G Data

Исследование безопасности 2011

Как пользователи оценивают угрозы в Интернете?

Больше, чем защита. **G Data.**

Содержание:

1 Сбор данных

1.1 Масштаб и цель исследования

Ежедневно средства массовой информации сообщают о новых атаках, направленных на пользователей Интернета и компании, о хищении данных, новых компьютерных вредоносных программах и структурах киберпреступных картелей. При этом частные пользователи все чаще оказываются под прицелом преступников и все чаще становятся жертвами действующих по всему миру кибербанд. Поэтому в эпоху Интернета защита цифровых данных на предприятиях приобретает исключительно важное значение. Пользователи могут защитить персональные компьютеры с помощью множества IT-решений безопасности. Но насколько пользователи хорошо информированы об интернет-угрозах и последовательности действий преступников? Кто на шаг впереди в отношении IT-безопасности — молодые или более старшие пользователи? Кто лучшие интернет-пользователи -—мужчины или женщины? В этом масштабном международном исследовании безопасности G Data поднимает эти и многие другие вопросы, исследует мифы об IT-безопасности и демонстрирует реальное отношение пользователей к интернет-угрозам.

1.2 Насколько хорошо пользователи знакомы с интернет-угрозами?

В своем исследовании безопасности компания G Data сравнила результаты опросов (т.е. восприятие угроз и их оценку пользователями) с фактическим уровнем опасности. Анализ результатов показывает, что знания, которыми располагают интернет-пользователи, во многом недостаточны и устаревшие.

Почти все участники опроса имеют общее представление о том, что угрозы поджидают пользователей в Интернете, и соответствующим образом пытаются защитить свои ПК. Знание очень редко является реальным отображением угроз. Таким образом, девять из десяти пользователей ПК считают, что пользователь замечает заражение вредоносной программой. По мнению опрошенных, такое заражение проявляется в виде странных всплывающих окон, замедлении работы компьютера или в прекращении его работы вообще. Большинство опрошенных твердо убеждены, что появляется хотя бы один из перечисленных выше признаков.

Однако цель интернет-преступников — заработать как можно больше денег, а значит, пользователь не должен замечать заражения как можно дольше. Как правило, вся персональная информация как то данные кредитной карточки, банковские данные, данные доступа к онлайн-магазинам, электронной почте и прочее воруются при первом заражении. За этим обычно следует подключение компьютера к бот-сетям для того, чтобы использовать их в качестве распространителей спама или DDoS-атак на форумах.

При распространении вредоносных кодов злоумышленники уже давно делают ставку на социальные сети, где публикуют ссылки на подготовленные веб-сайты. Распространение через электронные сообщения, содержащие спам и инфицированные вложения, все еще имеет место, однако, по мнению многих участников опроса, устарело. В концепции распространения вредоносных компьютерных программ спам используется для того, чтобы заманить получателя на веб-сайты, содержащие вредоносные коды, и для дальнейшего заражения ПК

т.н. вирусом для "попутной загрузки" (Drive-by-Download). (См. раздел 3.2.1 Одиннадцать мифов об IT-безопасности и где ошибаются интернет-пользователи").

Кредит доверия пользователей в социальных сетях бесконечен: 35% доверяют ссылкам, опубликованным в их социальной сети, 19% переходят по ссылкам, несмотря на их происхождение, и тем самым очень становятся мишенью для кибер-преступников и их незаконных действий.

Но как все-таки пользователи защищаются от атак? Хорошая новость: всего лишь 11% всех интернет-пользователей заходят в Интернет почти незащищенными и совершенно не используют надежные решения защиты от вирусов или пакеты безопасности. 48% опрошенных используют бесплатные антивирусные программы и при этом не используют автономный брандмауэр, http-защиту, "облачную" защиту, программы для борьбы со спамом или антиспамовый модуль. Более 50% этих пользователей даже хотели бы установить полный программный пакет с этими необходимыми технологиями защиты (см. раздел 3.1 "Как пользователи защищаются от угроз?").

Вывод: Исследование безопасности, проведенное компанией G Data, показывает, что пользователи неверно оценивают действительные угрозы в Интернете, и что больший процент частных пользователей неэффективно защищают свои компьютеры. Последствия налицо: слишком много людей подвергаются опасности заражения своих компьютеров вредоносными программами помимо своего желания. Недостаток знаний в два раза больше играет на руку интернет-преступникам и создателям вредоносного ПО.

2 Методика исследования

Исследование безопасности компании G Data под названием "Как пользователи оценивают угрозы в Интернете?" основано на международном онлайн-опросе 15 559 интернет-пользователей в возрасте от 18 до 65 лет в одиннадцати странах. Участники отвечали на вопросы на тему онлайн-угроз в Интернете, поведения во время интернет-серфинга, использования решений безопасности, а также понимании собственной безопасности в Интернете. Для каждой страны была создана собственная интернет-страница на языке этой страны, которая содержала каталог с одинаковыми вопросами. В распоряжении опрашиваемых находились отдельные ПК с отдельным доступом в Интернет. Сбор данных проходил с февраля по март 2011 г. по заказу G Data Software AG и при содействии компании Survey Sampling International[1]. Оценка и анализ данных были проведены в апреле-мае 2011 г.

[1] Подробные сведение о компании Survey Sampling International см. в приложении.

Таблица 1. Распределение опрошенныхх по возрасту и полу

Возраст	Мужчины	Женщины	Всего
18-24	1273	1430	2703
25-34	1636	1796	3432
35-44	1603	1784	3387
45-54	1585	1647	3232
55-65	1381	1424	2805
Всего	**7478**	**8081**	**15559**

Таблица 2. Число опрошенных в разных странах

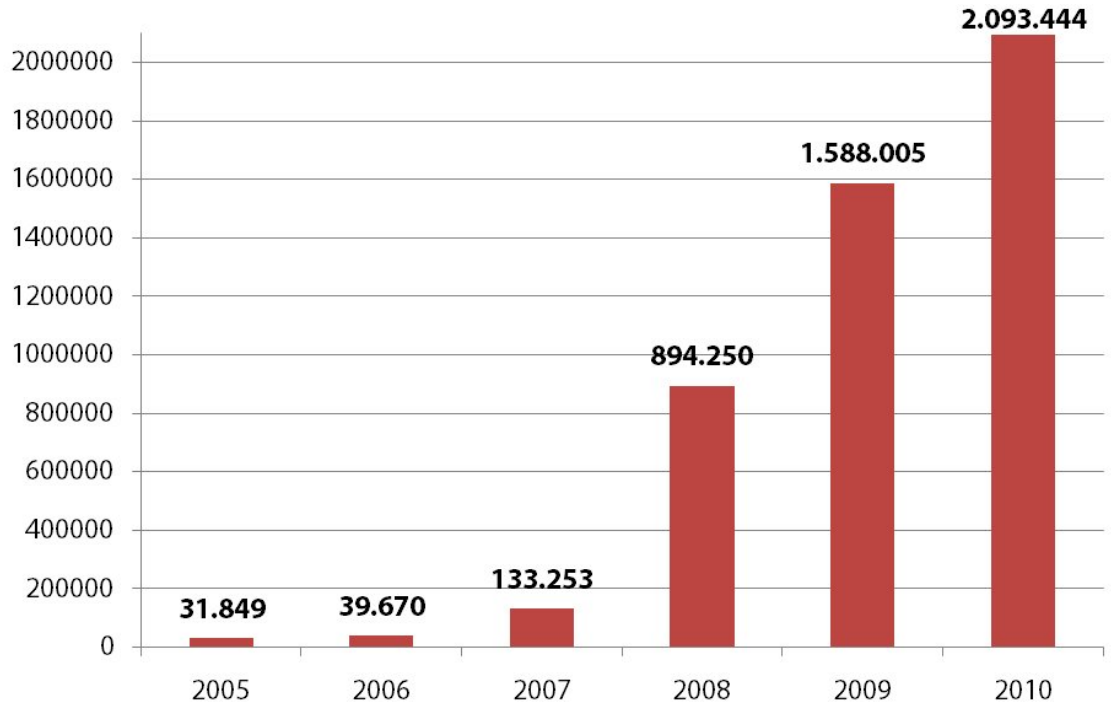
Страны	Мужчины	Женщины	Всего
Бельгия	432	496	928
Германия	591	603	1194
Франция	582	622	1204
Италия	575	563	1138
Нидерланды	336	367	703
Австрия	343	425	768
Россия	503	582	1085
Испания	579	579	1158
Великобритания	545	561	1106
США	2646	2958	5604
Швейцария	346	333	679
Всего	**7478**	**8081**	**15559**

3 Результаты исследования безопасности G Data

Атаки, направленные на компании и частных пользователей, стали очень популярными в последние годы. Не так давно интернет-преступность превратилась в прибыльный бизнес; во время атак злоумышленники применяют самые различные махинации, чтобы заразить компьютеры вредоносными программами, похитить у жертв всевозможные данные и выгодно их перепродать.

Лишь только в прошлом году G Data зарегистрировала более двух миллионов новых вредоносных программ для ОС Windows.[2]

График 1. Кол-во новых вредоносных программ за год, начиная с 2005 г.



Преступники распространяют вредоносный код при помощь множества уловок. Одной из них является является размещение вредоносных программ на интернет-страницах. Одного посещения опасного веб-сайта хватает для того, чтобы заразить компьютер так называемыми вирусами для "попутной загрузки", троянами, шпионскими и другими вредоносными программами. Пользователь заходит на такие коварные сайты во время интернет-поиска или злоумышленники размещают URL-адреса, например, в социальных сетях и в чатах в виде сообщений. Чтобы заманить пользователя на подготовленные веб-сайты или заставить его открыть зараженные вложения, интернет-преступники также рассылают сообщения, содержащие спам. В данном случае в сообщении речь идет, например, о мнимом счете, предупреждении или эксклюзивных фотографиях знаменитостей или важного события. Как только пользователи принимают такое приглашение, они попадают на сайты с вредоносным кодом и неумышленно заражаются вредоносной программой.

Пользователи могут защитить себя от поджидающих их угроз только с помощью сложных решений защиты и безопасности и осмотрительного пользования Интернетом.

[2] См. отчет G Data о вредоносном ПО за 2/2010, http://www.gdatasoftware.com/information/security-labs/information/whitepaper.html

3.1 Как пользователи защищаются от угроз?

Результат исследования безопасности G Data показывает, что из более 15 500 опрошенных пользователей более 89% используют на своих компьютерах защитное программное обеспечение, из них 48% доверяют бесплатным программам.

График 2. Какое решение безопасности пользователи используют на своих компьютерах?

