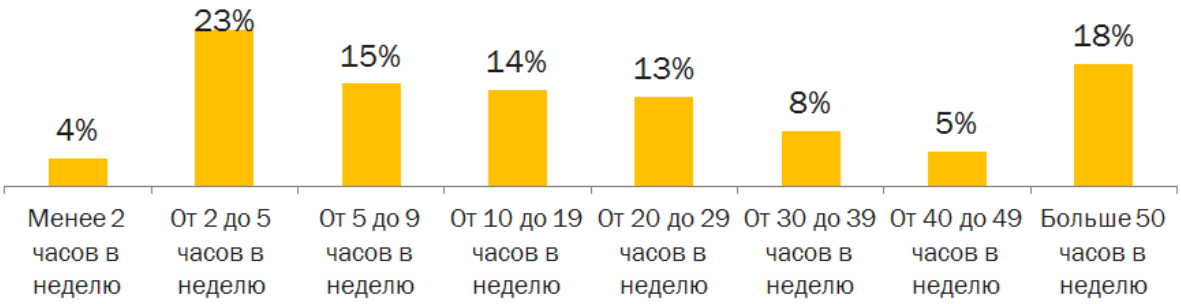
респондентов к использованию Wi-Fi соединения для решения своих задач онлайн. Опрос подтвердил, что подавляющее большинство россиян (89%) пользуются Wi-Fi, и этот процент еще выше для планшетов и смартфонов: 95% и 94% соответственно.



Значительно большинство респондентов в России (86%) регулярно пользуется бесплатными публичными Wi-Fi сетями, и наиболее активны в этом плане владельцы смартфонов (78%). Для сравнения, к подобным точкам доступа подключаются только 34% владельцев ноутбуков, и 58% пользователей планшетов. Это может быть связано с двумя факторами. Во-первых, гораздо быстрее и удобнее мимоходом подключиться к попавшейся бесплатной Wi-Fi сети со смартфона, в то время как планшет или ноутбук требуют больше времени на развертывание спонтанного рабочего места. Вторым фактором может быть понимание пользователями рисков, связанных с доступом к бесплатному Wi-Fi. Чтобы подтвердить или опровергнуть это предположение, респондентов спросили, предпринимают ли они в этих случаях какие-либо дополнительные меры защиты.

Выяснилось, что только 40% российских пользователей ограничивают свои онлайн-активности, когда подключаются к бесплатному Wi-Fi, еще меньше (9%) повышают уровень защиты в настройках устройства. В то же время **26% российских пользователей публичного Wi-Fi авторизуются в социальных сетях, почте и на прочих сайтах, а еще 4% совершают финансовые транзакции или покупки онлайн, подвергая тем самым риску свои данные (в том числе логины/пароли) и деньги.**

Участники опроса также рассказали, сколько времени они проводят в Сети *дома*: 38% российских пользователей блуждают по Интернету от 2 до 9 часов в неделю (около одного часа в день), 27% тратят на это от 10 до 29 часов в неделю, а 31% – более 30 часов (свыше 4 часов в сутки). При этом, когда речь заходит о нахождении в Сети более 50 часов в неделю, Россия оказывается абсолютным лидером в этом сегменте – 18% российских пользователей (и это наибольший показатель среди всех стран, участвовавших в исследовании) находятся в Сети свыше 7 часов в сутки.



При столь активном использовании возможностей Интернета и его многочисленных сервисов на устройствах пользователей неизбежно оказываются данные, часть из которых можно классифицировать как критичные для безопасности, о чем пойдет речь в следующей главе.

Глава 3. Данные, хранящиеся на устройствах, и отношение к ним

Исследование показало, что **95% российских пользователей хранят на своих устройствах какую-либо приватную информацию**, кража или потеря которой может представлять серьезный риск. Четверть респондентов (24%) хранит финансовые данные (банковские или платежные реквизиты, PIN-коды), а 41% – логины и пароли для доступа к почте, социальным сетям и другим профилям.

Данные	Любое устройство	Планшет	Смартфон	Настольный ПК / Ноутбук
Фото / видео / музыка	88%	71%	74%	83%
Личные файлы	75%	40%	30%	72%
Рабочие файлы	66%	29%	18%	65%
Личные сообщения по электронной почте	62%	39%	33%	58%
Адресная книга / список контактов	56%	25%	72%	19%
SMS или MMS	46%	21%	71%	0%
Рабочие сообщения по электронной почте	44%	27%	20%	41%
Пароли от личных онлайн-аккаунтов	29%	15%	12%	25%
Пароли от личных аккаунтов электронной почты	28%	14%	11%	25%
Конфиденциальная / личная информация	28%	10%	12%	24%
Пароли от рабочего аккаунта электронной почты	19%	9%	8%	16%
Другие платежные данные	15%	4%	6%	12%
Другие банковские данные	15%	6%	7%	11%
PIN-коды / пароли от онлайн-банкинга и т.п.	11%	5%	9%	6%
Пароли доступа к рабочему VPN / интранету	9%	4%	4%	8%
Любые финансовые данные	**24%**	**10%**	**15%**	**19%**
Любые пароли от аккаунтов	**41%**	**23%**	**24%**	**35%**
Любая личная информация	**95%**	**85%**	**93%**	**92%**

Примечательно, что финансовые данные, логины и пароли чаще хранятся на традиционных компьютерах. Однако процент пользователей, которые содержат ценные для киберпреступников сведения (финансовые данные и пароли к своим аккаунтам) на мобильных устройствах, тоже довольно велик. И в то же время именно смартфоны, как было показано в предыдущих главах, чаще всего оказываются незащищенными от проникновения.

Согласно опросу, для самих пользователей важнее всего их медиа-файлы (52% респондентов в России выбрали именно этот вариант), на втором и третьем месте – личные (41%) и рабочие (32%) документы. Настораживает тот факт, что банковские данные встречаются только на десятом месте (7%), в то время как о ценности других платежных данных задумалось всего лишь 4% опрошенных россиян. Такая статистика говорит о том, что большинство пользователей недооценивают существующие финансовые угрозы.

