БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ: ГОТОВЫ ЛИ ПОЛЬЗОВАТЕЛИ ПРОТИВОСТОЯТЬ КИБЕРУГРОЗАМ

@mail.ru group

Содержание

Введение

Интернет-отрасль стремительно развивается: осенью 2014 года месячная аудитория рунета достигла 72,3 млн пользователей, что составляет 62%[1] населения РФ, и эта цифра продолжает расти. Увеличивается и объем пользовательских данных в сети, ведь сегодня онлайн можно сделать практически все: от оплаты коммунальных услуг до покупки авиабилетов. Одновременно с этим растет количество киберугроз. Прошлый год ознаменовался целым рядом громких инцидентов: Heartbleed, Shellshock, слив фото обнаженных знаменитостей из iCloud — вот лишь несколько из них. При этом россияне находятся в большей опасности, чем зарубежные пользователи: по данным «Лаборатории Касперского», во втором квартале 2014 года Россия заняла первое место среди стран, в которых пользователи подвергались наибольшему риску заражения через интернет[2].

Но растет ли уровень знаний о том, как противостоять киберугрозам, особенно учитывая, что сегодня в результате взлома аккаунта можно потерять гораздо больше, чем на заре рунета? Многие эксперты считают, что огромное количество пользователей до сих пор пренебрегают элементарными правилами интернет-гигиены и своей беспечностью фактически сводят на нет усилия, прилагаемые онлайн-сервисами для повышения безопасности.

Мы проанализировали действия, которые российские пользователи предпринимают для того, чтобы обезопасить себя в интернете, а также выяснили, насколько часто они сталкиваются с мошенничеством. В онлайн-опросе, проведенном с привлечением исследовательской компании Nielsen, приняли участие 1783 человека в возрасте от 15 до 64 лет, которые проживают в городах с населением свыше 100 тысяч человек и заходят в интернет хотя бы один раз в неделю.

Это исследование будет интересно широкому кругу читателей — от обычных пользователей интернета до специалистов по безопасности и руководителей компаний.

1 Месячная аудитория по данным еженедельного опроса «ФОМнибус», на сентябрь-ноябрь 2014г. Вся Россия, 18 лет и старше. 30 000 респондентов.

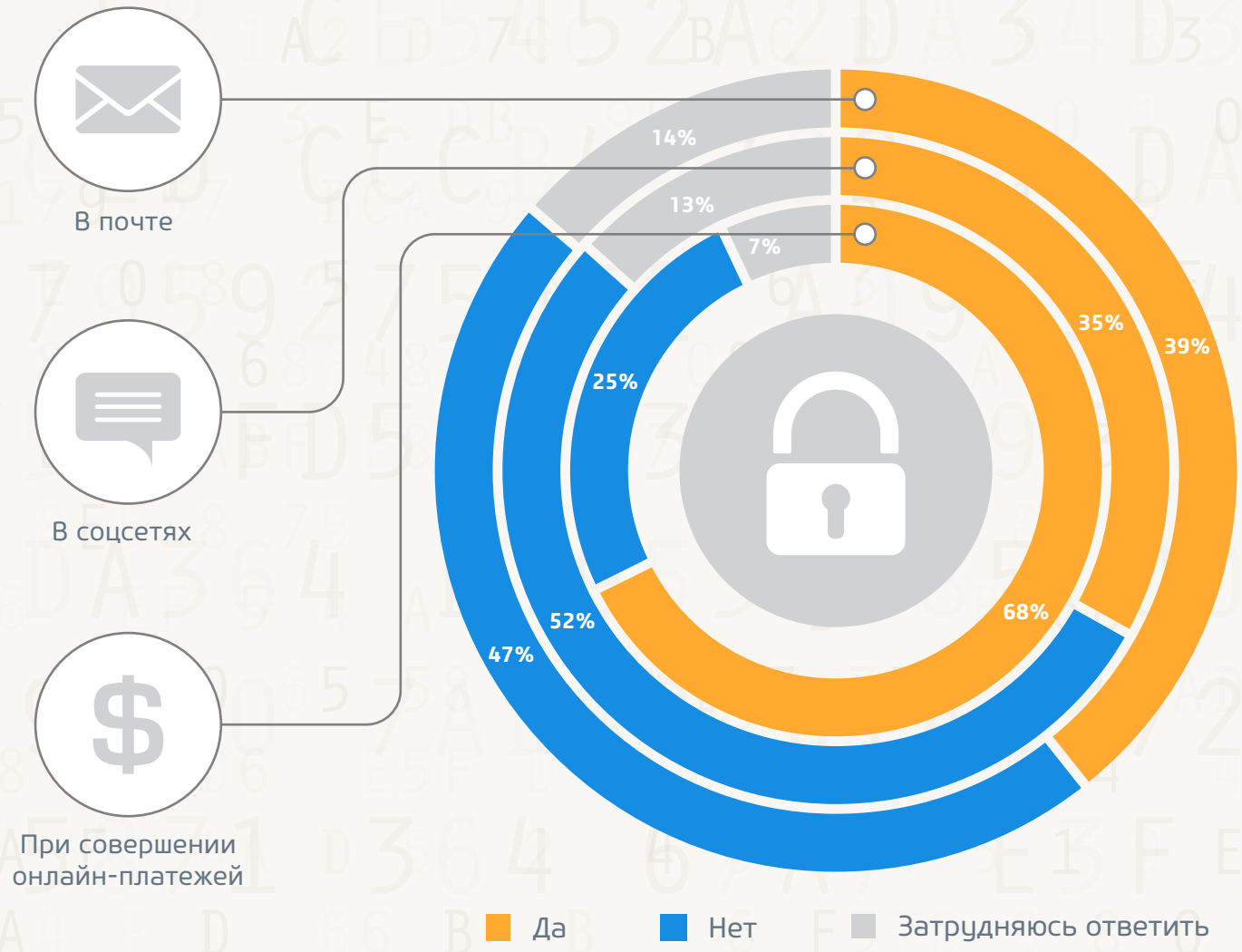
2 http://securelist.ru/analysis/malware-quarterly/21505/razvitie-informacionnyx-ugroz-vo-vtorom-kvartale-2014-goda/