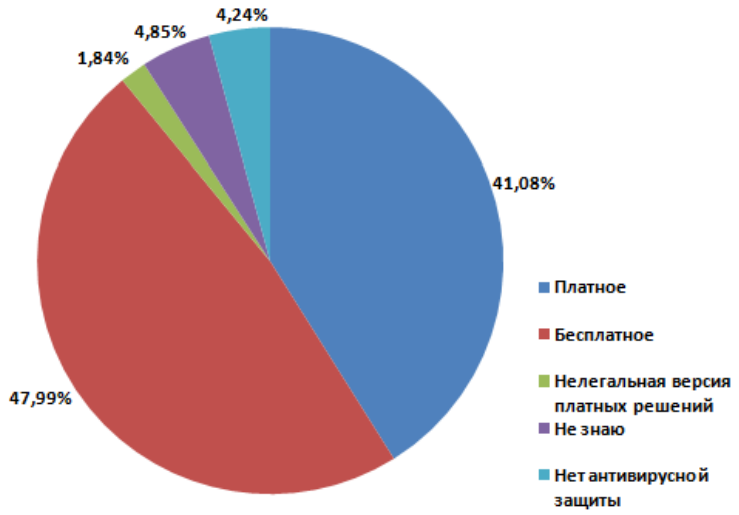


Таблица 3. Результаты опроса на тему, какое решение безопасности используют пользовател

Какое решение для безопасности Вы используете?					
	Платное	**Бесплатное**	**Нелегальная версия платных решений**	**Не знаю**	**Нет антивирусной защиты**
Мужчины (18-24)	39,83%	43,99%	4,08%	4,87%	7,23%
Мужчины (25-34)	42,60%	47,37%	2,14%	2,87%	5,01%
Мужчины (35-44)	42,98%	47,16%	1,62%	3,93%	4,30%
Мужчины (45-54)	42,15%	50,41%	1,32%	2,84%	3,28%
Мужчины (55-64)	44,97%	48,08%	1,16%	2,68%	3,11%
Всего мужчин	**42,55%**	**47,53%**	**2,01%**	**3,40%**	**4,52%**
Женщины (18-24)	34,69%	51,47%	2,10%	6,08%	5,66%
Женщины(25-34)	40,81%	47,05%	2,62%	5,57%	3,95%
Женщины (35-44)	42,60%	46,92%	1,51%	5,44%	3,53%
Женщины (45-54)	40,80%	48,33%	1,09%	6,86%	2,91%
Женщины (55-64)	38,48%	49,02%	1,05%	7,30%	4,14%
Всего женщин	**39,71%**	**48,41%**	**1,70%**	**6,20%**	**3,98%**
Всего	**41,08%**	**47,99%**	**1,84%**	**4,85%**	**4,24%**

В сравнении с общим результатом исследования безопасности Великобритания демонстрирует самые высокие показатели: более 94% опрашиваемых используют какое-либо решение безопасности. Самые низкие показатели у России, которые составили 83%. При этом во всех странах не менее четырех пятых опрошенных используют защитное ПО.

График 3. Какое решение безопасности пользователи используют на своих компьютерах в отдельных странах?

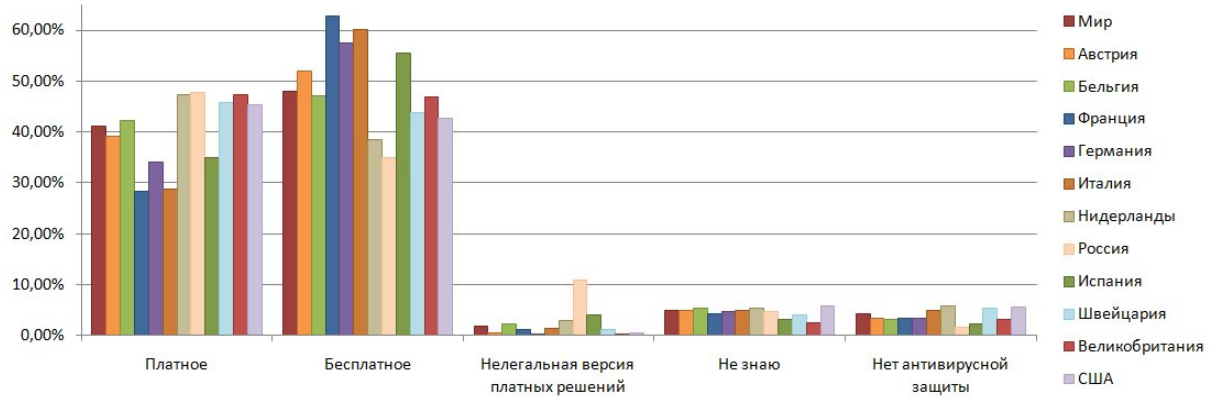


Таблица 4. Подробные результаты по странам: какое решение безопасности используют пользователи?

Какое решение для безопасности Вы используете?					
	Платное	**Бесплатное**	**Нелегальная версия платных решений**	**Не знаю**	**Нет антивирусной защиты**
Мир	41,08%	47,99%	1,84%	4,85%	4,24%
Австрия	39,19%	51,95%	0,52%	4,95%	3,39%
Бельгия	42,24%	47,09%	2,16%	5,39%	3,13%
Великобритания	47,29%	46,84%	0,27%	2,53%	3,07%
Германия	34,09%	57,37%	0,34%	4,77%	3,43%
Испания	34,96%	55,57%	4,00%	3,22%	2,26%
Италия	28,82%	60,01%	1,40%	4,92%	4,83%
Нидерланды	47,23%	38,55%	2,99%	5,41%	5,83%
Россия	47,83%	34,84%	10,97%	4,79%	1,57%
США	45,40%	42,74%	0,55%	5,71%	5,60%
Франция	28,41%	62,79%	1,16%	4,24%	3,41%
Швейцария	45,76%	43,80%	1,26%	3,92%	5,26%

Пользователи могут сочетать бесплатное антивирусное ПО и другие бесплатные инструменты. Проблемой может стать возможная несовместимость определенных программ с используемым защитным ПО.

Важнейшей составляющей эффективной защиты компьютера, наряду с антивирусной защитой, является персональный брандмауэр, спам-фильтр и, не в последнюю очередь, специальная интернет-защита. В данной области G Data предлагает "облачную" защиту G Data CloudSecurity - бесплатный плагин для браузера, совместимый со всеми решениями антивирусной защиты.[3]

[3] Подробные сведения о бесплатной интернет-защите см. на http://www.free-cloudsecurity.com/ru/

3.1.1 Как оценивают пользователи продуктивность бесплатного антивирусного ПО?

Как упоминалось выше, существуют различные лазейки для заражения ПК. Современные решения безопасности должны защищать от этих угроз. Бесплатные антивирусные программы, если их рассматривать отдельно, с этим не справляются. Бесплатные программы не предлагают защитных технологий, которые имеют исключительно важное значение для серьезной защиты. Сюда относятся антиспам, веб-фильтр, брандмауэр, поведенческое распознавание вредоносных кодов и «облачная» защита.

Итак, пользователям был задан вопрос о том, как они оценивают эффективность и качество бесплатных защитных программ. Почти 44% участников опроса считают, что эффективность и качество бесплатного защитного ПО находятся на уровне платных решений.

График 4. Оценка эффективности: является ли бесплатное защитное ПО таким же хорошим, как и платные решения безопасности?

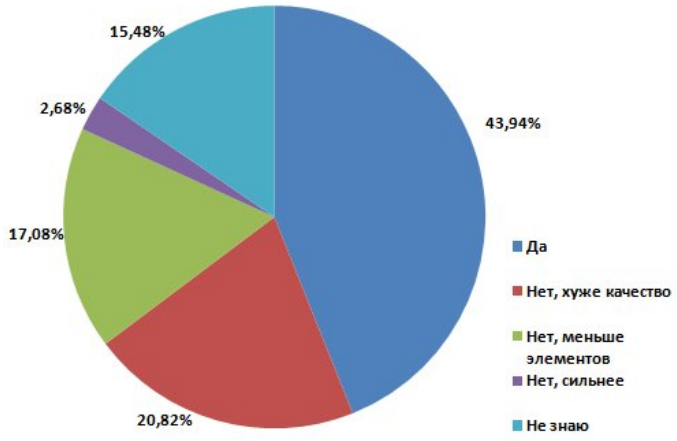


Таблица 5. Подробные результаты опроса: считают ли пользователи, что качество и возможности бесплатного и платного защитного ПО одинаковы?

Какое решение для безопасности Вы используете?					
	Платное	**Бесплатное**	**Нелегальная версия платных решений**	**Не знаю**	**Нет антивирусной защиты**
Мир	41,08%	47,99%	1,84%	4,85%	4,24%
Австрия	39,19%	51,95%	0,52%	4,95%	3,39%
Бельгия	42,24%	47,09%	2,16%	5,39%	3,13%
Великобритания	47,29%	46,84%	0,27%	2,53%	3,07%
Германия	34,09%	57,37%	0,34%	4,77%	3,43%
Испания	34,96%	55,57%	4,00%	3,22%	2,26%
Италия	28,82%	60,01%	1,40%	4,92%	4,83%
Нидерланды	47,23%	38,55%	2,99%	5,41%	5,83%
Россия	47,83%	34,84%	10,97%	4,79%	1,57%
США	45,40%	42,74%	0,55%	5,71%	5,60%
Франция	28,41%	62,79%	1,16%	4,24%	3,41%
Швейцария	45,76%	43,80%	1,26%	3,92%	5,26%

Лидером среди стран стала Франция: для 53% опрошенных во Франции нет никакой разницы между бесплатным и платным защитным программным обеспечением. По сравнению с этим опрошенные в Нидерландах показали наименьшее значение: здесь всего лишь 35% считают, что бесплатное и платное защитное ПО имеет одинаковые характеристики.

График 5. Оценка эффективности бесплатного защитного ПО в разных странах

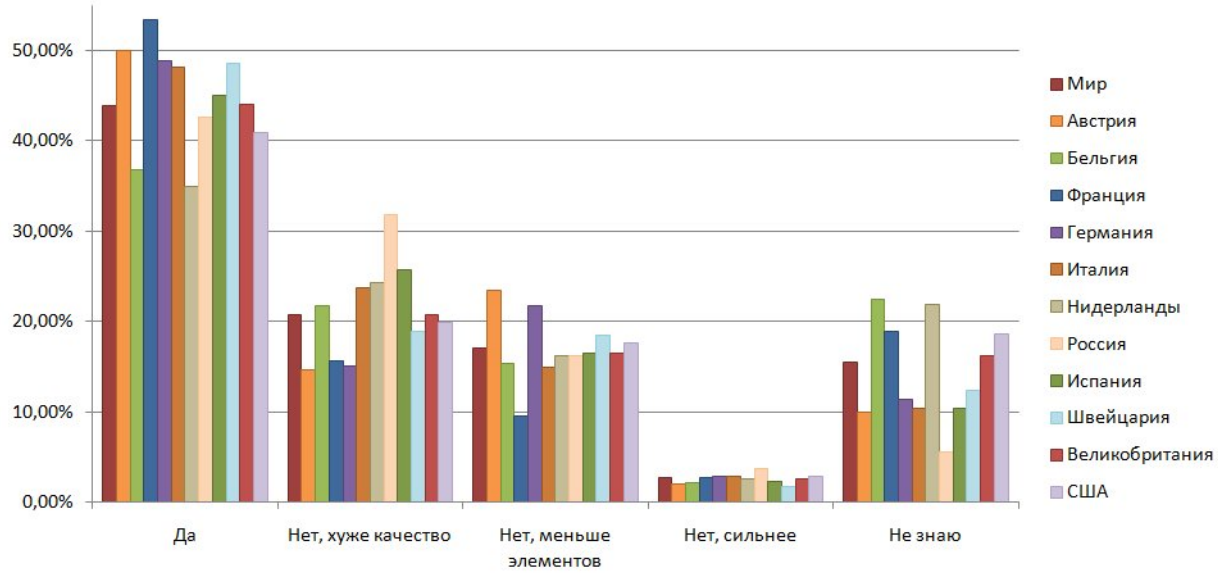


Таблица 6. Результаты по отдельным странам: является ли для опрашиваемых бесплатное защитное ПО эквивалентом платных решений безопасности?