Несмотря на то, что ценные воспоминания и плоды интеллектуального труда для пользователей в приоритете, только 13% из них подтвердили, что создают резервные копии всех своих файлов. При этом Россия оказалась той страной, в которой наименьшее число пользователей имеет такую привычку – в среднем по миру этот показатель составляет 29%. В противовес этому, 22% российских участников опроса сообщили, что не создают резервные копии и не планируют делать это в будущем.

96% тех, кто все-таки обеспечивает сохранность своих файлов при помощи бэкапа, используют физические носители – внешние жесткие диски (90%), а также CD и DVD-диски (6%), и только 3% российских пользователей обращаются к облачным хранилищам для бэкапов. Любопытно при этом, что все, кто пользуется облаком, также синхронизируют через облако часть своих устройств.

Характерно, что **37% респондентов в России, пользующихся физическими носителями для бэкапа, когда-либо теряли свои данные**, потому что носитель был поврежден (13%), украден (2%), потерян (11%) или становился нечитаем (11%).

Несмотря на риски, связанные с физическими носителями, многие пользователи не доверяют облачным хранилищам – 18% респондентов не уверены, что их данные

будут там в безопасности, а еще 28% не станет хранить в облаке самые важные файлы, потому что опасается утечки.

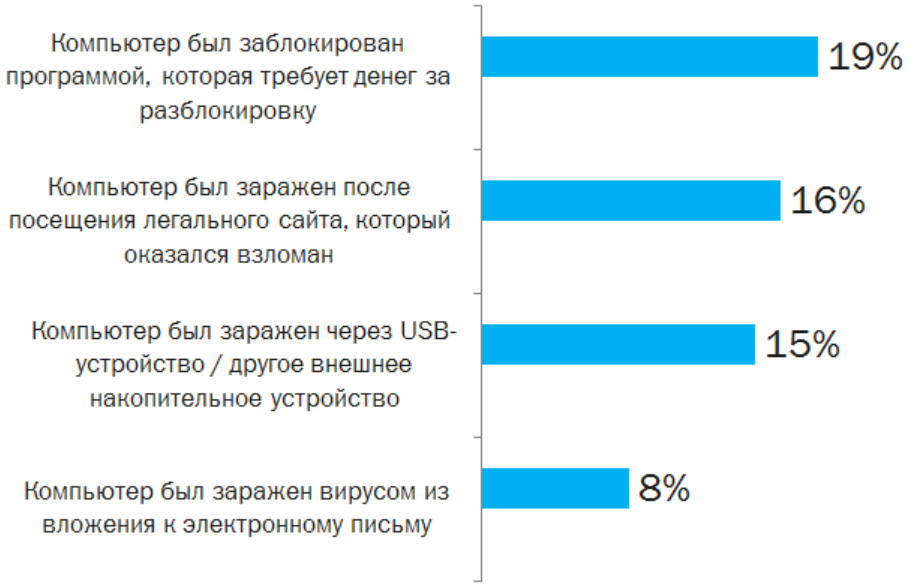
Следующая глава расскажет о том, с какими же киберугрозами пришлось столкнуться пользователям на самом деле.

Глава 4. Киберугрозы, с которыми столкнулись пользователи, и их последствия

Респонденты отметили опасные ситуации, с которыми им пришлось столкнуться в Сети за последние 12 месяцев, и оценили их негативный результат, после чего эксперты B2B International рассчитали среднюю стоимость, в которую обошлись пользователям те или иные «удачные» кибератаки.

- **44% опрошенных российских пользователей признались*, что их устройства были заражены вредоносной программой**:

**Представлен процент пользователей, которые смогли идентифицировать, что их устройство заражено*



- **26% респондентов в России сообщили о взломе одного или нескольких своих аккаунтов в социальных сетях, электронной почте или платежной системе**:

«Исследование рисков компьютерной безопасности для пользователей в России 2014», B2B International совместно с «Лабораторией Касперского»

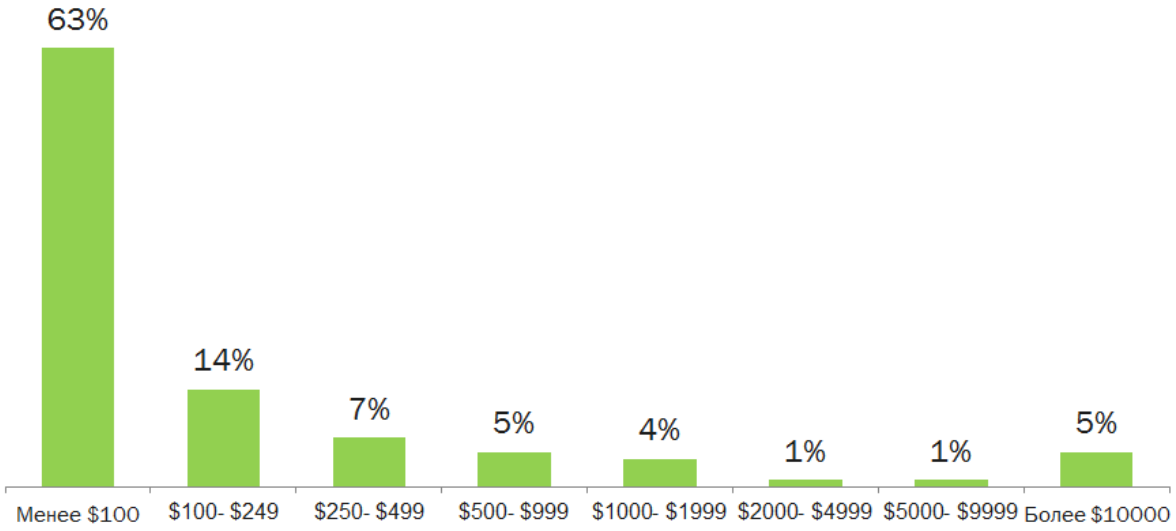
- **30% столкнулись с той или иной угрозой онлайн, целью которой был доступ к деньгам пользователя**:

В результате онлайн-мошенничества у 9% пользователей украли деньги, в то время как аналогичный показатель по миру составляет 5%.