Проверка безопасности соединения

Работа с различными интернет-сервисами — почтой, социальными сетями, интернет-магазинами и т.д. — начинается с регистрации и/или ввода логина и пароля. Один из способов защитить эту информацию от попадания в руки мошенников при передаче от клиента к серверу — использование зашифрованного соединения по протоколу HTTPS. Проверить, включено ли у интернет-ресурса защищенное соединение, можно в адресной строке браузера; как правило, оно обозначается иконкой в виде замка (в зависимости от типа браузера). Такая проверка позволяет дополнительно убедиться в том, что сайт не является фишинговым.

Исследование показало, что при вводе личных данных в почте и соцсетях пользователи не проверяют наличие значка безопасного соединения почти в половине случаев. При этом при совершении онлайн-платежей к проверке безопасного соединения обращаются почти в два раза чаще, чем в почте и соцсетях.

Проверяете ли вы значок безопасного соединения в адресной строке браузера при вводе личных данных?



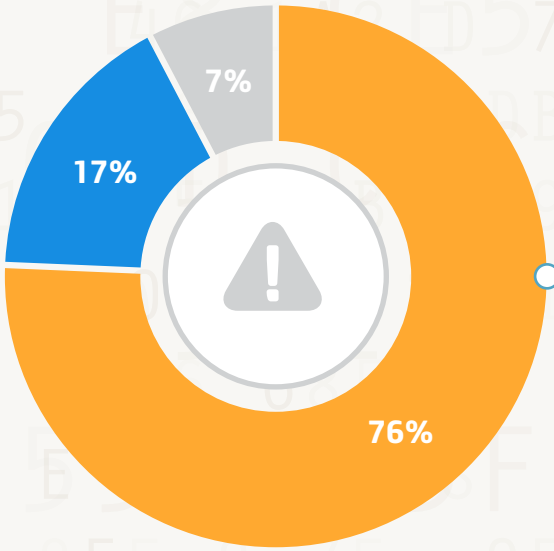
Источник: исследование Mail.Ru Group, 2014 г.

Проверка безопасного соединения

Иногда при посещении различных сайтов пользователи сталкиваются с объявлением об «Ошибке сертификата безопасности веб-узла». Наличие таких ошибок может означать, что пользователя пытаются обмануть или хотят перехватить информацию, передаваемую на сервер. При появлении объявления рекомендуется прекратить работу с подозрительным ресурсом.

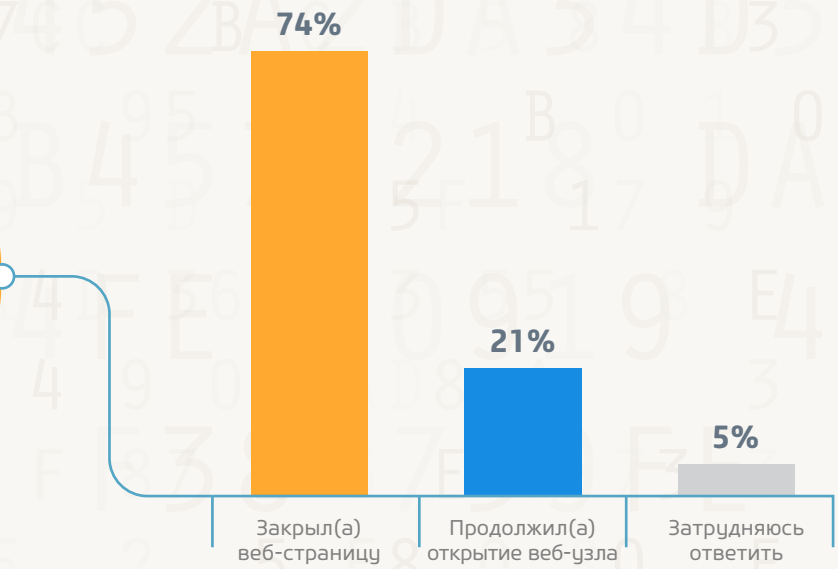
С сообщениями об ошибке в сертификате безопасности сталкивались большинство пользователей (три четверти). При этом 21% из них продолжили работу с сайтом. Интересно, что пользователи в возрасте до 34 лет почти в 2 раза реже обращают внимание на ошибку безопасности сертификата безопасности и продолжают открытие сайта, чем те, кому 34 года и более.

Сталкивались ли вы с ошибкой в сертификате безопасности веб-узла?



Да Нет Затрудняюсь ответить

Что вы делали при появлении ошибки сертификата безопасности веб-узла?