Бесплатные антивирусные программы так же эффективны, как и платные пакеты программ?					
	Да	**Нет, хуже качество**	**Нет, меньше элементов**	**Нет, сильнее**	**Не знаю**
Мир	43,94%	20,82%	17,08%	2,68%	15,48%
Австрия	50,00%	14,58%	23,44%	2,08%	9,90%
Бельгия	36,85%	21,77%	15,30%	2,16%	22,41%
Великобритания	44,03%	20,71%	16,46%	2,62%	16,18%
Германия	48,91%	15,08%	21,78%	2,85%	11,39%
Испания	45,04%	25,74%	16,52%	2,26%	10,43%
Италия	48,15%	23,72%	14,94%	2,81%	10,37%
Нидерланды	34,99%	24,32%	16,22%	2,56%	21,91%
Россия	42,58%	31,89%	16,22%	3,69%	5,62%
США	40,94%	19,91%	17,68%	2,82%	18,65%
Франция	53,32%	15,70%	9,47%	2,66%	18,85%
Швейцария	48,60%	18,85%	18,41%	1,77%	12,37%

3.1.2 Количество незащищенных ПК

Очевидно, что большинство пользователей осознают необходимость защиты персонального компьютера. Среди всех участников опроса количество незащищенных компьютеров было сравнительно небольшим и составило едва 4%, т.е. 659 опрошенных пользователей, и это в известной степени хорошо. Почти 5% пользователей не смогли ответить, установлено ли на их компьютерах какое-либо защитное ПО. 1,84% опрошенных заявили, что используют пиратские

копии. Таким образом, можно сделать вывод, что около 6% всех опрошенных не защищены во время Интернет-серфинга. Кроме того, есть подозрение, что ореспонденты, не уверенные, используют ли они защитное ПО, также не защищены.

Низкая осведомленность российских пользователей относительно безопасности

По сравнению с другими странами больше всего незащищенных компьютеров в России. Здесь также используется больше всего нелегальных версий платного защитного ПО (почти 11% пользователей). Всего в России 17% ПК в недостаточной степени защищены от угроз, подстерегающих в Интернете. Лидером - в положительном смысле - является Соединенное Королевство Великобритании. Здесь ответы всего 6% опрошенных указывают на то, что они не защищены.

3.1.3 Пакет антивирусных программ или одна программа?

Таблица 6. Подробные результаты опроса об установленном защитном ПО

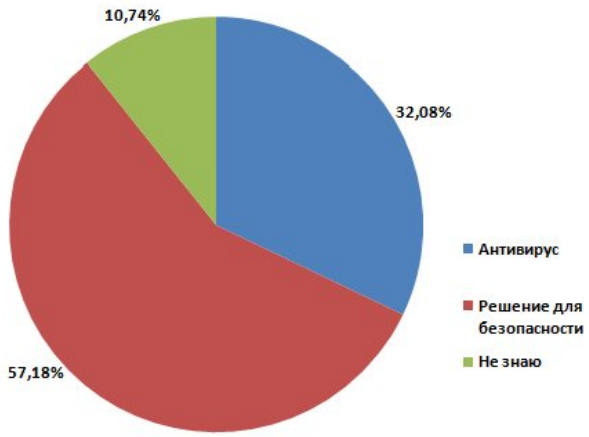
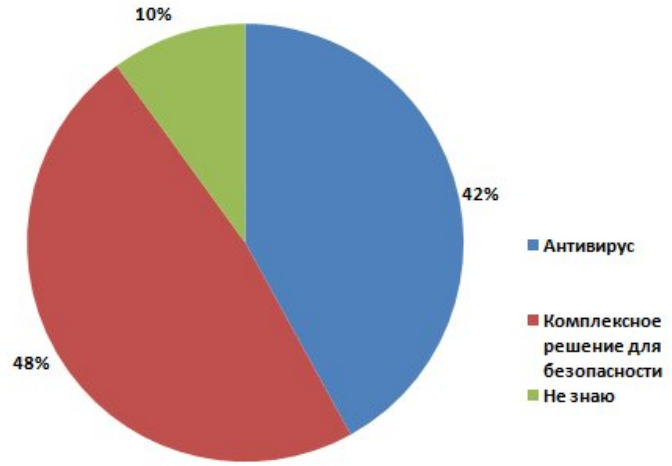


График 7. Какое решение безопасности используют пользователи?

Какой тип защиты?			
	Антивирус	**Решение для безопасности**	**Не знаю**
Мужчины (18-24)	37,00%	55,29%	7,71%
Мужчины (25-34)	35,52%	59,52%	4,95%
Мужчины (35-44)	32,46%	60,69%	6,84%
Мужчины (45-54)	29,55%	63,54%	6,91%
Мужчины (55-64)	29,67%	62,93%	7,40%
Всего мужчин	**32,73%**	**60,57%**	**6,69%**
Женщины (18-24)	36,03%	52,34%	11,64%
Женщины (25-34)	33,86%	53,39%	12,75%
Женщины (35-44)	29,92%	56,13%	13,95%
Женщины (45-54)	28,71%	56,29%	15,01%
Женщины (55-64)	29,23%	51,36%	19,41%
Всего женщин	**31,49%**	**54,05%**	**14,46%**
Всего	**32,08%**	**57,18%**	**10,74%**

Интернет-пользователи знают, что их в Интернете поджидают различные опасности, и от них необходимо защищаться, или нет? Если сравнить результаты упомянутых выше опросов (см. График 2) с вопросом "Какое защитное программное обеспечение установлено на Вашем компьютере?", возникает противоречие, поскольку
если говорить о бесплатных решениях безопасности, то здесь речь идет исключительно об антивирусной защите без дополнительных технологий защиты, таких как брандмауэр, антиспам или веб-защита. Бесплатные пакеты защитного ПО фактически отсутствуют на рынке. Несмотря на это, большинство участников опроса (см. График 7), сообщивших о том, что являются пользователями бесплатного антивирусного ПО, заявили, что они хотели бы иметь пакетное ПО для защиты в Интернете с персональным брандмауэром, антиспамом и веб-защитой.

График 7. Защитное ПО пользователей, которые указали, что используют бесплатное решение безопасности



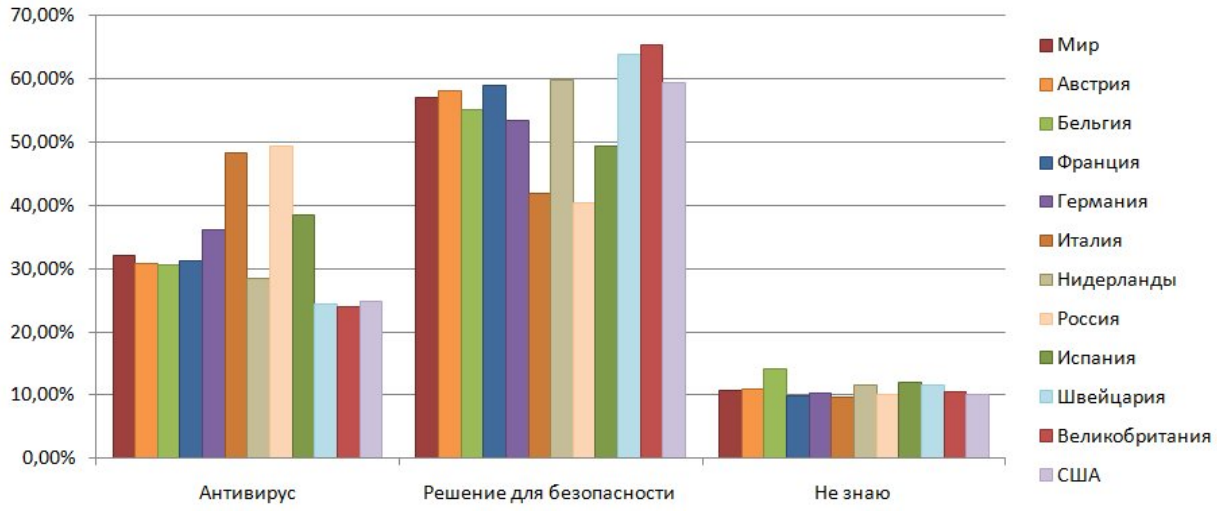
На что указывает это видимое противоречие? Похоже, большинство опрошенных конечных пользователей неправильно оценивают эффективность одной антивирусной программы по сравнению с пакетным ПО для защиты в Интернете и недостаточно информированы об интегрированных технологиях защиты. Большинство рассматривает бесплатную антивирусную защиту и пакетное ПО для защиты в Интернете, независимо от их технологических различий, как равнозначные программы. Это ошибочное мнение, которое может дорого стоить интернет-пользователям, если рассматривать разнообразие способов распространения вредоносного кода.

Таблица 8. Установленное защитное ПО по отдельным странам

Бесплатные антивирусные программы так же эффективны, как и платные пакеты программ?					
	Да	Нет, хуже качество	Нет, меньше элементов	Нет, сильнее	Не знаю
Мир	43,94%	20,82%	17,08%	2,68%	15,48%
Австрия	50,00%	14,58%	23,44%	2,08%	9,90%
Бельгия	36,85%	21,77%	15,30%	2,16%	22,41%
Великобритания	44,03%	20,71%	16,46%	2,62%	16,18%
Германия	48,91%	15,08%	21,78%	2,85%	11,39%
Испания	45,04%	25,74%	16,52%	2,26%	10,43%
Италия	48,15%	23,72%	14,94%	2,81%	10,37%
Нидерланды	34,99%	24,32%	16,22%	2,56%	21,91%
Россия	42,58%	31,89%	16,22%	3,69%	5,62%
США	40,94%	19,91%	17,68%	2,82%	18,65%
Франция	53,32%	15,70%	9,47%	2,66%	18,85%
Швейцария	48,60%	18,85%	18,41%	1,77%	12,37%

В отдельных странах часть пользователей, использующих пакетное защитное ПО, больше, чем использубщих антивирусную защиту. Исключением являются Италия и Россия: здесь это соотношение обратное (см. Таблицу 8).

График 8. Сравнение установленного защитного ПО по странам



3.2 Где больше всего опасностей для интернет-пользователей?

Чтобы получить представление о том, чего опасаются интернет-пользователи, G Data представила опрашиваемым одиннадцать ложных утверждений. Как выяснилось, некоторые из опрашиваемых приняли все эти ложные утверждения за верные. Мы приводим эти высказывания в виде одиннадцати тезисов интернет-безопасности.

3.2.1 Одиннадцать тезисов интернет-безопасности

Тезис 1. Если моя операционная система заражена вредоносной программой, то это так или иначе будет заметно на моем ПК (93%).

Первый тезис наиболее распространен. Почти все интернет-пользователи (93%) во всем мире убеждены в том, что вредоносные программы оказывают заметное воздействие на ПК. Так, более 45% всех опрашиваемых полагают, что в случае заражения вредоносным ПО компьютер сразу "зависает". Почти 57% считают, что в данном случае хотя бы одна из рабочих функций компьютера повреждена или определенное программное обеспечение перестает работать. 58% уверены, что при заражении компьютер выдает различные всплывающие окна и издает странные звуки. И наконец, почти 57% опрашиваемых считают, что компьютер начинает очень медленно работать. Менее 7,5% считают, что в случае заражения ничего необычного не обнаруживается, хотя именно это и происходит в большинстве случаев (см. Таблицу 9).

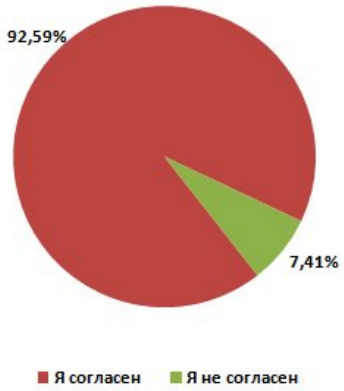


Таблица 9. Что, по мнению опрашиваемых, происходит при заражении компьютера? – Опрашиваемые могли выбирать несколько вариантов ответов.