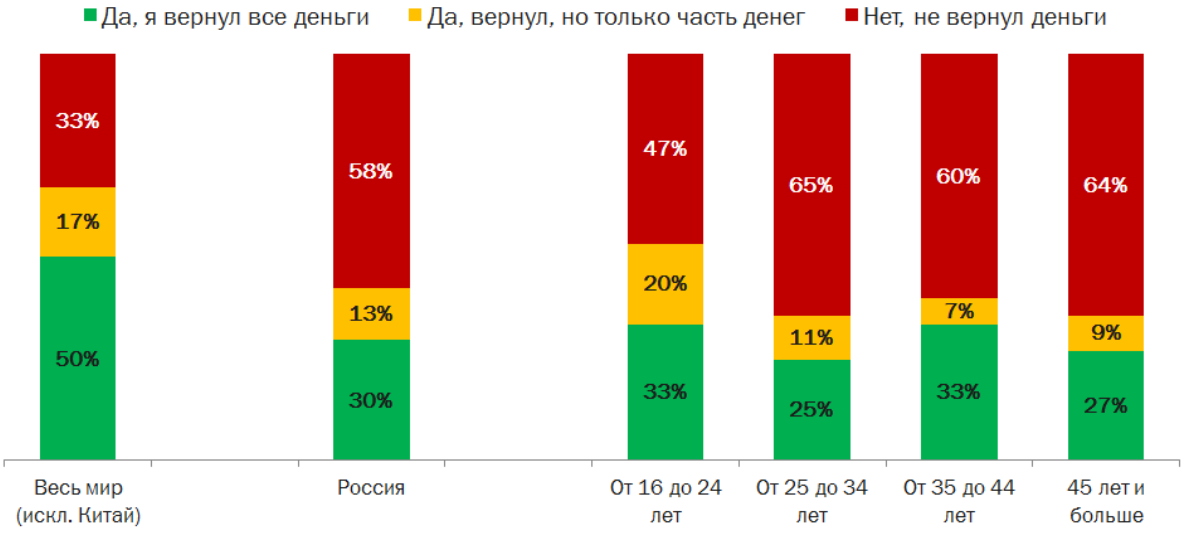
Если же посчитать прямые и косвенные финансовые потери пользователей, столкнувшихся с той или иной киберугрозой, то цифры получатся следующие.

В результате заражения вредоносной программой или взлома аккаунта почти каждый пятый (18% респондентов) понес финансовые затраты: 31% российских пользователей в таких случаях оплачивал услуги IT-специалиста, который помогал восстановить данные, 17% тратились на замену компонентов устройства, 13% покупали новый гаджет, а 14% приобретали специальное ПО для чистки зараженного устройства. В результате средняя «цена» атак за прошедшие 12 месяцев для российских пользователей составила $147. Дороже всего столкновение с вредоносной программой оказалось для жителей стран Азиатско-Тихоокеанского региона – $212.

Среди тех респондентов, у которых деньги были украдены напрямую через ту или иную мошенническую схему, **63% пользователей потеряли менее $100, однако 5% россиян лишились более $10000 в результате кибератаки:**



Заслуживающий внимания факт: **58% пострадавших россиян признались, что не смогли вернуть украденные у них деньги**. Еще 13% пользователей вернули лишь часть пропавших средств.

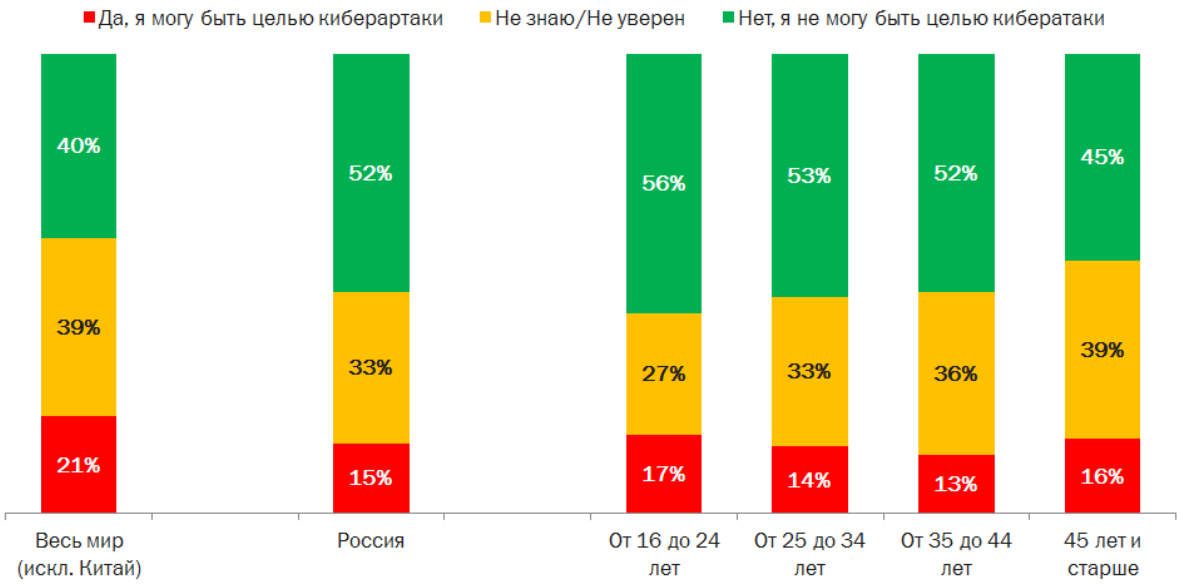


Зная то, с какими угрозами столкнулись респонденты за указанный период и какие издержки они понесли, можно сравнить эти данные с тем, что они думают об угрожающей им опасности, что им известно о современном ландшафте киберугроз и на кого они возлагают ответственность за свою защиту. Об этом – в следующей главе.