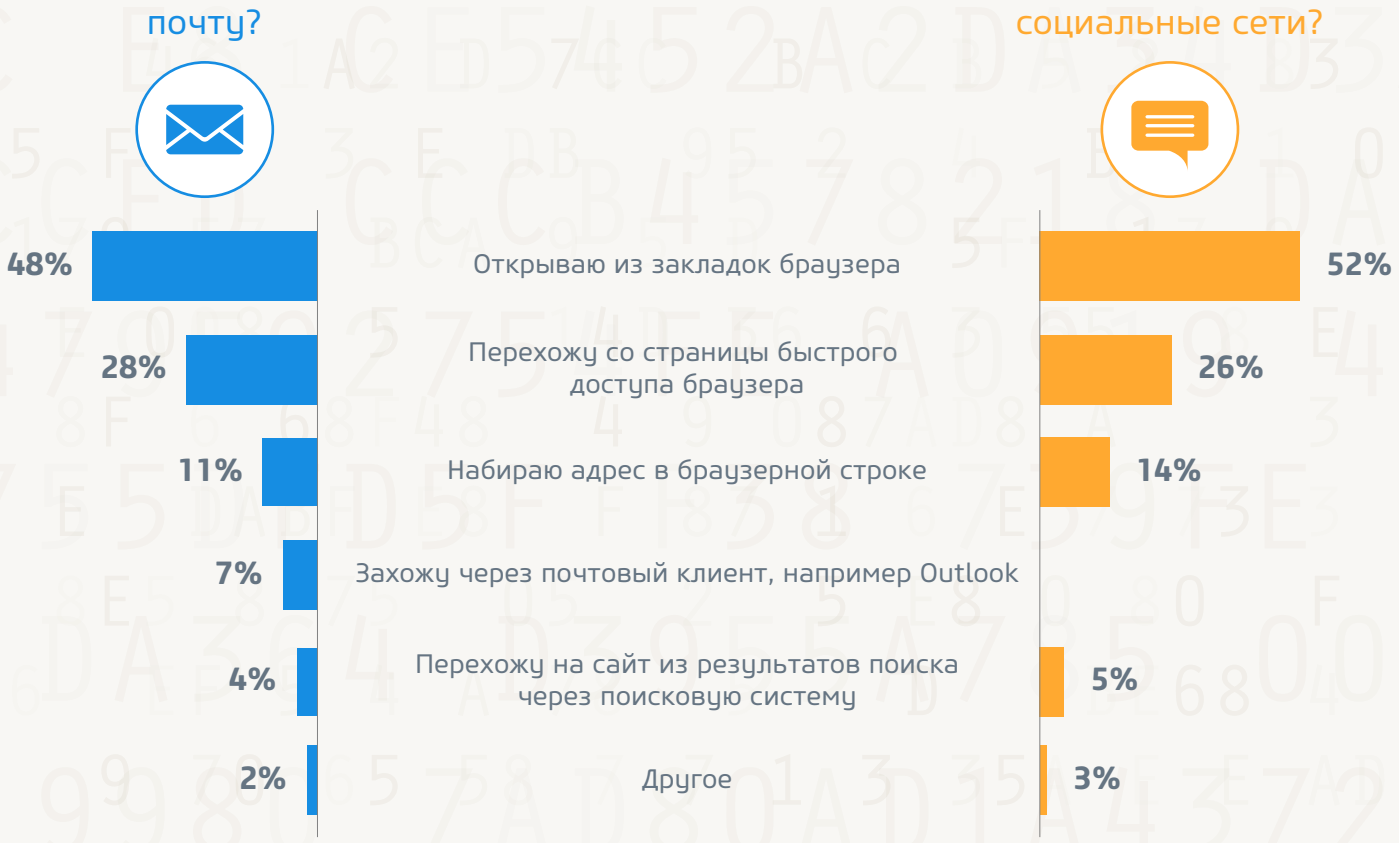
Источник: исследование Mail.Ru Group, 2014 г.

Проверка безопасного соединения

Для доступа как в электронную почту, так и в соцсети пользователи обычно используют закладки в браузере или ссылки на странице быстрого доступа. Такой способ является более безопасным, так как в этом случае пользователь защищен от опечаток, которые могут привести к попаданию на мошеннический сайт.

Тем не менее, каждый десятый пользователь набирает адрес в браузерной строке. При наборе адреса вручную или переходе по результатам поиска вероятность попасть на фишинговый сайт увеличивается.

Как вы обычно попадаете в ...



Источник: исследование Mail.Ru Group, 2014 г.

В целом можно сказать, что пользователи онлайн-сервисов не придают достаточного значения наличию или отсутствию значка безопасного соединения. В то же время внимательность к этой детали — один из самых эффективных способов защитить пользовательские данные от перехвата злоумышленниками.

Используемые пароли

Создание надежного пароля — это один из самых доступных способов повысить собственную безопасность и защитить конфиденциальную информацию, которая может храниться в почте, соцсетях и других онлайн-сервисах (Apple ID, Google ID, отчеты о банковских операциях, логины от онлайн-игр, пароли от других онлайн-сервисов и т.п.).

Очень важно заводить уникальные пароли для наиболее важных сервисов, ведь распространенный метод увода пароля — взлом сторонних ресурсов. Крупные сервисы постоянно работают над усилением уровня своей безопасности, тогда как многие мелкие форумы, торрент-трекеры, онлайн-магазины пренебрегают такими вещами — и хакеры, зная об этом, атакуют именно их. Если при регистрации на слабо защищенном ресурсе человек указал тот же пароль, который он использует для почты, то, взломав его, хакер автоматически получает и доступ к ящику. Результаты исследования говорят о том, что одинаковые пароли для всех учетных записей используют 12% опрошенных. 36% респондентов используют разные пароли для наиболее важных, одинаковые — для наименее.

Какие пароли вы используете для своих учетных записей?

Источник: исследование Mail.Ru Group, 2014 г.

Используемые пароли

По результатам исследования Mail.Ru Group, в среднем пользователь интернета имеет три ящика электронной почты. В отчете мы отдельно рассмотрим использование основного (под которым подразумевается единственный либо наиболее часто используемый в личных целях) и дополнительного почтовых аккаунтов.

Поскольку придумать разные пароли для всех аккаунтов достаточно сложно, многие эксперты рекомендуют использовать уникальные пароли для наиболее важных, включая почту и социальные сети, и одинаковые — для остальных. Однако результаты исследования показывают, что почти четверть (24%) пользователей электронной почты используют пароль от основного ящика на каких-либо других ресурсах, из них около двух третей пользователей почты используют тот же пароль и в социальных сетях (62%), 27% — в онлайн-магазинах, 25% — в дополнительном почтовом ящике.