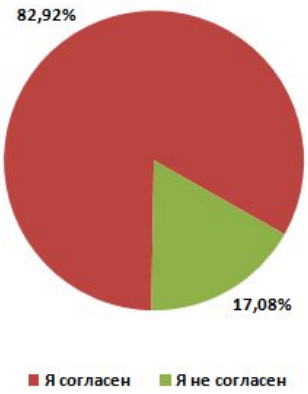
Что произойдет, если Ваш компьютер будет заражен?					
	Сбой в системе компьютера	Некоторые функции компьютера перестанут работать	Начнут происходить странные вещи	Компьютер начнет работать гораздо медленнее	Ничего особенного
Мужчины (18-24)	43,52%	52,24%	56,64%	58,84%	10,45%
Мужчины (25-34)	43,52%	57,46%	58,31%	59,96%	8,37%
Мужчины (35-44)	46,35%	56,33%	58,58%	57,70%	7,99%
Мужчины (45-54)	41,83%	54,57%	58,36%	57,03%	8,83%
Мужчины (55-64)	37,44%	57,42%	54,89%	55,10%	7,10%
Всего мужчин	**42,65%**	**55,71%**	**57,46%**	**57,77%**	**8,50%**
Женщины (18-24)	48,46%	58,18%	64,06%	62,52%	6,43%
Женщины (25-34)	50,17%	59,30%	64,37%	58,13%	5,57%
Женщины (35-44)	47,48%	57,51%	57,12%	55,27%	7,29%
Женщины (45-54)	46,81%	57,86%	56,22%	53,25%	5,65%
Женщины (55-64)	46,00%	57,23%	50,56%	48,17%	7,16%
Всего женщин	**47,85%**	**58,05%**	**58,62%**	**55,53%**	**6,40%**
Всего	**45,35%**	**56,93%**	**58,06%**	**56,60%**	**7,41%**

В прошлом вредоносные программы создавались разработчиками для того, чтобы доказать свои технические способности. Если заражение удавалось, жертва замечала это в виде всплывающих окон, функциональных сбоев или внезапного выхода компьютера из строя. По-видимому, многие хорошо помнят эти вещи. Сегодня же вредоносные коды программируются профессиональными и очень опытными злоумышленниками с целью заработать как можно больше денег. Хорошо прописанная вредоносная программа приносит много денег на черном рынке Интернета. При этом программный код покупают другие злоумышленники, которые используют его, например, для создания бот-сетей с целью доступа к максимально возможному количеству зараженных компьютеров во всем мире. С помощью таких бот-сетей

можно осуществлять, например, т.н. DDoS-атаки, рассылать спам или распространять вредоносное компьютерное ПО. Данный вид теневой экономики хорошо развит: разработчики и администраторы бот-сетей предлагают свое "ноу-хау" и свои услуги на специальных подпольных форумах. Другие злоумышленники покупают эти услуги или вредоносные коды, например, для атаки веб-сайта какой-либо организации или масштабной рассылки спама. Для совершения покупки не требуется никакого технического "ноу-хау".4Разработчики и администраторы бот-сетей следят за тем, чтобы бот-сеть была максимально большой и стабильной. Это означает, что каждый ПК, который вышел из группы, например, если заражение ПК было обнаружено и устранено, является для кибер-преступников экономической потерей. По этой причине вредоносные программы создаются разработчиками таким образом, чтобы заражение ПК не было замечено пользователем. Поэтому сегодня очень маловероятно, что заражение ПК будет проявляться в виде сбоя работы компьютера, его ограниченной производительности, появления странных всплывающих окон или других признаков. Такое изменение очень опасно для пользователей ПК, поскольку только то заражение, которое быстро обнаруживается, можно быстро устранить. Девять из десяти пользователей считают, что вредоносное ПО легко обнаружить. Такие пользователи считают, что если компьютер работает исправно, то он не может быть заражен. Это играет на руку кибер-преступникам.

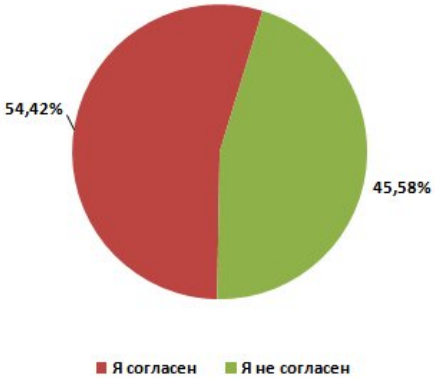
Тезис 2. Бесплатное антивирусное ПО и платное пакетное ПО одинаково защищают от вирусов (83%).

Данное ложное высказывание поддерживает 83%, т.е. большая часть опрашиваемых. Хотя 56% опрошенных при вопросе о различиях качества бесплатного и платного защитного ПО (см. Таблицу 6) выразили сомнение относительно того, что качество обоих видов защитного ПО сравнимо, большинство участников опроса не смогли в целом назвать разницу. 15% не имели никакого понятия, насколько бесплатные продукты безопасности проигрывают платным в отношении эффективности. Почти 3% опрошенных считают, что разница состоит в нагрузке на систему: бесплатное ПО больше нагружает систему, чем платное. Большая разница между платным и бесплатным ПО определяется тем, какие технологии безопасности включает в себя это ПО. Бесплатное защитное ПО предоставляет лишь антивирусную защиту. Платное защитное ПО охватывает больше элементов безопасности: наряду с антивирусной защитой такое ПО, как правило, включает http-фильтр, брандмауэр, антиспамовый модуль и функцию поведенческого распознавания вредоносных кодов. Это было известно только 17% участников опроса.



[4] Дополнительные сведения о теневой экономике см. в бюллетене G Data: http://www.gdata.de/virenforschung/info/whitepaper.html

Тезис 3. Большинство вредоносных программ распространяется по электронной почте (54%)



Данный тезис также устарел, как и первый, но несмотря на это, этойточки зрения придерживается 54% участников опроса. В конце прошлого тысячелетия рассылка вирусов "Melissa" и "I love you" по электронной почте стала наиболее популярным способом распространения вредоносных программ. Заражение вирусом происходило через зараженные вложения, которые рекламировались с помощью приемов социальной инженерии. Многие пользователи помнят сообщения со снимкамиобнаженной российской теннисистки Анны Курниковой. Фактически каждый, кто открывал такое вложение, устанавливал вирус на свой компьютер. Приблизительно шесть лет назад на смену отправке электронных сообщений с зараженными вложениями пришли сообщения с ссылками на файлы, размещенные на веб-сайтах (хотя уже несколько месяцев случаи использования файловых вложений снова переживают подъем). Данная тактика позволяла злоумышленникам обходить очень эффективные спам-фильтры и доставлять сообщения ничего не подозревающему пользователю. С другой стороны, многие пользователи стали очень осторожны с сообщениями от неизвестных отправителей и в лучшем случае сразу удаляют их, не открывая. В большинстве случаев ссылки в электронных сообщениях направляют на вредоносные веб-сайты. Таким образом появляются дополнительные возможности для поиска жертв: например, социальные сети (см. раздел 3.3), оптимизация поисковых запросов, ошибочные домены и т.д. Вредоносные программы находятся на веб-сайтах, а веб-сайты являются вектором заражения номер один.

Тезис 4. Заражение ПК не происходит при загрузке зараженного веб-сайта (48%).

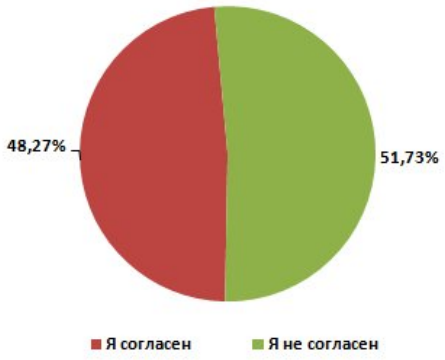
То, что почти половина интернет-пользователей считают данное утверждение правильным, шокирует. Заражение компьютера вредоносными кодами посредством вирусов "попутной загрузки" возможно уже на протяжение многих лет. Одного лишь посещения соответствующего интернет-сайта достаточно для заражения вирусом. Гипотеза о том, что одной лишь загрузки недостаточно для заражения, является опасным ложным заключением, поскольку данный вид атаки практикуется изо дня в день.

Существует два варианта заражения при "попутной загрузке". Во-первых, существуют веб-сайты, созданные специально с целью заражения ПК. Кибер-преступники пытаются заманить жертв на зараженные веб-сайты, публикуя в социальных сетях ссылки, содержащие интересное описание, а также размещая баннеры или рассылая электронные сообщения со встроенными ссылками.

Второй вариант более утонченный: вредоносный код внедряется на один из заслуживающих доверия популярных в настоящее время интернет-сайтов. Так, скажем, открывается незаметное для интернет-пользователя окно, например, размером 0x0 пикселей. Через это окно начинается загрузка, посредством которой происходит автоматическое и скрытое

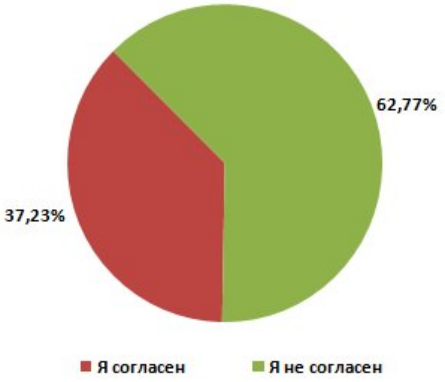
заражение ПК вредоносной программой. Преимуществом данного способа для кибер-преступников является то, что им не приходится рекламировать веб-сайт. Для дальнейшей манипуляции данным веб-сайтом злоумышленникам необходимо в него внедриться. Если веб-сайт хорошо защищен, чтоможно сказать лишь о малой части сайтов, то осуществить такое внедрение очень сложно.

Тезис 5. Большинство вирусов и вредоносных компьютерных программ распространяются посредством зараженных файлов на файлообменниках, таких как одноранговые сети и торренты (48%).



Бесспорно, определенное количество вредоносных программ распространяется через такие системы обмена файлами, как торренты и одноранговые сети. Неудивительно, что 48% участников опроса считают, что данный способ является основным в распространении вредоносного ПО. Наверняка тот или другой пользователь уже хотя бы раз заражал свой компьютер вирусом после посещения подобных сайтов. Однако данный тезис также ложен и является мифом, поскольку большинство вредоносных программ (как упоминалось раньше) распространяется через вредоносные веб-сайты.

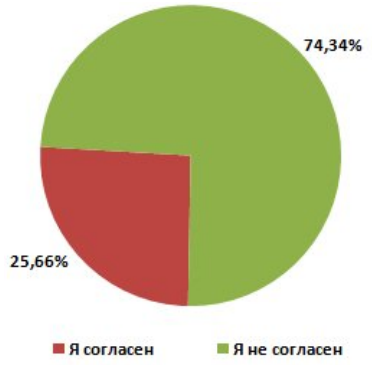
Тезис 6. Риск встретить вредоносное ПО на порносайтах выше, чем, например, при посещении сайтов о конном спорте или о путешествиях (37%).