Глава 5. Отношение респондентов к вопросам кибербезопасности

Восприятие онлайн-угроз

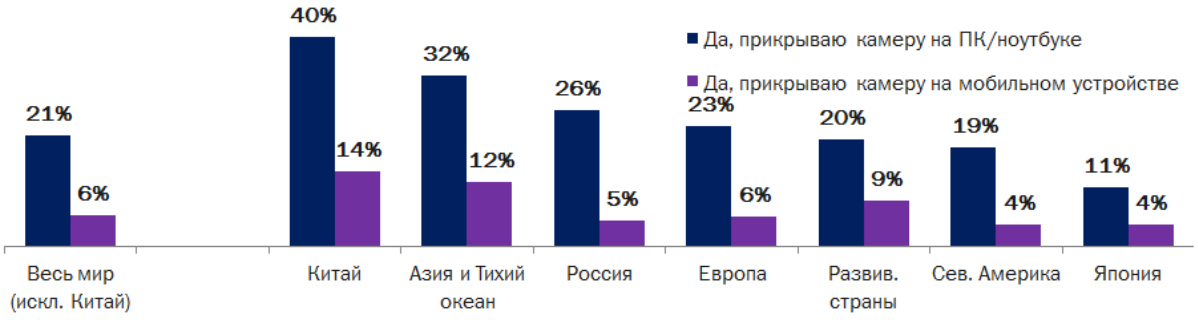
Несмотря на то что число угроз в Интернете с каждым годом растет, риск столкновения с киберугрозами сильно недооценен пользователями. **Всего лишь 15% опрошенных россиян на сегодняшний день считают, что могут быть целью кибератаки**. Еще менее уязвимыми себя считают только жители Японии (там этот показатель составляет 11%). В среднем же по миру 22% пользователей полагают, что их данные могут быть интересны киберпреступникам, а около 40% считают, что они не могут стать жертвой кибератаки



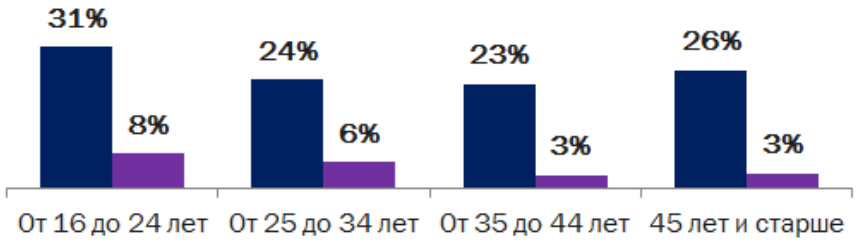
Более того, **13% российских пользователей уверены, что защитные решения – это рекламный трюк, и не верят в их необходимость**. Еще больше уверенных в этом пользователей проживает в странах Азиатско-Тихоокеанского региона (24%) и в Китае (23%).

В противоположность этому, почти половина респондентов чувствует прямую угрозу в свой адрес: **45% опрошенных в России волнуются, что их персональная информация может быть украдена и использована другими людьми, а 68% российских пользователей переживают, что за ними могут незаметно следить на их собственном устройстве.** Многие россияне также опасаются слежки со стороны правительственных организаций или не доверяют компаниям, которым передают свои данные:

Кроме того, **52% российских пользователей волнуются, что кто-то может получить доступ к их веб-камере, и 26% респондентов сознались, что из-за этого даже заклеивали ее на своем компьютере** (интересно, что среди российских мужчин таких насчитывается 30%, тогда как среди женщин этот показатель составляет 22%). Причем 5% опрошенных заклеивают камеру даже на своем смартфоне. Особенно этим выделяются респонденты из Китая и стран Азиатско-Тихоокеанского региона:



Молодые респонденты в России при этом оказались подозрительнее старшего поколения:



Если же объединить пользователей, переживающих из-за возможной слежки с помощью вредоносной программы и веб-камеры, то окажется, что такое опасение выразили 74% опрошенных в России. Но, несмотря на то, что пользователи

переживают за свое личное пространство онлайн и за сохранность конфиденциальных данных, треть (33%) респондентов созналась, что когда-либо делилась своими персональными данными с третьей стороной ради получения скидки или приза, а 20% признают, что размещают в социальных сетях больше личной информации, чем следовало бы.

Кроме того, каждый третий пользователь в России (32%) уверен, что может не осторожничать, пребывая в Интернете, если у него на устройстве стоит защитное решение. В довершение всего 27% российских пользователей все равно вводят свои персональные данные на сайте, даже если не уверены в его легитимности.

Понимание ландшафта киберугроз

Чтобы выяснить, насколько пользователи вообще осведомлены о текущих киберугрозах, эксперты предоставили им список таких угроз с кратким описанием каждой и с предложением ответить, знают ли они о ней и насколько она их беспокоит. Результаты получились следующие:

Киберугроза	**% пользователей, которые испытывают беспокойство**
Рекламное ПО	**31%**
Перехват данных через Wi-Fi	**35%**
DDoS-атаки	**32%**
Международные кампании кибершпионажа	**39%**
Мобильное вредоносное ПО	**38%**
Вредоносное ПО для веб-камер	**34%**
Вредоносное ПО, собирающее данные/перехватывающее пароли	**24%**
Взлом онлайн-аккаунтов	**22%**
Фишиновые письма/веб-страницы	**28%**
ПО порнографического характера	**38%**
Программы-вымогатели	**36%**
Эксплойты	**34%**
Спам	**12%**
Угрозы, нацеленные на банковские аккаунты	**31%**

Опрос показал, что больше всего российские пользователи опасаются международных кампаний кибершпионажа (39%), а также переживают из-за возможности столкнуться с мобильным вредоносным ПО или баннерами и программами с порнографическим содержанием (по 38%). Наименьшую же опасность, по мнению пользователей, для них представляет спам (12% обеспокоенных).

