Об угрозах в Сети мало что известно

Информация о кибератаках приходит на ленты информационных агентств ежедневно и каждый раз - с устрашающими подробностями. :) Доходя до пользователя, правда, такая информация превращается в классическую страшилку из серии "эти злобные хакеры появились ниоткуда и все сломали". На самом деле, бОльшая часть проблем в этой сфере - от недальновидности и ошибок самих пользователей, которые и становятся жертвами преступников. Навряд ли профессиональной аудитории необходимо говорить о том, что в эпоху всепроникающей Сети защита цифровых данных на предприятиях приобретает исключительно важное значение. Правда, ведь, все в курсе? Осталось только понять, что же знают об интернет-угрозах самые обычные пользователи, чтобы купировать возможные проблемы еще до их появления. :)

Не скрою, что к исследованиям я отношусь осторожно - особенно когда не совсем понимаю методологию или не уверен в правильности интерпретации данных. :) Но с данными GData, полагаю, все хорошо - 15 тыс. респондентов из 11 стран мира вполне достаточно для построения если не объективной картины мира, то, как минимум, для организации качественного социологического среза. Давайте попробуем вытащить из массивного отчета действительно самые интересные факты, которые помогут сотрудникам самых разных провайдеров связи лучше понять свою аудиторию - тех пользователей, которые находятся от них "по ту сторону экрана".

Общие положения

Самое главное, что удалось сделать экспертам G Data - сравнить результаты ответов, полученные от респондентов, с текущим уровнем угроз и выявить наиболее слабые места с точки зрения обычных пользователей Сети. Это, к примеру, показывает, что те средства, которыми располагают интернет-пользователи, во многом недостаточны и устаревшие. Ни один провайдер связи в России не занимается долгосрочным просвещением детей, а только взрослых пользователей в области банальной информационной безопасности. Поэтому массовое знание очень редко является реальным отображением угроз. Отсюда и утечки, и проблемы и сложности с защитой своих данных. К примеру, девять из десяти пользователей ПК считают, что пользователь замечает заражение вредоносной программой! То есть если ничего не тормозит и диск не взрывается - то компьютер не заражен. :) И это ведь консолидированное мнение пользователей НЕ только из России. :) 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. Не новость для профи, конечно, но для обычных "юзверей" это вполне может быть реальным откровением. :)

Правда, есть и хорошие новости. 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. Большая ошибка. :) Более 50% этих пользователей даже хотели бы установить полный программный пакет с этими необходимыми технологиями защиты. По сути, самые обычные пользователи, которых у любого оператора связи стабильное большинство, совершенно неверно оценивают действительные угрозы в Интернете, причем огромное число "юзверей" неэффективно защищают свои компьютеры. Думаю, на таком незнании операторы вполне могут заработать - надо только предлагать не дешевый антивирус с помесячной оплатой, а недорогие пакеты комплексной безопасности.

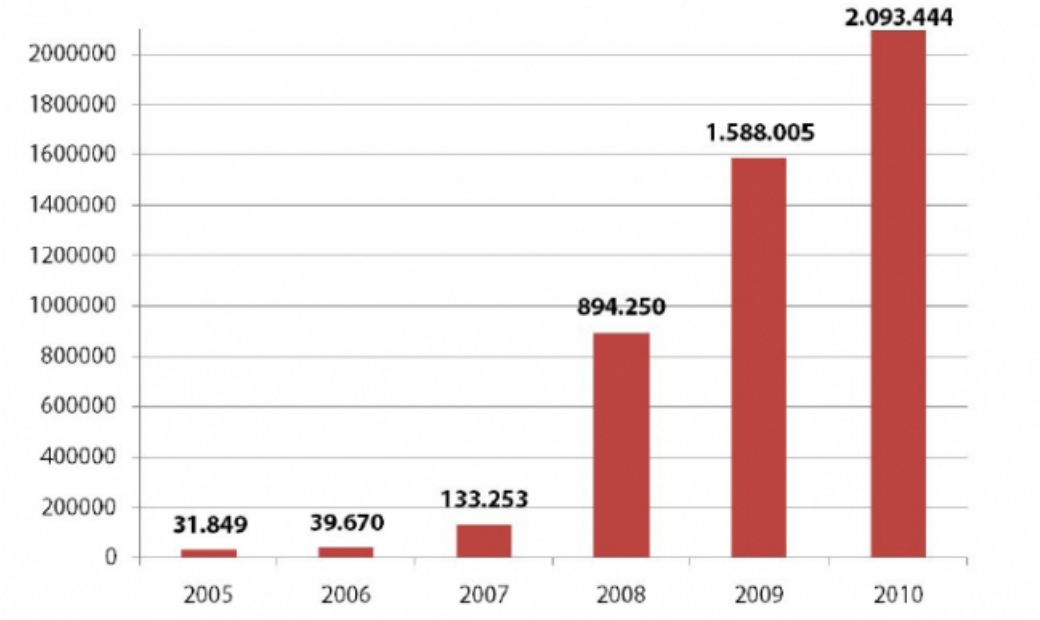
Но, давайте все-таки перейдем к более системному анализу полученных результатов. Все-таки исследование безопасности компании G Data под названием "Как пользователи оценивают угрозы в Интернете?" основано на международном онлайн-опросе 15,5 тыс. интернет-пользователей в возрасте от 18 до 65 лет в одиннадцати 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. Сбор данных проходил с февраля по март 2011 г. по заказу G Data Software AG и при содействии компании Survey Sampling International1. Оценка и анализ данных были проведены в апреле-мае 2011 г.