Порнография имеет подозрительную репутацию. Поэтому вовсе неудивительно, что многие (37% опрашиваемых) предполагают в данном случае о существовании связи с интернет-преступностью. Однако нельзя с уверенностью утверждать, что на самом деле порносайты оказываются зараженными чаще, чем сайты, посвященные конному спорту и другим темам досуга. В порноиндустрии крутится много денег. Для владельца порносайтов интернет-сайт представляет основной источник доходов. Поэтому, как правило, такие сайты разрабатываются, обслуживаются и защищаются профессионалами. Платежеспособный клиент, который во время посещения порносайта заражает свой ПК вредоносным ПО, был бы потерян для владельца этого сайта, что означало бы для него финансовый убыток. Владелец сайта, для которого данный сайт всего лишь хобби, вряд ли является профессиональным веб-дизайнером и поэтому вряд ли регулярно обновляет необходимое программное обеспечение и патчи для того, чтобы закрыть уязвимые места безопасности. Таким образом, преступникам легче внедриться в такие веб-сайты и разместить там вредоносные коды, чем сделать это на профессионально защищенных порносайтах. К тому же, подобные веб-сайты очень просто найти в Google: для этого необходимо всего лишь знать название одного из приложений и его пробелы в безопасности. Таким образом можно обнаружить множество веб-сайтов, которыми легко манипулировать. В целом порносайты

могут огут быть опасны, если они имеют сомнительное происхождение; если речь идет о серьезных секс-сайтах, то уровень потенциальной опасности на них не так высок.

Тезис 7. Мой брандмауэр защищает меня от заражения при "попутной загрузке" (26%).

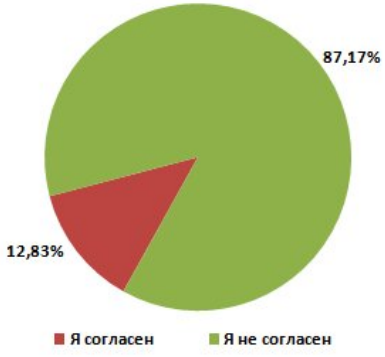


Данному утверждению верит 26% опрашиваемых. Этот тезис ложен. Брандмауэры -— это важная составляющая защиты компьютера. Однако невозможно защитить ПК от заражений при "попутной загрузке" с помощью одного лишь брандмауэра. Для полной и эффективной защиты интернет-пользователь должен дополнительно установить комплексное решение безопасности с интегрированной веб-защитой. При успешном заражении компьютера брандмауэр не всегда может предотвратить выполнение вредоносных заданий вредоносной программой и, например, отправку данных злоумышленникам, если речь идет о шпионских программах.

Тезис 8. Если не открывать зараженные файлы, то ПК нельзя заразить (22%).

Это высказывание, как и некоторые другие, основано на устаревших сведениях, которые до сегодняшнего дня сохранились в виде полузнаний, и которым верит почти 22% участников опроса. Разумеется, заражение компьютера почти всегда происходит, когда пользователи открывают опасные файлы. Однако автоматическое исполнение вредоносных файлов возможно тишь в том случае, если злоумышленники используют существующие пробелы в безопасности. В таком случае вредоносные коды активируются без открывания зараженного файла. Поэтому всегда следует исходить из того, что зараженные файлы опасны для пользователей ПК и могут исполняться независимо от действий пользователя.

Тезис 9. Большинство вредоносных программ распространяется через USB-накопители (12,83%).



Мы выяснили, что большинство вредоносных программ распространяется с помощью вредоносных веб-сайтов, но возможны и другие пути заражения. В 80-е - 90-е гг., когда Интернет еще не был столь доступным, часто источниками заражения были дискеты. В последние годы популярность "флешек" и других съемных USB-накопителей значительно возросла среди кибер-преступников. Здесь используются функции автозапуска носителя данных для исполнения вредоносных программ при его подсоединении к ПК. Самым ярким примером является червь Conficker. Поэтому

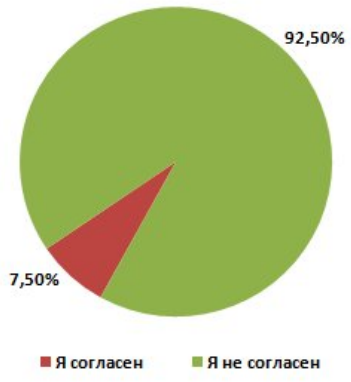
настоятельно рекомендуется отключить функцию автоматического запуска файлов операционной системой. Таким образом можно предотвратить автоматическую установку червя компьютером при подсоединении USB-накопителя.

Тезис 10. Я не посещаю странные веб-сайты, поэтому мне не угрожает заражение при "попутной загрузке" (13%).

Данное утверждение можно опровергнуть так же, как и шестой тезис ("Риск встретить вредоносное ПО на порносайтах выше, чем, например, при посещении сайтов о конном спорте или о путешествиях"). Тематика веб-сайта не играет для кибер-преступников никакой роли. Они заинтересованы в том, чтобы с минимальными затратами заразить вредоносными кодами максимальное количество посетителей. Это удается злоумышленникам, помимо всего прочего, с помощью манипуляций с баннерами и постоянных атак крупных доменов. В случае успеха и получения доступа они внедряют вредоносный код с помощью т.н. эксплойт-инструментов, и специальные знания для этого не требуются. Веб-сайты, которые на протяжение многих лет считались достойными доверия, могут очень быть взломанными и в результате таить в себе опасность заражения. Однако данный тезис считают правдивым всего лишь 13% опрошенных.

Тезис 11. Кибер-преступников не интересуют компьютеры частных лиц (8%).

К счастью, этому высказыванию верят наименее, и только лишь 8% считают этот тезис правильным. В данном случае утверждение также ложно. Разумеется, корпоративные сети очень интересуют кибер-преступников. Но в целом такие сети сложнее заразить. Сегодня частные компьютеры также очень производительны и хорошо подходят в качестве составляющих ботсетей. К тому же, очень часто на них хранится много интересных персональных данных, таких как данные доступа к онлайн-магазинам, социальным сетям и учетным записям электронной почты или данные о кредитных картах, из которых кибер-преступники могут извлечь выгоду. Поэтому не стоит недооценивать значение частных компьютеров для злоумышленников.



3.2.2 Кто информирован лучше: более молодые и более старшие интернет-пользователи?

Молодые интернет-пользователи от 18 до 25 лет в значительной мере выросли с компьютером и Интернетом. Следовательно, данная группа пользуется Интернетом очень активно. В отношении более старших опрошенных возрастом от 55 до 64 лет ситуация выглядит иначе. Данное исследование проводилось исключительно в режиме онлайн. Следовательно, все опрошенные активны в Интернете. Разве что для людей в возрасте среди опрошенных данное

средство коммуникации относительно ново. Поэтому вполне естественно было бы предположить, что младшее поколение знает об опасностях в Интернете намного больше, чем старшее. Однако иная гипотеза гласит о том, что в результате относительного незнания Интернета и компьютера старшее поколение везде видит опасность и поэтому ведет себя более осторожно в сети.

Чтобы узнать, как у молодого и старшего поколений опрашиваемых обстоят дела с информированностью, мы проверили, насколько обе группы доверяют вышеуказанным тезисам. Результаты представлены в таблице ниже.

Таблица 10. Кто больше верит указанным тезисам: более молодые или более старшие пользователи

Мифы	18-25 лет	55-64 лет	Всего
1) Если мой компьютер инфицирован вирусами, я сразу об этом узнаю	91,68%	92,87%	92,59%
2) Бесплатные антивирусные решения предлагают такой же набор элементов, что и платные	82,17%	83,17%	82,92%
3) Большинство вирусов и других видов вредоносного программного обеспечения распространяются через электронную почту	46,54%	61,46%	54,42%
4) Вы не сможете заразить свой компьютер вирусами, посетив зараженный веб-сайт	53,42%	46,67%	48,33%
5) Большинство вредоносного программного обеспечения распространяется через зараженные файлы, которые были загружены из P2P-сетей и торрент-сайтов	53,42%	45,67%	48,27%
6) Возможность заражения компьютера выше при посещении порно-сайтов, чем сайтов о верховой езде	39,18%	35,40%	37,23%
7) Файервол может защитить мой компьютер от опасности при скачивании файлов	32,89%	17,47%	25,66%
8) Мой компьютер не будет инфицирован вирусом, если я не открою зараженный файл	22,42%	25,13%	21,88%
9) Большинство вредоносного программного обеспечения распространяется через разраженные флеш-карты	16,91%	9,02%	12,83%
10) Я не посещаю небезопасные сайты, поэтому я защищен от вирусов, которые загружаются во время скачивания файлов	14,39%	13,69%	12,66%
11) Киберпреступники не заинтересованы в компьютерах частных пользователей	10,03%	6,77%	7,50%

Если посмотреть на столбец с ответами молодых пользователей, результат, в основном, положительный. Молодое поколение менее доверяет трем главным тезисам, однако этот процент мало отличается от среднего процента опрошенных. А вот четвертый тезис, представляющий собой очень опасное заблуждение, поскольку он касается возможности заражения при "попутной загрузке", молодые люди считают правдивым гораздо чаще, чем другие опрашиваемые. Это же касается и пятого тезиса относительно наличия вредоносного ПО на таких системах обмена файлами, как торренты и одноранговые сети. Возможно, причиной этому является то, что молодое поколение загружает очень много файлов с подобных сайтов и при этом сталкивается с уже зараженными файлами.

Также молодые респонденты подозревают о большем риске заражения на порносайтах, чем старшие участники опроса. Вероятно, младшее поколение хуже информировано относительно того, какими функциями обладает брандмауэр. Это противоречит гипотезе о том, что молодые пользователи хорошо знают технологии, с которыми растут. Молодому поколению также менее известен тот факт, что для заражения вирусом не обязательно открывать файл. Кроме этого, молодые участники опроса считают, что USB-накопители — это главный источник заражения вредоносным ПО. Молодые опрашиваемые больше других возрастных групп переоценивают свои знания о возможности избежать заражения при "попутной загрузке". Кроме того, больший процент молодежи, по сравнению со средним показателем, считает, что их частные компьютеры интересны киберпреступникам.

В целом молодые опрашиваемые не слишком вырвались вперед. Их уровень знаний даже ниже, чем уровень знаний среднестатистического интернет-пользователя, поэтому гипотеза относительно того, что молодые люди должны знать Интернет лучше других возркастных категорий, потому что они росли с этой технологией, необоснованна.

При рассмотрении столбца, который касается опрашиваемых старшего возраста, видно, что старшее поколение больше доверяет трем главным тезисам, чем среднестатистический опрашиваемый. Однако в отношении четвертого тезиса об атаках вирусов для "попутной загрузки" возникает другая картина. Видимо, опрашиваемые старшего возраста информированы об опасностях таких атак намного лучше, чем более молодые возрастные группы и, прежде всего, лучше, чем совсем молодые пользователи. Но при этом остается повод для беспокойтсва, поскольку среди людей старшего возраста почти каждый второй опрашиваемый считает, что вирусов "попутной загрузки" не существует. В среднем многие участники опроса старшего возраста считают, что файлообменники являются основным источником заражения вредоносным ПО. При этом разница межу этим показателем и среднестатистическим незначительная. Порносайты вызывают у старшего поколения меньше недоверия, чем у среднестатистического числа опрошенных. Люди старшего возраста меньше доверяют защитным функциям брандмауэра от вирусов "попутной загрузки", чем молодые опрашиваемые. Зато старшие респонденты чаще придерживаются мнения, что невозможно заразиться вирусом, если не открывать файл, что в сущности противоречит ранее высказанному убеждению относительно опасности заражения при "попутной загрузке". USB-накопители рассматриваются старшим поколением в качестве основного источника распространения вредоносного ПО намного реже, в чем они правы. Менее оправдана повышенная уверенность в безопасности собственных привычек работы в Интернете, которая, с точки зрения более старших опрашиваемых, лучше защищает от атак вирусов "попутной загрузки". Тем не менее, люди старшего возраста менее легкомысленны, чем молодежь и признают, что их ПК могут представлять интерес для киберпреступников.

В итоге старшее поколение также не лидирует в опросе, хотя его представители явно лучше представляют себе опасности в Интернете, чем молодые опрашиваемые. Из данного анализа можно сделать вывод, что возрастная группа от 25 до 54 лет может похвастаться лучшим знанием опасностей Интернета. Однако необходимо указать на то, что в этих возрастных

группах существует много ложных убеждений по данной теме, и что знания данных опрошенных также недостаточны.