Стоит отметить, что 36% российских пользователей уделяют внимание опасности, исходящей от программ-вымогателей, однако риск этой угрозы недооценен. Ведь по данным облачной инфраструктуры Kaspersky Security Network, количество атак с использованием данного типа зловредов стремительно растет: только в 2013 году их было зафиксировано более 2,7 млн, что в 9 раз больше, чем в 2012 году.

Опасения также вызывает тот факт, что **лишь около трети опрошенных уделяет должное внимание таким известным им угрозам, как фишинг (28%) и перехват данных через Wi-Fi (35%)**, хотя именно эти способы часто используются киберпреступниками для кражи данных пользователя и его денежных средств, так как требуют минимальных вложений.

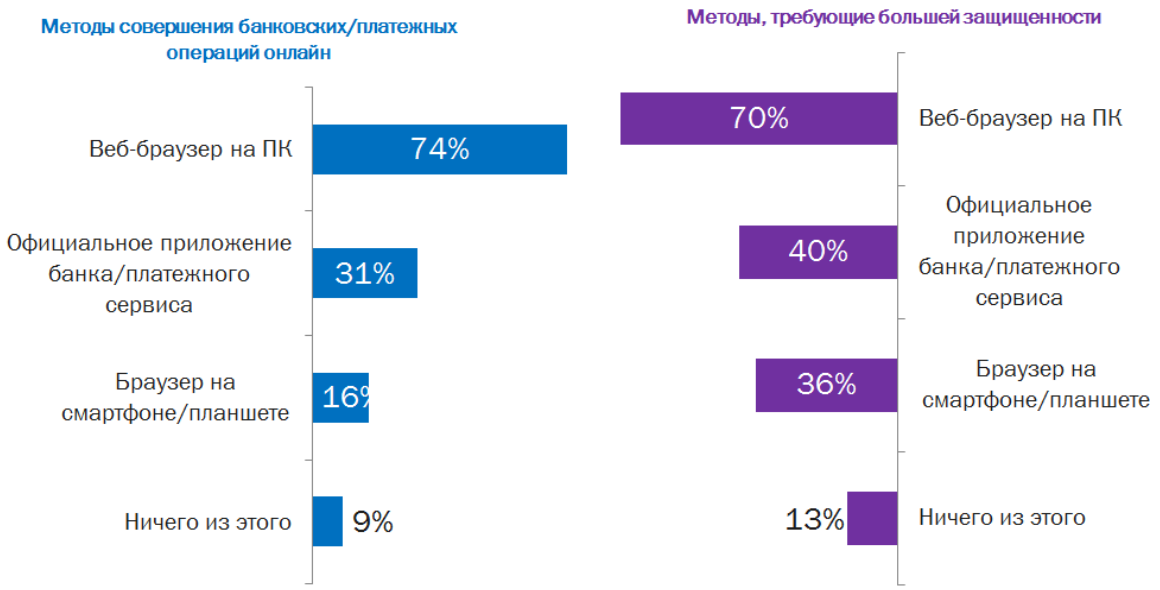
В связи с тем, что меньше половины респондентов выразили обеспокоенность в связи с мобильными угрозами, им было задано несколько дополнительных вопросов на эту тему. **72% российских пользователей согласны, что мобильные устройства сегодня так же уязвимы для киберугроз, как и традиционные компьютеры**. Однако одновременно с этим каждый пятый (20%) все еще чувствует себя в полной безопасности, выходя в Интернет с планшета и смартфона. Рискованное поведение, если принять во внимание, что многим типам угроз, в частности финансовым, больше подвержены именно мобильные устройства.

Понимание финансовых угроз

В условиях, когда киберпреступники все больше внимания акцентируют на финансовых данных пользователя, как никогда важным становится понимание соответствующих рисков и умение защититься от них. Поэтому респондентам было предложено согласиться или не согласиться с одним из утверждений о киберугрозах, нацеленных на их кошелек.

Опрос показал, что **63% российских пользователей волнуются из-за возможного финансового мошенничества онлайн**. Еще 41% респондентов сообщили, что чувствуют себя уязвимыми, когда совершают финансовую транзакцию или покупают что-либо в Интернете. И неожиданно 17% российских пользователей заявили, что киберпреступления, направленные на кражу денег через Интернет, — большая редкость, и вряд ли такое случится с ними.

74% респондентов в России для проведения онлайн-платежей пользуются веб-браузером, а 16% – мобильным браузером. Еще 31% пользователей выбирают для этого официальное мобильное приложение, предоставляемое финансовым провайдером – банком или платежной системой. Однако только 13% опрошенных россиян считают эти способы достаточно безопасными:



Когда же пользователям предложили выбрать два самых безопасных способа оплаты, включая оффлайн, веб-браузер на компьютере оказался лишь на третьем месте по популярности – 23% респондентов указали этот способ как самый безопасный. На первом и втором месте – оффлайн-платежи: 61% опрошенных россиян выбрали наличные, а 30% – банковскую карту. Любопытно, что 17% российских пользователей назвали в качестве самого безопасного способа оплаты электронные деньги (биткойны, PayPal и др.).