Антивирусная безопасность

Атаки, направленные на компании и частных пользователей, вполне выгодный бизнес. Основная задача уже не уничтожить компьютеры, а похитить оперативно-коммерческую или личную информацию с целью дальнейшей перепродажи. Сделать это проще всего с помощью компьютерных вирусов - только в прошлом году G Data зарегистрировала более двух миллионов новых вредоносных

программ для ОС Windows. Правда, рассылать вирусы по электронной почте давно закончили - это неэффективно. Размещение вредоносного кода на интернет-страницах имеет смысл, но в 2011 году основным трендом являются вирусы для "попутной загрузки" троянцев, шпионских программ и другого вредоносного софта.

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



Результат исследования безопасности G Data показывает, что более 89% опрошенных пользователей используют на своих компьютерах защитное программное обеспечение, из них 48% доверяют бесплатным программам. 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. Уже хоть что-то. :) Разумеется, пользователи вполне могут сочетать бесплатное антивирусное ПО и другие бесплатные инструменты. Проблемой может стать возможная несовместимость определенных программ с используемым защитным ПО. Основная задача на ближайшее будущее - объяснить обычным пользователям, что важнейшей составляющей эффективной защиты компьютера, наряду с антивирусной защитой, является, как минимум, персональный брандмауэр.

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



Кстати, в своем исследовании G Data качественно "топит" бесплатное антивирусное ПО. :) "Современные решения безопасности должны защищать от многих угроз, - пишут составители исследования. - А вот 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". И это при том, что 44% участников опроса считают, что эффективность и качество бесплатного защитного ПО находятся на уровне платных решений. 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. Интересно, где же истина на самом деле? Бесплатное антивирусное ПО действительно может быть нормальной преградой "зловредам"?

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 целом, антивирусным компаниям удалось решить вопрос о том, что подобное защитное ПО должно быть чуть ли не на любом компьютере: пользователей они качественно напугали. :) Согласно результатам исследования, всего около 6% всех опрошенных не защищены во время Интернет-серфинга - среди всех участников количество полностью незащищенных компьютеров было сравнительно небольшим и составило едва 4%. 1,84% опрошенных заявили, что используют пиратские версии антивирусного ПО без регулярного обновления баз. А вот еще 5% пользователей не смогли ответить... установлено ли на их компьютерах какое-либо защитное ПО. Кстати, 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.

Опасности в Сети

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.

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%**

Тезис 1. Если моя операционная система заражена вредоносной программой, то это, так или иначе, будет заметно на моем ПК. С этим согласны 93% пользователей! 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. По-моему очаровательная статистика. :) И это при том, что разработчики вирусов тщательно следят за тем, чтобы владелец зараженного компьютера как можно дольше не замечал, что с его машиной что-то не так. :) Кстати, девять из десяти пользователей 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 (согласны - 83%). Хотя 56% опрошенных при вопросе о различиях качества бесплатного и платного защитного ПО 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, - пишут исследователи из G Data. - 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.

Тезис 3. Большинство вредоносных программ распространяется по электронной почте (54%). Данный тезис также устарел, как и первый, но, несмотря на это, этой точки 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 снимками обнаженной 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, - отмечено в отчете G Data. - 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, 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%). И сюда же тезис 5. Большинство вирусов и вредоносных компьютерных программ распространяются посредством зараженных файлов на файлообменниках, таких как одноранговые сети и торренты (48%). На самом-то деле самое качественное заражение компьютера вредоносными кодами осуществляется с помощью вирусов "попутной загрузки". В этой связи мне нравится "утонченный" вариант заражения - когда 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 зараженный веб-сайт. Надо только найти "сайт-цель" и грамотно использовать его уязвимости, которые есть практически у всех. 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.