3.2.3 В какой стране интернет-пользователи лучше всего информированы об опасностях?

Существует много предубеждений относительно того, в каких странах пользователи информированы лучше, а в каких хуже. Так, например, многие уверены в том, что американцы и британцы хорошо информированы об интернет-угрозах, а итальянцы и русские, наоборот,. Чтобы узнать, действительно ли существуют страны, в которых интернет-пользователи информированы об опасностях намного лучше или хуже, в Таблице 11 в процентном эквиваленте приведено количество опрошенных, которые верят в вышеупомянутые мифы. Зеленый цвет указывает на страны, в которых тезисам доверяют меньше. Красный цвет указывает на страны, в которых с тезисами совершенно согласны.

Таблица 11. В какой стране больше всего доверяют тезисам?

Мифы	Нидерланды	Бельгия	Франция	Испания	США	Италия	Германия	Россия	Великобритания	Австрия	Швейцария	Мир
1) Заметное заражение	86,63%	93,97%	92,28%	95,30%	94,29%	94,38%	83,17%	97,88%	91,40%	86,46%	90,13%	92,59%
2) Бесплатный антивирус	83,78%	83,19%	90,53%	83,48%	82,32%	85,06%	78,22%	83,78%	83,54%	76,56%	81,59%	82,92%
3) Зараженное электронное сообщение	58,89%	62,18%	57,64%	58,61%	52,37%	58,88%	52,85%	38,80%	52,89%	55,47%	57,73%	54,42%
4) Зараженный веб-сайт	51,49%	49,03%	49,25%	57,83%	40,95%	63,44%	62,90%	48,48%	42,85%	60,68%	54,93%	48,33%
5) Торрен-сайтов и P2P-сети	43,53%	46,76%	48,17%	52,43%	52,73%	45,52%	35,26%	49,49%	48,73%	41,02%	44,48%	48,27%
6) Зараженный порно-сайт	25,32%	34,27%	31,89%	32,43%	40,13%	32,25%	30,65%	60,18%	35,80%	34,11%	36,23%	37,23%
7) Файервол	31,44%	28,34%	18,77%	26,78%	24,32%	28,03%	29,31%	17,05%	24,95%	28,26%	29,16%	25,66%
8) Зараженный файл	16,50%	26,29%	23,59%	30,78%	18,18%	30,67%	13,32%	38,53%	20,43%	14,06%	18,56%	21,88%
9) Зараженная флеш-карта	8,11%	10,67%	17,28%	20,09%	9,92%	15,38%	8,38%	30,05%	10,49%	8,72%	8,98%	12,83%
10) Небезопасные сайты	18,07%	13,69%	14,78%	14,00%	10,79%	17,84%	11,81%	11,89%	9,67%	12,50%	14,14%	12,66%
11) Компьютеры конечных пользователей	5,12%	6,90%	5,98%	8,87%	7,50%	8,35%	7,20%	6,54%	8,77%	9,90%	6,63%	7,50%

Данная таблица демонстрирует, что опрашиваемые из Германии лучше других информированы об опасностях в Интернете, С и меньше всего доверяют трем тезисам. То же можно сказать и о Нидерландах. Однако при этом следует принять во внимание то, что Нидерланды, оценивая утверждения, дважды оказывались самыми далекими от правды. Интересно, что американцы, от которых, возможно, ожидался более высокий уровень

информированности об опасностях в Интернете, , лишь только на четвертом тезисе продемонстрировали наименьшее количество пользователей, которые ему доверяют. Больше всего американские респонденты верят тезису о том, что в основном вредоносные коды распространяются через файлообменники. Тем не менее, хуже всех информированы об опасностях Интернета вовсе не американцы — процессию замыкает Россия. Среди всех других россияне больше всего верят в четыре ложных высказывания. С другой стороны, то, что они менее других верят в два другие мифа, избавляет их от последнего места в данном опросе.

3.2.4 Являются ли мужчины лучшими интернет-пользователями?

Многие люди глубоко (и неосознанно) убеждены, что мужчины лучше разбираются в технике, чем женщины. Если данное убеждение верно, то мужчины также должны быть лучше информированы, чем женщины относительно того, какие опасности существуют в Интернете, и какие страхи устарели или нереалистичны. Правда ли это? Приведенная ниже таблица демонстрирует оценку мифов, связанных с Интернетом, со стороны мужчин и женщин.

Таблица 12. Кто больше верит утверждениям: мужчины или женщины?

Мифы	Мужчины	Женщины	Всего
1) Если мой компьютер инфицирован вирусами, я сразу об этом узнаю	91,50%	93,60%	92,59%
2) Бесплатные антивирусные решения предлагают такой же набор элементов, что и платные	84,01%	81,73%	82,92%
3) Большинство вирусов и других видов вредоносного программного обеспечения распространяются через электронную почту	54,53%	54,31%	54,42%
4) Вы не сможете заразить свой компьютер вирусами, посетив зараженный веб-сайт	48,19%	48,46%	48,33%
5) Большинство вредоносного программного обеспечения распространяется через зараженные файлы, которые были загружены из P2P-сетей и торрент-сайтов	49,13%	47,47%	48,27%
6) Возможность заражения компьютера выше при посещении порно-сайтов, чем сайтов о верховой езде	43,88%	31,07%	37,23%
7) Файервол может защитить мой компьютер от опасности при скачивании файлов	26,02%	25,32%	25,66%
8) Мой компьютер не будет инфицирован вирусом, если я не открою зараженный файл	22,65%	21,16%	21,88%
9) Большинство вредоносного программного обеспечения распространяется через разраженные флеш-карты	13,47%	12,24%	12,83%
10) Я не посещаю небезопасные сайты, поэтому я защищен от вирусов, которые загружаются во время скачивания файлов	11,74%	13,51%	12,66%
11) Киберпреступники не заинтересованы в компьютерах частных пользователей	8,75%	6,35%	7,50%

Таблица указывает на то, что женщины явно чаще оказываются ближе к правде, чем мужчины. Только в отношении трех ложных утверждений женщины ошибались чаще, чем мужчины. Однако вывод, что женщины являются лучшими интернет-пользователями, остается под вопросом. В большинстве случаев процентные показатели отличаются друг от друга менее, чем на 2%.

Явное различие в ответах мужчин и женщин относится к тезису "Риск встретить вредоносное ПО на порносайтах выше, чем, например, при посещении сайтов о конном спорте или о путешествиях". Почему этому ложному утверждению мужчины верят намного чаще, вероятно, можно объяснить также, как и ответы молодых опрошенных, которые больше всего доверяют утверждению "Большинство вирусов и вредоносных компьютерных программ распространяются посредством зараженных файлов на файлообменниках, таких как одноранговые сети и торренты". Если какая-либо целевая группа имеет больше опыта в обращении с подобными веб-сайтами, то, возможно, опрашиваемые из этой группы чаще встречается с вредоносным ПО на данных веб-сайтах. Тем не менее, это не доказывает верности утверждения. Разве мужская часть опрашиваемых также часто посещает веб-сайты, посвященные конному спорту? А если бы это было и так (и ни на каком из данных веб-сайтов не произошло заражение вредоносным ПО), то не могло бы это быть совпадением? Женщины, вероятно, имеют меньше опыта в посещении порносайтов и поэтому, скорее всего, не сталкивались с атаками вирусов "попутной загрузки" на таком сайте. Вероятно, поэтому, по мнению женщин, порносайт является таким же опасным или безопасным, как и любой другой сайт в Интернете. Еще одним объяснением разных результатов опросаможет быть разный психологический подход. Большинство людей считают порнографию чем-то неприличным и плохим, тем, что следует смотреть тайком. Если у человека есть ощущение, что он делает что-то запрещенное, то, возможно, он в большей степени ожидает получить за свое поведение какое-то наказание. В данном случае таким наказанием является заражение вредоносной программой. Статистически доказано, что потребителями порнографии больше являются мужчины, чем женщины, и поэтому мужчины подозревают о возможности столкнуться с вредоносными кодами на порносайтах.

Наряду с вопросом о порносайтах существует еще оно утверждение, которое мужчины и женщины оценивают по-разному: мужчины чаще дают положительный ответ на вопрос относительно того, что их частные компьютеры не представляют интереса для киберпреступников. Женщины менее уверены в данном утверждении. Возможно, это объясняется тем, что женщины в целом более осторожно обращаются со своими ПК, а, возможно, они менее уверены в данном отношении, и мужчины больше готовы идти на риск. А может быть, это утверждение прежде всего является надеждой мужской части опрашиваемых.

3.3 Поведение в социальных сетях

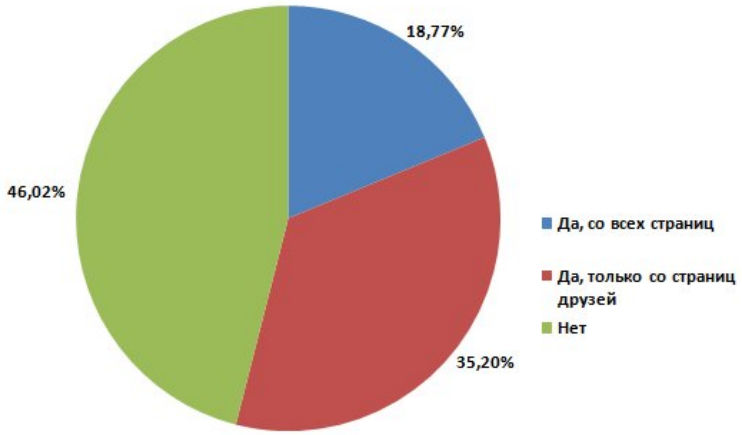
Социальные сети становятся все популярнее и превращаются в неотъемлемую составляющую Интернета. На сайтах Facebook, Twitter и им подобных пользователи часто общаются с друзьями из разных стран. Разумеется, большая популярность социальных сетей все больше

привлекает злоумышленников, которые используют социальные порталы в своих криминальных махинациях.

У мошенников появляется все больше возможностей нанести вред пользователям: можно украсть данные пользователя для входа в сеть с помощью "классического" фишинга с использованием вводящих в заблуждение веб-сайтов или путем кражи базы данных провайдера. Другой очень распространенной лазейкой преступников на социальных платформах является распространение вредоносных интернет-адресов через доски объявлений, чаты или отправку личных сообщений. Такие рассылки содержат, например, ссылку на видеозапись.

Рекламируемые адреса веб-сайтов иногда так сокращаются с помощью сервисов сокращения URL, что пользователь не замечает даже намека на риск. Нажатие на такую ссылку ведет к переходу на внешний интернет-сайт, содержащий вредоносный код, ворует данные путем фишинга или с помощью клик-джекинга превращает жертву в распространителя спама. При этом пользователь отправляет эту ссылку своим друзьям, даже не подозревая об этом. Поэтому при получении ссылок от неизвестных лиц необходимо быть осторожным. Друзья также могут распространять подобные интернет-адреса, например, если учетная запись пользователя была взломана и используется злоумышленником. Из-за высокого уровня опасности исследование безопасности G Data 2011 содержало вопрос о том, переходят ли пользователи по ссылкам в социальных сетях.

График 9. Переход по ссылкам в социальных сетях



Большинство опрошенных в рамках исследования переходят по предложенным в социальных сетях ссылкам. 46% всех опрошенных не переходят по URL-адресам сайтов, независимо от того, получены ли они от друзей или от неизвестных лиц. Больше одной третей опрошенных доверяют интернет-адресам, опубликованным друзьями из той же сети. Только 19% переходят по ссылкам, независимо от того, кто их отправил, и таким образом легко становятся целью киберпреступников и их незаконных действий.