В то же время подавляющее большинство пользователей сходятся во мнении, что безопасность финансовых транзакций должна быть обеспечена компаниями, которые эти транзакции проводят. **76% респондентов в России предпочитают, чтобы банки, платежные системы и онлайн-магазины предоставляли им специальные защитные решения, в том числе для мобильных устройств**:

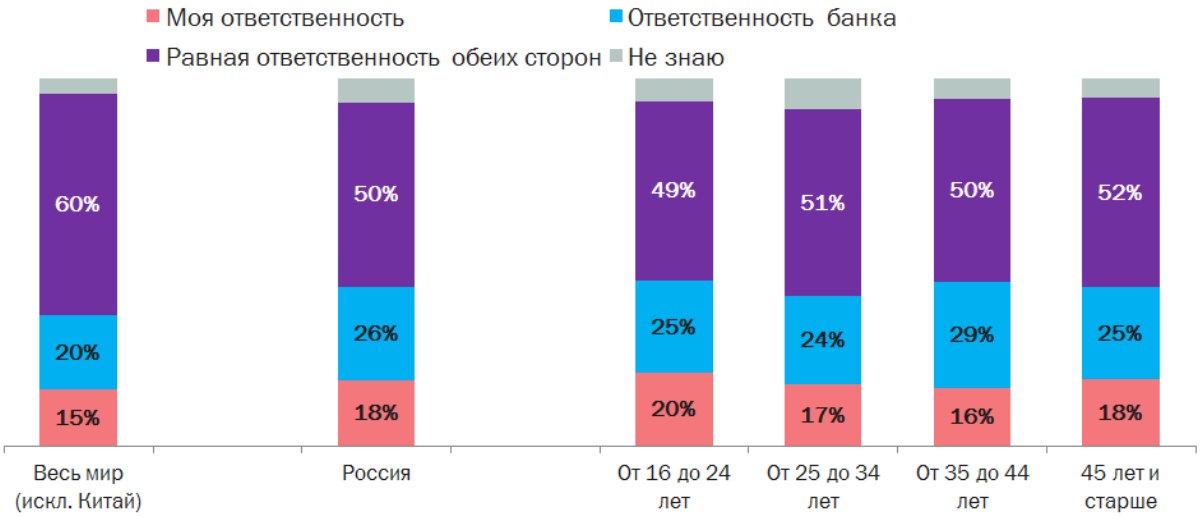
Более того, уровень защиты онлайн-транзакций напрямую влияет на финансовую активность пользователей онлайн: **44% опрошенных россиян признают, что**

«Исследование рисков компьютерной безопасности для пользователей в России 2014», B2B International совместно с «Лабораторией Касперского»

использовали бы такой способ оплаты гораздо чаще, если бы имели надежное защитное решение на своем устройстве. При этом 14% пользователей, случалось, отказывались от онлайн-платежа на полпути, потому что не были уверены в его безопасности.

Кроме того, российские пользователи признались, что, если мошенническая схема оказалась успешной для преступников, они ждут, что финансовые компании возместят им украденные средства без вопросов – так считает 20% респондентов.

На вопрос, кто должен отвечать за защиту финансовых операций онлайн, всего 18% российских пользователей ответили, что они сами, в то время как 26% возлагают полную ответственность на банк. Однако половина (50%) опрошенных россиян уверена, что обе стороны должны в равной степени заботиться о защите электронных переводов и платежей:



Одним из самых простых и эффективных вариантов доступа киберпреступников к данным пользователя, включая банковский аккаунт или личную страницу в интернет-магазине, является использование логина и пароля самого пользователя.

Отношение к паролям

Мошенники могут получить пароль пользователя разными способами: с помощью специальных вредоносных программ, фишинговых веб-страниц и электронных писем, путем перехвата трафика Wi-Fi и др. При этом угроза для пользователя еще масштабнее, если он использует один пароль для разных аккаунтов – тогда, заполучив всего лишь один пароль, преступники смогут открыть доступ к нескольким ресурсам и, соответственно, извлечь бóльшую выгоду.

В связи с этим респондентов спросили, сколько паролей они используют в Сети. Выяснилось, что только треть (31%) опрошенных россиян придумывает разные пароли для разных аккаунтов, а 26% оперируют ограниченным количеством паролей. Кроме того, 6% российских пользователей применяют один и тот же пароль ко всем своим учетным записям.

Такой подход к выбору паролей может быть обусловлен тем, что подавляющее большинство пользователей предпочитают пароли запоминать, нежели использовать для этого специальные решения, призванные генерировать устойчивые пароли и хранить их в защищенном виде. Хуже того, 51% россиян используют для хранения паролей потенциально небезопасные способы: записную книжку, стикер рядом с компьютером, мобильный телефон и др.:

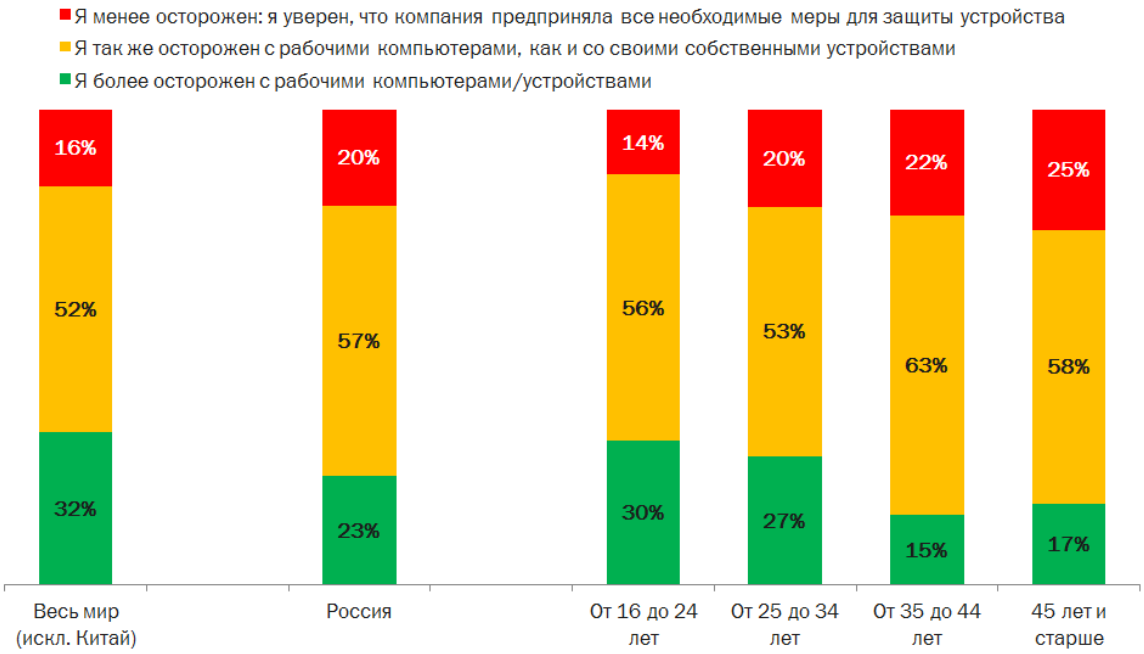
Несмотря на то, что 69% пользователей полагаются на свою память, когда идет речь о пароле, только 14% никогда не забывали его, а 5% признались, что из-за этого теряли доступ к своему аккаунту.