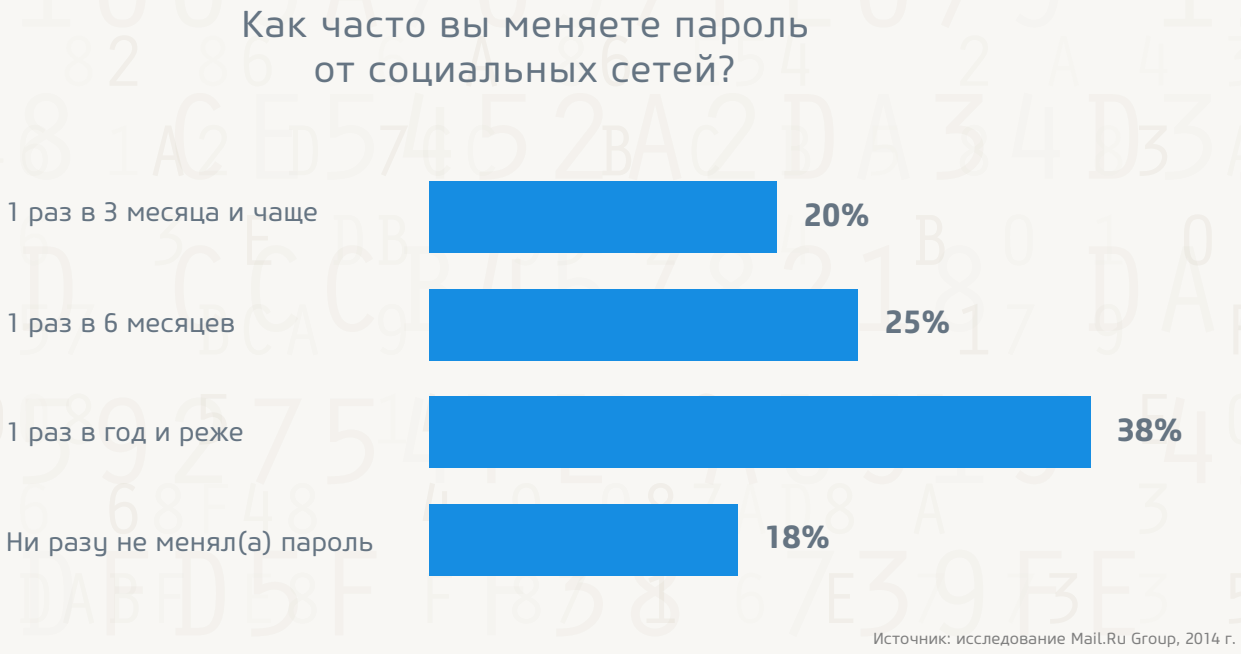
Одно из важных правил интернет-безопасности — частая смена паролей. В идеале это должно происходить раз в три месяца. Однако так поступает лишь пятая часть респондентов. Примечательно, что каждый пятый участник исследования никогда не менял пароль от своего основного ящика, а каждый третий — от дополнительного.

Как часто вы меняете пароль от почты?

Источник: исследование Mail.Ru Group, 2014 г.

Используемые пароли

К смене пароля в социальных сетях пользователи прибегают редко — 38% меняют пароль не чаще раза в год, а 18% вообще никогда не меняли пароль.



Источник: исследование Mail.Ru Group, 2014 г.

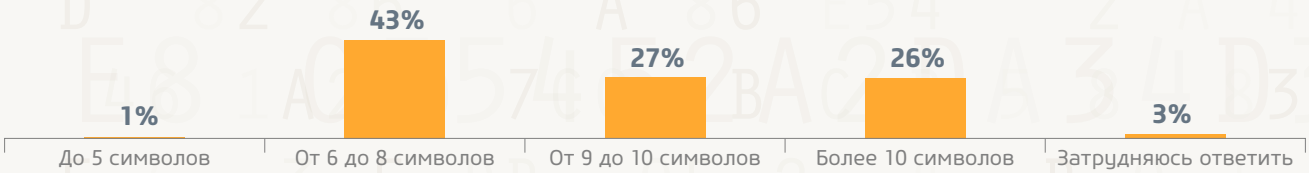
Используемые пароли

Согласно современным стандартам безопасности, надежный пароль должен состоять не менее чем из восьми символов и представлять собой сочетание букв в разном регистре, цифр и специальных символов, подобранных по случайному или понятному одному лишь пользователю принципу. Пароль, состоящий из символов, букв и цифр использует лишь четверть респондентов.

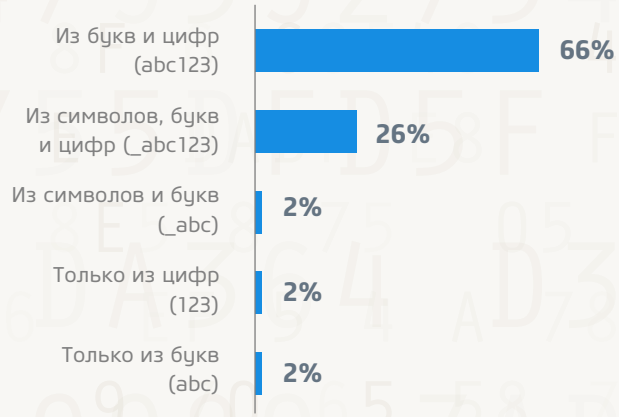
У большинства пользователей пароль состоит только из букв и цифр. 37% респондентов использует в пароле только строчные буквы. Причем среди обладателей относительно коротких (менее 8 символов) паролей такая беспечность встречается в 1,4 раза чаще, чем среди тех, чей пароль состоит из 8 символов и более (44% и 32% соответственно).