По сравнению с другими странами больше других выделяется Франция

60% французов не переходят по ссылкам в социальных сетях. Показатель Франции является наивысшим по сравнению с остальными странами. 18% переходят по ссылкам на интернет-сайты, которые приходят от всех пользователей. Этот показатель один в один совпадает со

средним значением по странам. Кроме этого, только 21% опрошенных переходит по ссылкам, которые были размещены на социальной платформе друзьями пользователей. По сравнению с показателями других стран и средним значением данный показатель самый низкий. Таким образом, французы оказались самыми восприимчивыми к опасностям, которые представляют собой ссылки на веб-сайты в социальных сетях.

График 10. Переход по ссылкам в социальных сетях по странам

Меньше других знают об опасностях ссылок опрашиваемые из России: больше одной четвертой участников опроса указали, что переходят по ссылкам, полученным как от знакомых, так и от незнакомых пользователей социальной сети, и таким образом стали лидером данного варианта ответа. Только 35% вовсе не переходят по ссылкам на другие веб-сайты. 37% опрошенных россиян открывают только ссылки, полученные от друзей.

Таблица 13. Переход по ссылкам в социальных сетях по отдельным странам.

Вы переходите по ссылкам в социальных сетях?			
	Да, со всех страниц	**Да, только со страниц друзей**	**Нет**
Мир	18,77%	35,20%	46,02%
Австрия	22,27%	42,45%	35,29%
Бельгия	17,34%	34,80%	46,17%
Великобритания	14,29%	31,46%	54,25%
Германия	22,95%	38,36%	38,69%
Испания	18,43%	45,04%	36,52%
Италия	21,44%	33,66%	44,90%
Нидерланды	17,50%	34,14%	48,36%
Россия	27,74%	37,14%	35,12%
США	15,79%	34,80%	49,41%
Франция	18,77%	21,01%	60,22%
Швейцария	23,71%	38,14%	38,14%

3.3.1 Кто чувствует себя более уверенно в социальных сетях: мужчины или женщины?

Исследование безопасности G Data указывает на то, что между мужчинами и женщинами в отношении использования ссылок в социальных сетях действительно есть разница. Как и следовало ожидать, в социальных сообществах женщины ведут себя более осмотрительно.

Однако разница совсем небольшая: 47% женщин игнорируют ссылки на социальных платформах, в то время как то же самое можно сказать о 45% мужчин. Зато мужчины, наоборот, чаще открывают ссылки, которые не обязательно были опубликованы знакомыми из сети друзей. Женщины в два раза чаще открывают ссылки от друзей, чем ссылки от других пользователей социальной платформы. Среди мужчин почти одна треть опрошенных, скорее, отдают предпочтение интернет-адресам, полученным от друзей, чем от других пользователей.

Таблица 14. Подробные результаты опроса (общий результат по всем странам)

Вы переходите по ссылкам в социальных сетях?			
	Да, со всех страниц	Да, только со страниц	Нет
Мужчины (18-24)	26,24%	38,02%	35,74%
Мужчины (25-34)	25,92%	38,63%	35,45%
Мужчины (35-44)	21,09%	33,56%	45,35%
Мужчины (45-54)	18,23%	31,10%	50,66%
Мужчины (55-64)	15,93%	26,21%	57,86%
Всего мужчин	**21,46%**	**33,55%**	**44,99%**
Женщины (18-24)	21,54%	45,38%	33,08%
Женщины (25-34)	20,43%	40,92%	38,64%
Женщины (35-44)	15,41%	35,59%	48,99%
Женщины (45-54)	13,72%	31,27%	55,01%
Женщины (55-64)	9,83%	30,48%	59,69%
Всего женщин	**16,29%**	**36,73%**	**46,99%**
Всего	**18,77%**	**35,20%**	**46,02%**

Результаты по отдельным странам, за исключением Италии, Бельгии и Австрии почти одинаковы. Женщины в этих странах также ведут себя более осмотрительно в социальных сетях и игнорируют переход по ссылкам в целом или если ссылки были отправлены неизвестным пользователем. По сравнению с мужчинами они делают это чаще, даже если разница в поведении обоих полов, как правило, незначительная. Результаты исследования безопасности, проведенного в Италии, Бельгии и Австрии указывают на совершенно противоположное поведение: кажется, здесь мужчины менее восприимчивы к опасностям, которые представляют собой ссылки на социальных платформах. Разрыв в показателях здесь также минимален.

Также видно, что разница между мужчинами и женщинами присутствует, но незначительная. Таким образом, нельзя сделать четкий вывод относительно того, что один из полов более осторожно ведет себя в социальных сетях.

3.3.2 Кто чувствует себя более уверенно в социальных сетях: молодые или более старшие пользователи?

Молодые интернет-пользователи, как известно, чаще общаются в социальных сетях и пользуются ими гораздо больше, чем старшие пользователи. Несмотря на это, как показывает общий результат исследования, старшее поколение ведет более осторожно с социальными платформами. Особенно осмотрительными среди мужчин и женщин оказались в равной степени обе возрастные категории — от 45 до 54 и от 55 до 64 лет (см. Таблицу 14).
Больше половины участников опроса указанного возраста категорически отклоняют переход по ссылкам в социальных сетях. Женщины этого поколения даже немножко более критичны в данном отношении, чем их ровесники-мужчины. Три более младших возрастных категории (до 44 лет), как и следовало ожидать, явно предпочитают переходить по ссылкам на веб-сайты, опубликованные как знакомыми, так и незнакомыми пользователям

Вывод: поколение интернет-пользователей в зрелом возрасте на шаг впереди

Чем старше опрашиваемые мужчины и женщины, тем реже они переходят по ссылкам на внешние интернет-сайты, размещенные в социальных сетях. При этом не имеет значения, публикуют ли эти ссылки знакомые или незнакомые люди. Тогда как среди мужчин в возрасте от 55 до 64 лет отклоняют ссылки почти 58%, среди мужчин в возрасте от 18 до 24 лет это делают только 36%. В отношении женщин эта разница еще больше: среди женщин самого старшего возраста ссылки отклоняют 60% по сравнению с одной третей женщин в возрасте от 18 до 24 лет. Чем младше возраст опрошенных женщин, тем чаще они переходят по ссылкам от известных и от неизвестных лиц. То же самое можно сказать в отношении писем со ссылками от знакомых из круга друзей.

Осторожность более старших пользователей может иметь больше причин. Конечно же, старшее поколение, как правило, более неуверенно в обращении с социальными сетями. Такая форма участия и общения ему не так хорошо знакома, как молодому поколению. Поэтому у некоторых людей старшего возраста при использовании социального портала может возникать элементарная неуверенность. Люди старшего возраста пользуются (как уже упоминалось выше) социальными сетями не так интенсивно, как молодые пользователи, и также проводят там не так много времени. К тому же существует вероятность, что люди из списка контактов пользователей данной возрастной группы не публикуют или очень редко публикуют внешние ссылки, и, таким образом, опрашиваемые просто не сталкиваются с этот темой. Еще одна точка зрения состоит в том, что молодые интернет-пользователи воспринимают сам Интернет, а также социальные сети как своего рода инструмент: с его помощью можно поддерживать или создавать новые контакты, проводить время и делиться личным.

4. Выводы

Сначала из данного исследования можно сделать очень положительный вывод: большинство интернет-пользователей, независимо от возраста, пола или национальной принадлежности, знают о существовании опасностей в Интернете. При этом, к сожалению, знаний большинства пользователей несколько недостаточно, поэтому лишь немногие опрашиваемые смогли правильно указать опасности, которые существуют сегодня в Интернете. Уровень знаний о том, как пользователи могут эффективно защитить себя от вредоносных программ, также очень низкий среди участников опроса. Следовательно, лишь немногие знают, как эффективно защититься от подстерегающих угроз. Кроме этого, оказывается, существует очень много ошибочных гипотез об интернет-угрозах. Знания почти всех участников о вирусах и других вредоносных кодах при этом базируются на полностью устаревших фактах. Существует множество страхов перед опасностями, которые сегодня возникают все реже, например, массовая рассылка электронных сообщений, содержащих вредоносные программы (54% считают, что компьютерные вредоносные программы распространяются именно таким способом), или предположение относительно того, что вредоносное ПО каким-либо образом ухудшает работу ПК (так считает 92%). Несмотря на то, что такие случаи имели место в девяностых годах и частично в первом десятилетии нового века, они уже давно не возникают. Сегодня большинство вредоносных программ написаны так профессионально, что они почти незаметны для пользователя ПК. Одним из немногих исключений являются, например, поддельные программы обеспечения безопасности, т.н. ложные антивирусы (англ. "rogueware"). Что касается заблуждения о том, что большинство вредоносных программ рассылаются по электронной почте, то это вряд ли создает проблемы. С электронными сообщениями всегда рекомендуется быть начеку. Как и раньше, переход по ссылкам и открытие приложений являются рискованными. Бдительность здесь, точно, не навредит. Другой пример — представление о том, что вредоносная программа отрицательно влияет на работу компьютера — создает больше проблем. Когда пользователь не замечает ничего необычного в работе своего компьютера, он тешит себя мнимой безопасностью. Как уже упоминалось выше, сегодня заражение вредоносными кодами не заметно для пользователей. Вредоносная программа способна долго выполнять свое предназначение и приносить выгоду злоумышленнику.

Очередным неутешительным фактом является то, что опасности, которые представляют собой веб-сайты, относительно неизвестны. Почти половина опрашиваемых не верит в существование вирусов "попутной загрузки". 48% участников опроса не считают, что можно заразить свой компьютер, просто посетив зараженный веб-сайт. В настоящее время данный способ заражения киберпреступники чаще всего используют для распространения вредоносного ПО. Те пользователи, которые слышали или знают о заражении при "попутной загрузке", часто имеют четкое представление о том, где, прежде всего, можно встретить такие зараженные веб-сайты. Мужчины (почти 44%), прежде всего, подозревают, что уровень опасности порносайтов выше среднего. Более того они считаю, что зараженные веб-сайты не случайно разбросаны по всему Интернету. При этом тот факт, что известные и достойные доверия веб-сайты могут взламываться и заражаться вредоносными кодами, не учитывается. Почти каждую неделю средства массовой информации сообщают об известных брендах, веб-сайты которых были взломаны. И это только те случаи, о которых стало известно средствам массовой информации Никто не знает, сколько случаев остается нераскрытыми? Иными словами, пользователи не могут определить заражение при "попутной загрузке". В результате любого поведения в сети невозможно избежать контактирования ПК с данным вирусом.

Единственный эффективный способ защиты ПК от заражения при "попутной загрузке" — использование комплексного решения безопасности, включающее в себя HTTP-фильтр, который сканирует веб-сайты на предмет наличия вредоносных программ перед их загрузкой. Бесплатное антивирусное ПО не имеет данной технологии защиты, поэтому пользователи, которые используют такое ПО, защищены в недостаточной степени. Однако, как показало исследование, данные пользователи часто считают, что используемое ими ПО обеспечивает достаточную комплексную защиту от интернет-угроз. Заблуждение такого характера может привести к заражению опасным вредоносным кодом.

Не менее 62,58% пользователей считают, что бесплатное антивирусное ПО защищает ПК от вирусов "попутной загрузки". 25,39% пользователей полагают (ошибочно), что их компьютер защищен от вирусов "попутной загрузки" с помощью брандмауэра. Из-за своей ложной точки зрения эти пользователи не будут искать HTTP-фильтр, чтобы защититься от зараженных веб-сайтов.