Пользователи довольно оптимистичны, говоря о паролях: **так, 39% опрошенных россиян уверены, что их пароли не могут быть полезны киберпреступникам**, а 13% не делают из пароля тайны, когда речь идет о родственниках и друзьях. Также каждый пятый пользователь (19%) не предпринимает никаких дополнительных мер, чтобы защитить свой пароль, а еще 29% считают, что все веб-сайты надежно хранят их пароли. Однако, напротив, периодически пароли пользователей становятся доступны в результате крупных утечек у компаний.

Опрос показывает, что, несмотря на все опасения, большинство пользователей все еще беспечны, когда речь идет о защите их «цифрового я» и личных данных онлайн. Поэтому было интересно узнать, остаются ли они так же беспечны и на работе.

Отношение к угрозам на работе

Согласно опросу, **86% респондентов в России используют свое устройство в том числе и для работы**. При этом 20% из них признались, что в этом случае они менее осторожны, так как уверены, что компания уже предприняла все необходимые меры защиты:



Интересно, что 57% опрошенных в России, использующих свое устройство для работы, считают, что киберугрозы для домашнего пользователя и для компаний мало чем отличаются. В то же время только 51% российских пользователей уверены, что смогут отличить настоящее письмо от спама, а 34% не проверяют ссылки и вложения, получаемые по корпоративной электронной почте:

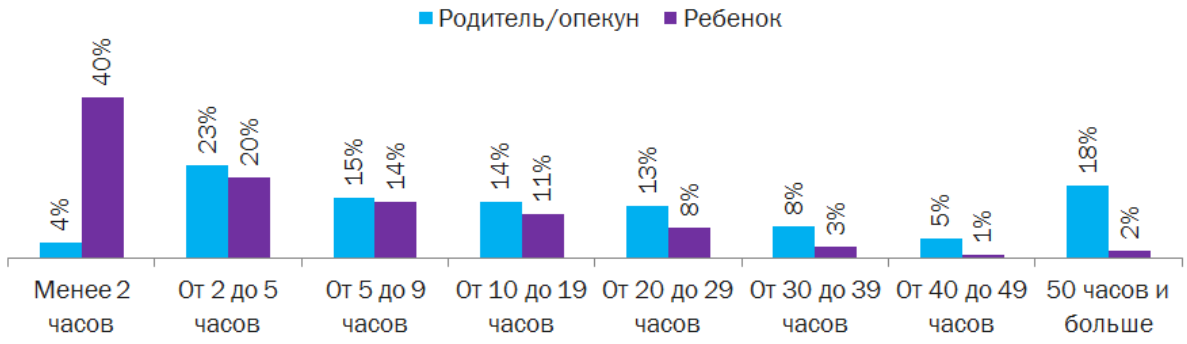
Таким образом, пользователи подвергают риску не только личную, но и бизнес-информацию. В дополнение **пятая часть респондентов (20%) призналась, что хотя бы раз открывала потенциально опасную ссылку или вложение**. Любопытно, что чаще других в этом признавались участники опроса из Китая и стран Азиатско-Тихоокеанского региона (58% и 42% соответственно).

В следующей главе приводятся результаты исследования, демонстрирующие, как пользователи относятся к тому, что происходит в Сети с их детьми, и способны ли они защитить их от киберугроз.

Глава 6. Дети онлайн: отношение родителей, инциденты и решения

Вопросы, представленные в этой главе, были заданы респондентам, которые сообщили, что в их семье есть дети до 16 лет, их доля составила около 40%. Вопросы касались угроз, с которыми сталкиваются дети онлайн, и предпринимаемых мерах защиты. Выяснилось, что большая часть взрослых серьезно обеспокоена вопросами безопасности детей в Интернете, при этом **35% опрошенных россиян, имеющих детей в семье, согласились с утверждением, что количество онлайн-угроз для их детей растет**.

Согласно опросу, часто дети находятся в Сети не меньше, чем их родители, — в 16% случаев дети и взрослые пользуются Интернетом примерно одинаковое количество времени, а в 12% дети находятся онлайн дольше, чем взрослые. Чаще всего дети российских респондентов используют Интернет менее 2 часов в неделю:

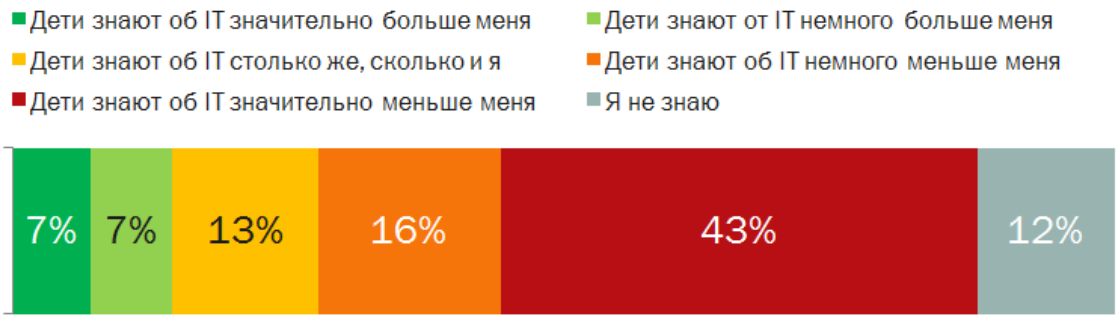


Россия оказалась в числе тех стран, где родители наиболее строги со своими детьми в том, что касается продолжительности пребывания в Сети – 40% опрошенных сообщили, что не позволяют своему ребенку проводить в Интернете больше 2-х часов в неделю. Еще более жесткими в этом вопросе оказались жители Японии — вариант «менее двух часов» выбрали 52% респондентов из этой страны.