43% респондентов используют пароли длиной от 6 до 8 символов. Чуть более четверти (27%) — от 9 до 10 символов. Лишь у 26% пользователей пароли имеют длину более 10 символов.

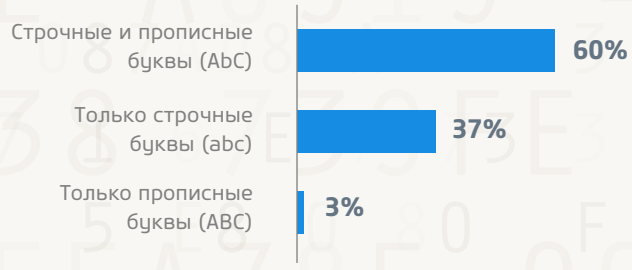
Какая длина у вашего пароля?



Из каких символов состоит ваш пароль?



Какие буквы вы используете в пароле?



Источник: исследование Mail.Ru Group, 2014 г.

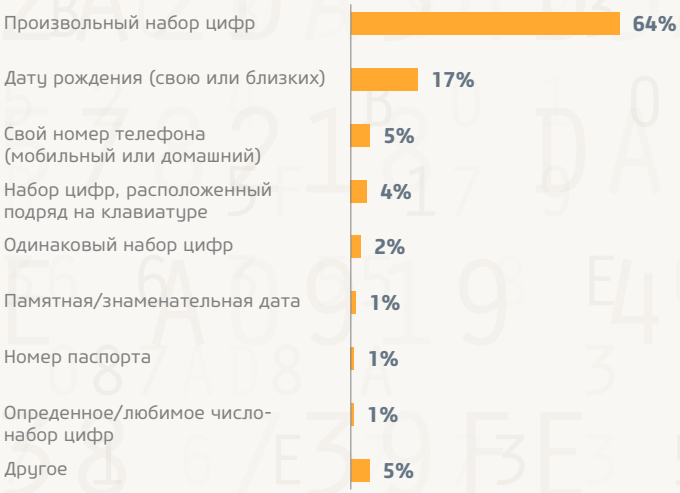
Используемые пароли

Почти треть пользователей используют в качестве пароля произвольный набор букв (29%), а еще 27% — выдуманное ими самими слово. 17% предпочитают использовать в пароле русское слово, набранное латинскими буквами (например, «пароль» превращается в «gfhjkm», «солнышко» — в «cjkysirj»), что является небезопасной опцией, поскольку злоумышленники тоже умеют переключать раскладку клавиатуры.

Среди тех, в чьих паролях встречаются цифры, 17% используют дату рождения (свою или близких), 5% — номер телефона.

Какие сочетания букв вы используете в пароле?

Какие сочетания цифр вы используете в пароле?

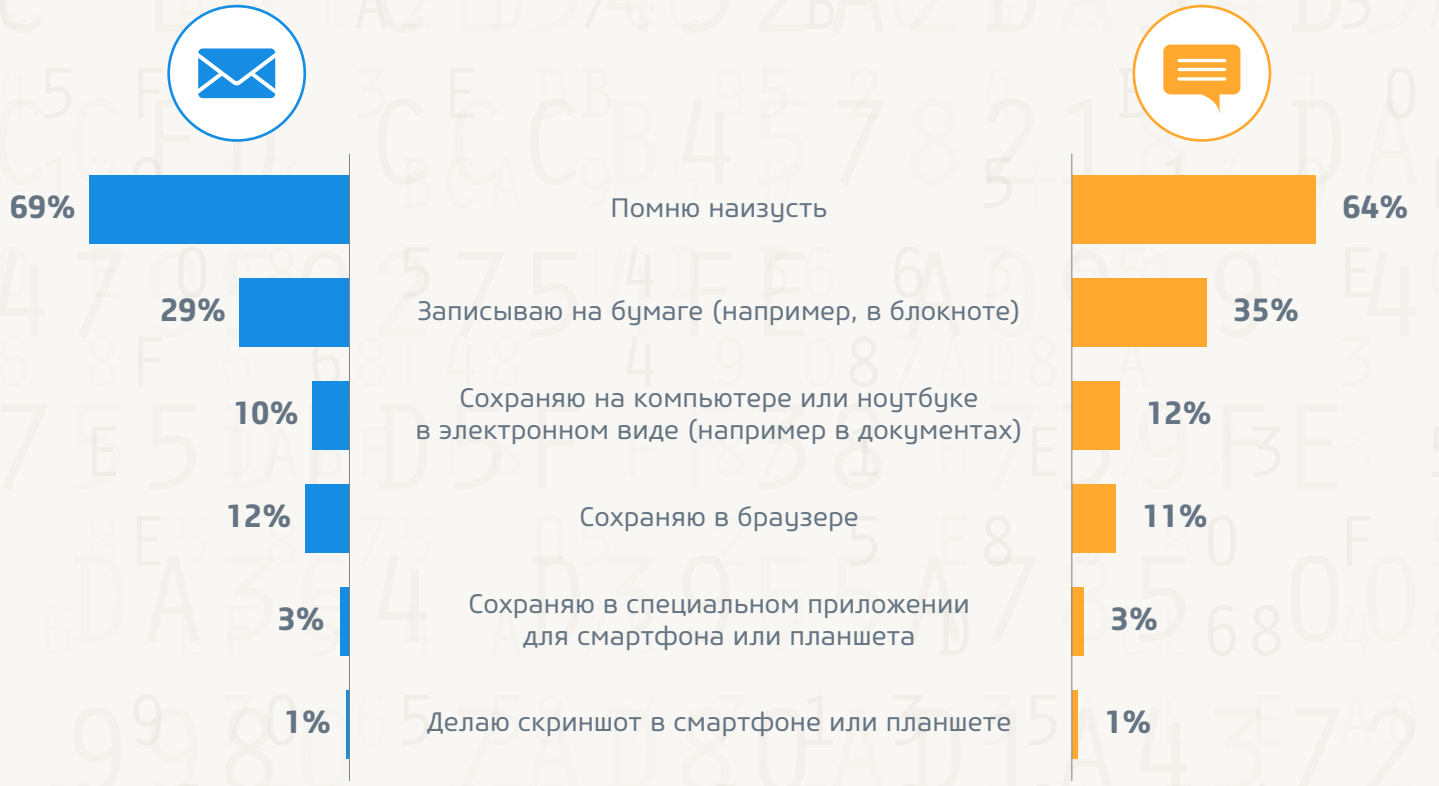


Источник: исследование Mail.Ru Group, 2014 г.