Защита от зараженных веб-сайтов также очень важна для пользователей социальных сетей. На данных платформах постоянно публикуются ссылки на внешние интернет-сайты со смешным или информативным содержимым, или трейлерами к фильмам. Подобные функции делают такие сети, как Twitter и Facebook очень привлекательными для пользователей. Поэтому было неправильно, исходя из причин безопасности, оставлять такие ссылки вовсе без внимания — прием, которому поддаются, тем не менее, 46% участников опроса. Здесь следует упомянуть, что сокращенные URL-адреса сайтов представляют повышенный риск и не только на социальных платформах. Предназначение сокращенных ссылок нельзя определить непосредственно. С помощью такой онлайновой службы как http://longurl.org можно определить исходные интернет-адреса. Подобные службы совместно с хорошим HTTP-фильтром делают переход по ссылкам, которые публикуются в социальных сетях, более безопасными для пользователей.

Сделать выводы относительно того, кто лучше всего информирован обо всех опасностях, тяжело. Очевидно, средняя и большая возрастная группа опрошенных от 25 до 54 лет лучше всего осведомлена об интернет-угрозах, однако они также часто сомневаются в ситуациях, которые едва таят в себе угрозы. Таким образом, сомнительно было бы считать данных интернет-пользователей более грамотными.

Разница между мужчинами и женщинами очень незначительна, несмотря на то, что, согласно общему результату исследования безопасности G Data, женщины кажутся несколько лучше информированными. Сделать общий вывод относительно того, какой из полов обладает большими знаниями о потенциальных опасностях в Интернете, невозможно. При рассмотрении национальной принадлежности опрашиваемых также не удается выделить однозначного лидера. В Германии, Великобритании и Северной Ирландии пользователи, очевидно, больше информированы о том, какие интернет-угрозы реальны, а какие нет, однако расхождение со средним показателем здесь также минимальное. Определенно можно говорить об одном результате: в России уровень неосведомленности относительно интернет-угроз самый высокий. К счастью, процент российских интернет-пользователей, которые используют платное пакетное защитное ПО, самый высокий по сравнению с другими странами. Следует также отметить, что в России в основном используют пиратские копии платного пакетного защитного ПО, которое менее надежно и безопасно, чем легальные версии.

В качестве окончательного вывода исследования безопасности G Data можно сказать, что, несмотря на широкое использование Интернета, большинство пользователей мало знает об опасностях и, следовательно, почти ничего не знает о стратегиях предотвращения заражения компьютера вредоносным кодом.

Приложение

G Data Software AG

G Data Software AG - это инновационная и быстро развивающаяся компания, которая занимается разработкой программного обеспечения. Основным направлением работы компании является обеспечение IT-безопасности. Более 20 лет назад, в 1985 году, компания, являющаяся экспертом в области Интернет безопасности и пионером в защите от вирусов, разработала первую антивирусную программу. В 2010 году компания отметила свой 25-й день рождения!

G Data является одной из первых компаний в мире, которая начала заниматься программным обеспечением безопасности. В течение последних пяти лет ни один производитель программного обеспечения IT безопасности в мире, кроме G Data, не стал бесспорным лидером многочисленных национальных и международных тестирований, и не получил столько наград, сколько G Data!

Продуктовая линейка включает решения безопасности для конечных пользователей, и для корпоративных клиентов для защиты как средних, так и больших сетей. Решения безопасности G Data доступны в более чем в 60 странах мира.

Более подробную информацию о компании и о решениях безопасности Вы можете получить на сайте www.gdatasoftware.ru

Основные вехи развития компании G Data

1986
Выставка CeBIT выходит на самостоятельный путь, и компания G Data представляет первую концепцию антивирусной защиты для компьютеров ATARI.

1987
G Data разрабатывает многочисленные инновационные программы для компьютеров ATARI ST, в том числе и первую в мире антивирусную программу G Data AntiVirenKit.

1990
Использование персональных компьютеров стремительно возрастает. G Data начинает разработку программного обеспечения для MS-Dos. Первым проектом становится преобразование AntiVirenKit для ПК – что тогда было нечто совершенно новым – программа получает собственный пользовательский интерфейс.

1991
G Data постоянно развивается и предлагает широкий ассортимент различного программного обеспечения для ATARI ST.

1992
Наряду с антивирусными программами G Data разрабатывает многочисленные пользовательские программы для MS-DOS и Windows. Особой новизной отличался планировщик маршрута GeoRoute, первая программа по планировке маршрута с интерактивной картой.

1995
Открытие первого заграничного филиала в Польше.

1998
PowerRoute, количество проданных экземпляров составило больше 1 млн., становится самым успешным планировщиком маршрута для ПК в Германии.

2000
Преобразование компании в акционерное общество: работникам G Data предоставляется доля акций компании. По сегодняшний день большинство акций принадлежит сотрудникам и основателям компании.

2001
Выход на сетевой и деловой рынок такого программного обеспечения G Data, как AntiVirus Business и AntiVirus Enterprise.

2002
G Data разрабатывает технологию двойного сканирования (DoubleScan) и становится первым производителем, использующим в своих продуктах параллельно два антивирусных движка.

2003
Выход на международный уровень: появление на рынке в Японии.

2004
На выставке CeBIT G Data представляет первое поколение программного обеспечения своего комплексного пакета защиты G Data InternetSecurity.

2005
Опережая свою эпоху: G Data становится первой в мире компанией, интегрировавшей технологию "облачной" защиты в свое защитное ПО. Модуль OutbreakShield одновременно защищает от спама и неизвестных вредоносных программ, независимо от содержимого. Немецкая организация по сравнению потребительских товаров Stiftung Warentest признает G Data InternetSecurity лучшим пакетом безопасности.

Выход на международный уровень: открытие филиалов во Франции и Италии.

2006
Количество компьютерных вредоносных программ растет, на что реагирует G Data : компания быстро защищает своих клиентов от нового вредоносного ПО с помощью ежечасных обновлений сигнатур.

2007
Stiftung Warentest: второй раз подряд продукт G Data InternetSecurity 2010 получает первое место в масштабном сравнительном тестировании известного немецкого потребительского журнала.
CeBit-2007: премьера решения G Data TotalCare.

2008
Выход на рынок специального решения безопасности для владельцев ноутбуков: высокоэффективное решение "все в одном" G Data NotebookSecurity объединило в себе антивирусную защиту, технологию резервного копирования и шифрования.

2009
Решения безопасности G Data доступны в более чем в 60 странах. С выходом на рынок в

Южной Америке, России, Южной Африке и Китае G Data продолжает реализацию своей успешной политики расширения.

2010
Компания G Data отмечает свой 25-летний юбилей. Выставка CeBIT: премьера ПО G Data EndpointProtection.

2011
Премьера на выставке CeBIT ПО G Data CloudSecurity – бесплатного плагина для браузера, предназначенного для обеспечения интернет-защиты. Интеллектуальная защита для смартфонов на базе ОС Androoid и планшетных ПК: ПО G Data MobileSecurity.

Survey Sampling International

В 1977 г. SSI основала в США фирму, занимающуюся выборочными испытаниями. Уже более тридцати лет мы устанавливаем стандарт специальных знаний и качества услуг по выборочным испытаниям и обслуживанию клиентов в области маркетинга.

SSI предоставляет доступ к более 6 млн. участникам опроса в 54 странах. Нашими источниками являются собственные комиссии SSI в 27 странах, постоянно возрастающее количество дочерних предприятий, которые мы возглавляем, и обширная сеть партнерских компаний по всему миру. В SSI работает 400 сотрудников из 50 стран, которые говорят на 36 языках, к тому же компания сотрудничает с 1 800 клиентами и третей четвертью крупнейших в мире компаний по исследованию рынка.

Компания имеет более 17 офисов по всему миру: в Пекине, Франкфурте, Лондоне, Лос-Анджелесе, Мадриде, Мехико, Париже, Роттердаме, Сеуле, Шанхае, Шелтоне (штат Коннектикут), Сингапуре, Стокгольме, Сиднее, Тимишоаре (Румыния), Токио и Торонто. Кроме этого представительства SSI есть и в Гонконге.

Подробнее о компании Survey Sampling International см. на сайте www.surveysampling.com

Глоссарий

Бот. Боты — это хакерские программы, которые, как правило, незаметно работают в фоновом режиме на компьютере жертвы и, в зависимости от функций, выполняют различные вещи — от DDoS-атак, рассылки спама по электронной почте, до считывания вводов с клавиатуры и многое другое. Объем функций, в первую очередь, зависит от того, сколько денег готовы заплатить за данный бот. Боты, обладающие широким набором функций, естественно, дороже, чем просты боты, которые могут очень мало. Данные программы продаются в том числе и на подпольных форумах.

Бот-сети. Ботсеть является составляющей т.н. зомби-ПК. Для управления ботсетью используется сервер управления и контроля (C&C-сервер). Ботсети также используются для целенаправленных атак на веб-сервера (DoS- и DDoS-атаки) с целью их перегрузки и рассылки спама.

DoS (Denial of Service, "отказ в обслуживании"). Во время DoS-атак компьютеры (а чаще веб-сервера) "бомбардируют" целенаправленными запросами или их очень большим количеством. В результате они становятся неспособны продолжать выполнять свою работу и "сдаются" под таким натиском.

DDoS (Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»). DDoS-атака основана та том же принципе, что и обычная DoS-атака с единственной разницей в том, что здесь речь идет о распределённой атаке. Часто данный тип атаки осуществляется несколькими тысячами зомби-ПК.

Попутное заражение (попутная загрузка). При попутном заражении во время посещения подготовленного веб-сайта вредоносный код незаметно загружается и распаковывается на компьютере жертвы и. Для атаки данного типа злоумышленники используют пробелы безопасности в браузере и его плагинах. Особое внимание взломщики обращают на слабые места функций выполнения активного содержимого (напр., JavaScript, Flash или Java).

Эксплойт. Эксплойт является программой, которая использует существующие пробелы безопасности на целевом компьютере для того, чтобы выполнить программный код.

Фишинг. Под фишингом подразумеваются попытки заполучить такие персональные данные, как логины, пароли, номера кредитных карточек, банковские данные доступа и др. с помощью сфальсифицированных веб-страниц или электронных сообщений. В большинстве случаев фишинг направлен на клиентов банков, предлагающих услуги онлайн-банкинга (CityBank, Postbank), платежных служб (Paypal), провайдеров интернет-услуг (AOL) или онлайн-магазины (eBay, Amazon). Для этого, как правило, через электронную почту или программу мгновенного обмена сообщениями выполняется перенаправление на поддельные веб-сайты, которые очень точно создаются по образцу настоящих сайтов.

Социотехника. Под социотехникой подразумевают убежденческие тактики, с помощью которых взломщик побуждает пользователя выдать информацию, которую можно использовать для нанесения вреда самому пользователю или организации, в которой он работает. Часто, чтобы заполучить данные доступа или пароли, используется мнимый авторитет.

Спам. Середина 90-х гг. характеризует спам как многочисленное распространение одинаковых сообщений на форумах Usenet. Само понятие происходит из скетча группы "Монти Пайтон". Между тем слово "спам" используется в нескольких значениях. В широком понятии "спам" применяется ко всем нежелательным электронным сообщениям. В более узком смысле понятие "спам" ограничивается электронными рассылками рекламного характера; это означает, что черви, программы-мистификаторы и автоответчики сюда не относятся.

Зомби-ПК. Зомби называют ПК, удаленное управление которыми осуществляется с помощью программы Backdoor. Аналогично своему прототипу из фильмов, зомби-ПК подчиняется только скрытому хозяину и исполняет его часто преступные команды. Многие зомби объединяются в т.н. ботсети.