Тезис 6. Риск встретить вредоносное ПО на порносайтах выше, чем, например, при посещении сайтов о конном спорте или о путешествиях (37%). В отношении этого тезиса исследователи из G Data написали следующее - цитирую с улыбкой и без купюр: "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... В целом порносайты могут 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". 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. 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 лишь 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%). Ради справедливости отметим, что 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", - пишут исследователи из G Data.

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.

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

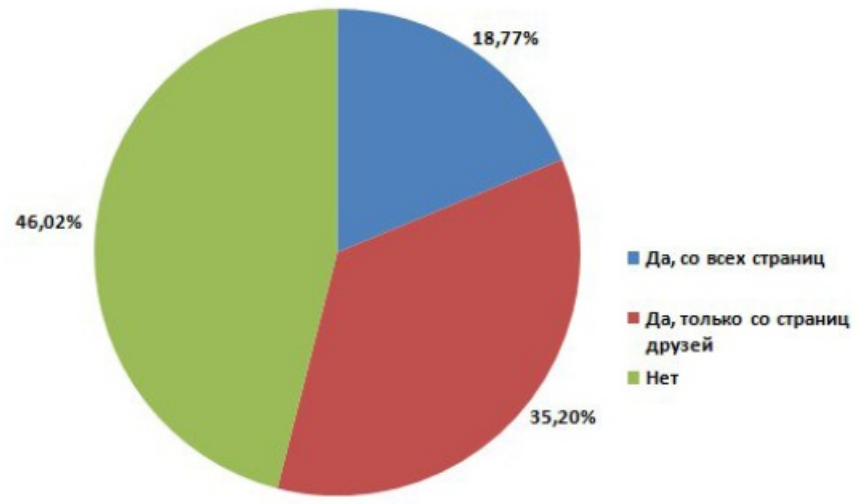
Мифы	18-25 лет	55-64 лет	Всего
1) Если мой компьютер инфицирован вирусами, я сразу об этом узнаю	91,68%	92,87%	92,59%
2) Бесплатные антивирусные решения предлагают такой же набор элементов, что и платные	82,17%	83,17%	82,92%
3) Большинство вирусов и других видов вредоносного программного обеспечения 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%

В целом, по данным исследования G Data, 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.

Опасности в соцсетях

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. Хотя, кто бы сомневался с этом тезисе. :)

График 9. Переход по ссылкам в социальных сетях



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 группы 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, который ворует данные путем фишинга или с помощью клик-джекинга превращает жертву в распространителя спама.

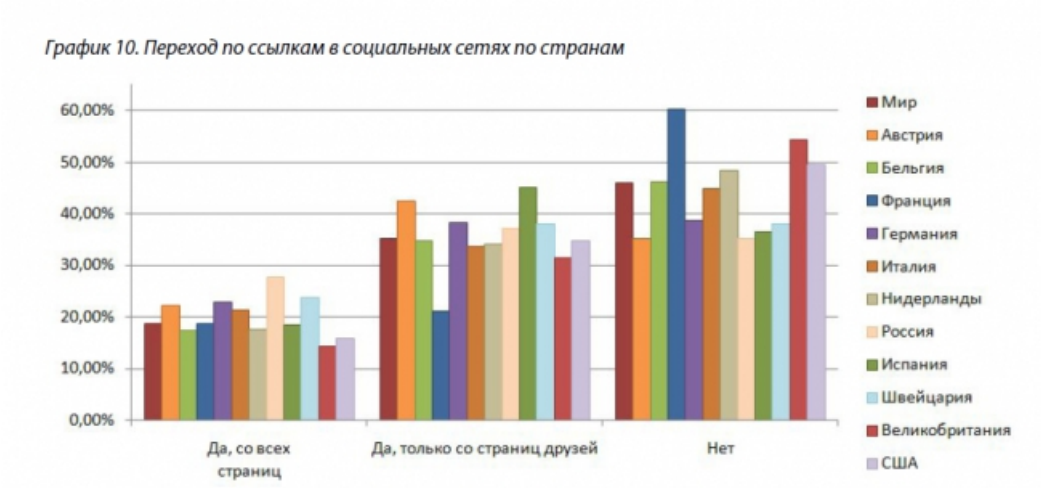


График 10. Переход по ссылкам в социальных сетях по странам

Из-за высокого уровня опасности исследование безопасности G Data 2011 содержало вопрос о том, переходят ли пользователи 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 трети 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. Этот показатель Франции является наивысшим по сравнению с остальными странами. 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 без дополнительного вопроса "а что это такое?".

В целом, несмотря на широкое использование Интернета, большинство пользователей мало знают об опасностях и, следовательно, почти ничего не знают о стратегиях предотвращения заражения компьютера вредоносным кодом.