Используемые пароли

Большинство пользователей помнят пароли от почты и соцсетей наизусть, практически треть записывают их на бумаге. Специальными приложениями для хранения паролей пользуются лишь 3% пользователей.

Где вы храните пароли?



Источник: исследование Mail.Ru Group, 2014 г.

Качество и частота смены пароля зависят в основном от пользователя, однако сегодня у интернет-сервисов есть возможность влиять на уровень его сложности. Многие ресурсы не допускают создания короткого пароля без цифр. Так, например, в Почте Mail.Ru невозможно завести пароль короче шести символов, совпадающий с логином, только из цифр или из цифр и точек и при этом короче 10 символов, являющийся словарным словом. Кроме того, в процессе создания пароля показывается оценка уровня его сложности, а также всплывают рекомендательные подсказки, призывающие использовать заглавные и строчные буквы, цифры и специальные символы.

Меры безопасности при пользовании онлайн-сервисами

В данном разделе мы предлагаем рассмотреть меры безопасности, которые принимают пользователи различных интернет-сервисов: какие методы восстановления пароля они используют, как относятся к приходящим в почту ссылкам, а также как оценивают защищенность своих аккаунтов. Отдельно будут рассмотрены меры безопасности, к которым пользователи чаще всего прибегают при совершении онлайн-платежей.

На сегодняшний день самым безопасным способом восстановления пароля считается привязка к номеру мобильного телефона. Этот метод для восстановления пароля от основного ящика использует большинство респондентов (68%).

Тех, кто привязывает к номеру телефона дополнительный ящик, меньше — 41%. Чаще всего для восстановления пароля от дополнительного ящика используют секретный вопрос, который является гораздо менее безопасным по сравнению с привязкой к номеру телефона, поскольку по сути представляет собой еще один пароль.

Как вы восстанавливаете пароль от электронной почты?

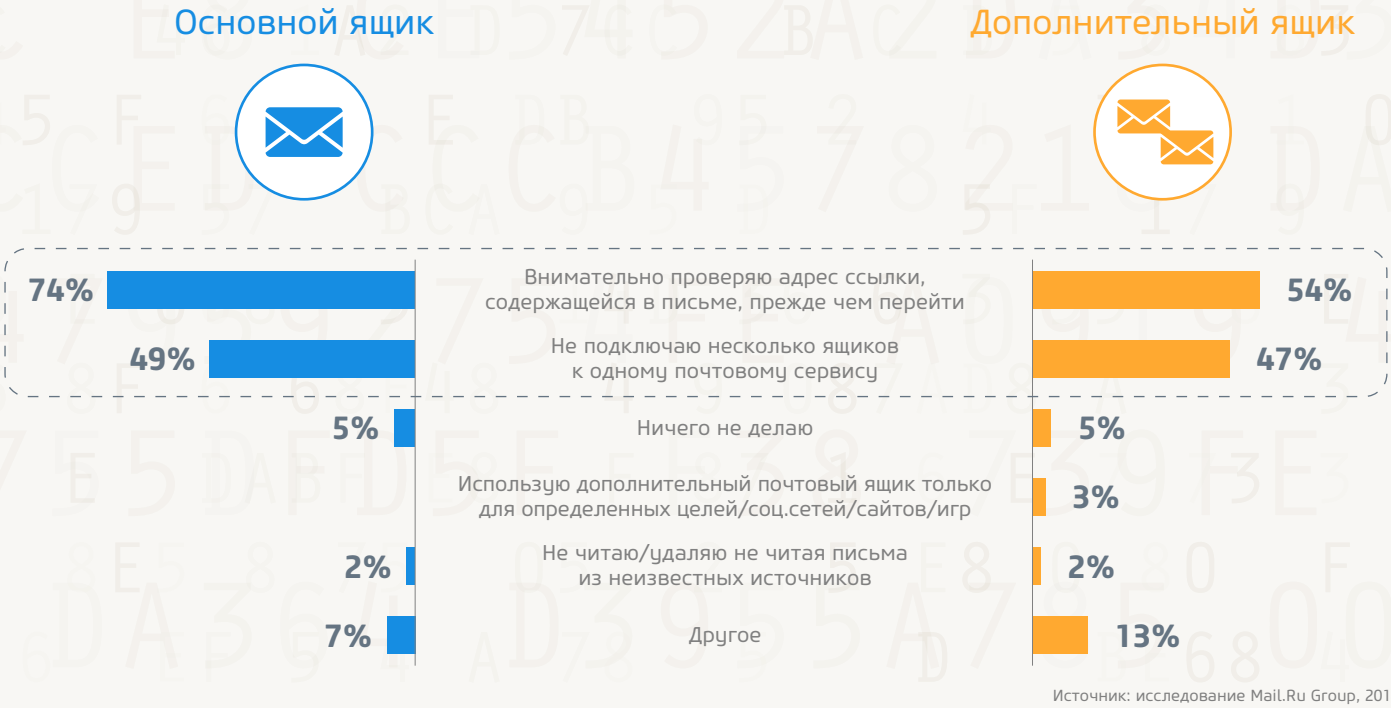
Источник: исследование Mail.Ru Group, 2014 г.