Отвечая на вопрос, чем же занимаются их дети в Интернете, большинство взрослых россиян (62%) сообщили, что дети играют в онлайн-игры. На втором по популярности месте у юных пользователей оказались социальные сети (45%). Примечательно, что у взрослых соцмедиа заняли третью строку в списке онлайн активностей.

К сожалению, неизвестно, как на эти вопросы ответили бы сами дети, поскольку далеко не все взрослые точно знают, чем занимаются их дети онлайн. Почти половина респондентов в России (47%) переживает, что ребенок может увидеть в Сети нежелательный контент, почти столько же (48%) – что ребенок может стать жертвой онлайн-травли. 31% родителей волнуются, что их дети могут общаться в Сети с подозрительными незнакомцами, а 22% опрошенных считают, что те излишне делятся личной информацией в Сети.

Более того, **14% опрошенных россиян считают, что их дети знают об информационных технологиях больше или даже значительно больше их самих**:



При этом 45% опрошенных россиян полагают, что дети ничего не знают о киберугрозах:

15% россиян, имеющие детей в семье, чувствуют, что не могут контролировать, что их дети видят или делают онлайн. На вопрос, какие же действия они предпринимают, чтобы защитить своих детей от угроз в Интернете, 33% российских пользователей ответили, что следят за тем, чем ребенок занят онлайн, а 36% ограничивают время пребывания в Сети. Еще 26% опрошенных россиян проводят с детьми воспитательные беседы, а 14% «подружились» с ними в социальных сетях. И только 19% респондентов в России используют специальное ПО, которое позволяет отсеивать нежелательный для ребенка контент или ограничивать время, проводимое им в Сети.

Интересно, что 22% (т.е. каждый пятый родитель или попечитель) не применяют ни одну из указанных мер – и в этом Россия вновь оказалась на втором месте. Еще больше пользователей, не уделяющих внимания защите детей от киберугроз, проживает только в Японии – 35%.

В то же время, значительное число респондентов в России признают, что их дети сталкиваются с онлайн-угрозами или становятся их источником. Так, **20% опрошенных заявили, что за последние 12 месяцев с их детьми случались инциденты, угрожавшие непосредственно детям, а 14% отметили, что их дети совершили нечто, приведшее к потере денег или данных взрослых**:

Одним из самых неприятных явлений в Интернете остается так называемый кибербуллинг, или травля ребенка в Сети посредством, например, социальных сетей. О таком прецеденте за последние 12 месяцев заявили 4% родителей в России. При этом, согласно исследованию, в подавляющем большинстве случаев онлайн-агрессия имела негативные последствия в реальности: 58% родителей были вынуждены вмешаться, чтобы уладить конфликт, в 13% ситуаций онлайн-травля перешла в оффлайн, а **в 26% случаев ребенок получал настолько тяжелую психологическую травму, что длительное время не мог прийти в себя**.

Иными словами, Интернет един, и в нем хватает угроз для всех: детей и взрослых, покупателей интернет-магазинов и любителей социальных сетей, пользователей Windows и почитателей Mac OS X. Поэтому пользователю так важно соблюдать осторожность и знать, чем может грозить то или иное действие в Сети. Как говорится, предупрежден – значит вооружен.

Заключение

Пользователи сегодня выходят в Интернет сразу с нескольких устройств и доверяют им самое ценное: свои секреты, приватную информацию, свое «я». Неудивительно, что большинство из них, осознавая важность «цифровой» части своей жизни, боятся потерять эти данные или стать объектом слежки в Сети со стороны третьих лиц. Но, несмотря на опасения, люди все еще мало склонны к безопасному поведению – многие из них не только не устанавливают защитные решения на устройства, но даже не защищают их паролем, и лишь малая часть пользователей знает о тех угрозах, с которыми могут столкнуться в Сети они сами или их родные.

В то же время, как показывает статистика, все больше владельцев устройств теряют в Сети свои файлы, деньги или свое «цифровое я», вернуть которые порой оказывается невозможно. В связи с этим «Лаборатория Касперского» рекомендует не только пользоваться защитными решениями для своей безопасности и уверенности, но и быть осторожными в Интернете, особенно когда речь идет о передаче конфиденциальной информации и финансовых операциях: пользоваться надежными паролями, не вводить свои данные на подозрительных сайтах или через незащищенную Wi-Fi сеть, не открывать неизвестные файлы и не забывать о защите для своих детей.

Интересные ссылки по теме:

Отчет «Финансовые киберугрозы в 2013 году»:
http://securelist.ru/analysis/obzor/19180/finansovye-kiberugrozy-v-2013-godu-chast-1-fishing/

Отчёт «Развитие информационных угроз в первом квартале 2014 года»:
http://securelist.ru/analysis/malware-quarterly/19176/razvitie-informacionnyx-ugroz-v-pervom-kvartale-2014-goda/

Отчёт «Развитие информационных угроз во втором квартале 2014 года»:
http://securelist.ru/analysis/malware-quarterly/21505/razvitie-informacionnyx-ugroz-vo-vtorom-kvartale-2014-goda/

Блогпост «Обманщики в социальных сетях»:
http://securelist.ru/featured/20052/obmanshhiki-v-socialnyx-setyax/

Блогпост «Дети в Сети: формула безопасности»:
http://securelist.ru/analysis/obzor/20171/deti-v-seti-formula-bezopasnosti/