Один из распространенных методов взлома аккаунтов — фишинг. Типичный пример — пользователю отправляют ссылку на сайт, замаскированный под страницу авторизации на каком-либо популярном ресурсе. Человек вводит логин и пароль, которые тут же отправляются в руки злоумышленнику. Поэтому при переходе по ссылкам, которые приходят от незнакомых отправителей, нужно быть очень внимательным: в идеале — не открывать их совсем или, по меньшей мере, проверить адрес сайта.

Результаты исследования говорят о том, что пользователи с осторожностью относятся к ссылкам, пришедшим на основной электронный ящик: почти три четверти опрошенных (74%) в таких случаях всегда внимательно проверяют адрес, прежде чем перейти по ссылке.

Люди менее бережно относятся к безопасности дополнительного аккаунта по сравнению с основным: реже меняют пароль, реже используют привязку номера телефона, предпочитая секретный вопрос для восстановления.

Какие меры предосторожности вы соблюдаете при использовании электронной почты?



Источник: исследование Mail.Ru Group, 2014 г.

Меры безопасности при пользовании онлайн-сервисами

Рассмотрим, к каким мерам безопасности пользователи чаще всего прибегают при онлайн-платежах. В первую очередь они изучают информацию об онлайн-магазине в сети (60%). 27% стараются не совершать покупки в магазинах с бесплатным хостингом. Проверяют сертификат подлинности, выданный сайту, 17%. Еще один шаг к повышению безопасности — использование виртуальной клавиатуры (это позволяет защититься от перехвата конфиденциальных данных зловредными программами, которые отслеживают нажатие клавиш на физической клавиатуре). К этой мере прибегают 17% пользователей.

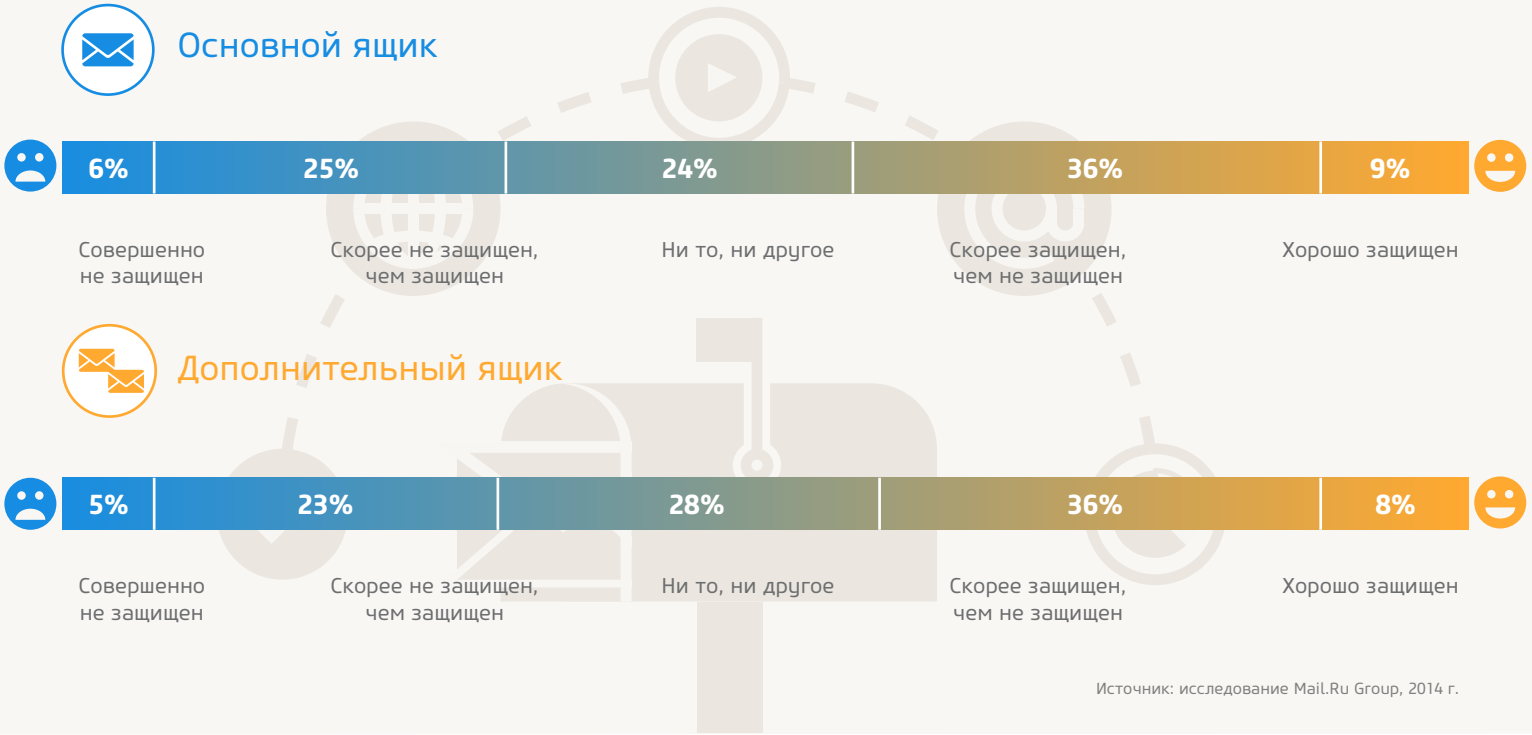
Меры безопасности при пользовании онлайн-сервисами

Помимо знания пользователей о возможных мерах безопасности, нам было интересно проанализировать их мнение о том, насколько в принципе защищены их аккаунты в почте и социальных сетях.

Почти половина пользователей считает, что их аккаунты в безопасности. Около трети обеспокоены незащищенностью своих почтовых аккаунтов, считая, что их ящики «совершенно не защищены» или «скорее не защищены».

В среднем защищенность основного и дополнительного ящика оценивают одинаково.

Насколько ваш почтовый аккаунт защищен от мошенников?



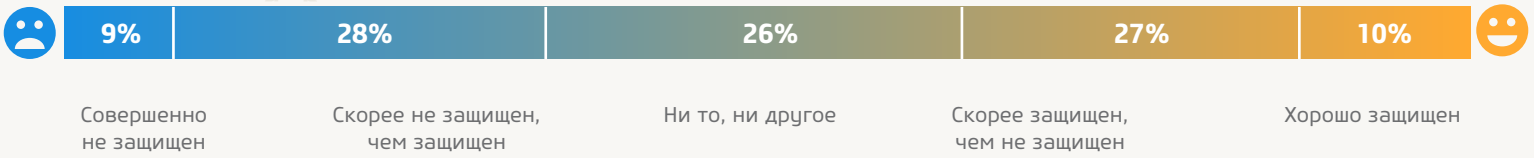
Источник: исследование Mail.Ru Group, 2014 г.

Меры безопасности при пользовании онлайн-сервисами

Среди пользователей социальных сетей тех, кто не уверен в защищенности своих аккаунтов, больше по сравнению с пользователями почты. Кроме того, почти две трети пользователей опасаются, что информация, которую они публикуют в соцсетях, может попасть в руки мошенников.

Насколько ваш аккаунт в соцсети защищен от мошенников?

63% ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ СЕТЕЙ ОПАСАЮТСЯ, ЧТО ИНФОРМАЦИЯ В СОЦИАЛЬНЫХ СЕТЯХ МОЖЕТ БЫТЬ ИСПОЛЬЗОВАНА В МОШЕННИЧЕСКИХ ЦЕЛЯХ



Источник: исследование Mail.Ru Group, 2014 г.

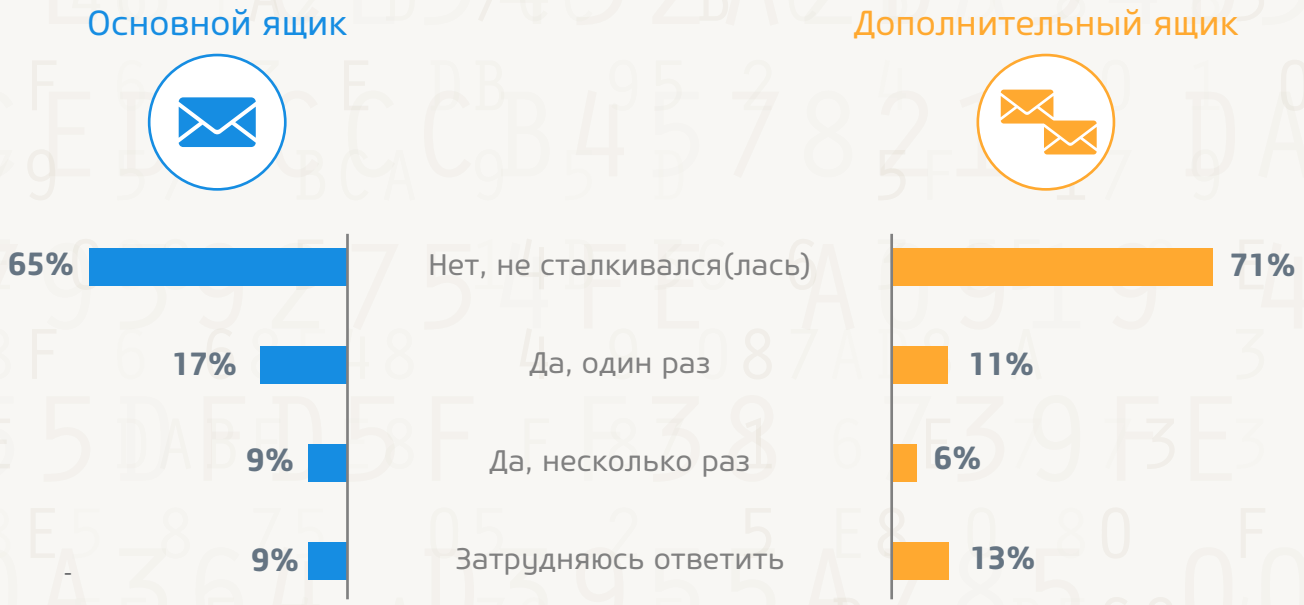
Опыт столкновения с мошенничеством[3]

На сегодняшний день интернет-мошенничество довольно распространено, и с ним ежедневно сталкиваются тысячи людей. Многие эксперты говорят о том, что чаще всего пользователи страдают из-за собственной беспечности или невнимательности, сводя на нет усилия интернет-компаний по повышению уровня безопасности. Это подтверждают и результаты нашего исследования.

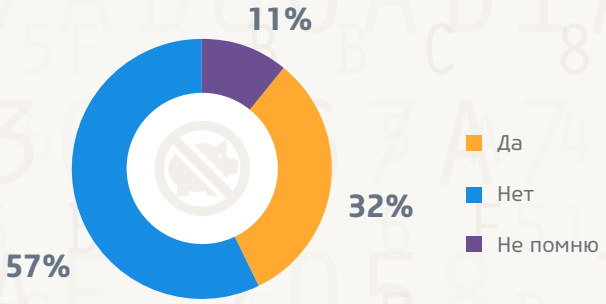
Четверть участников исследования сталкивались с кражей пароля от основного ящика, причем 9% — неоднократно. У 17% респондентов был украден пароль от дополнительного ящика.

Мошенничество в электронной почте

Сталкивались ли вы с кражей пароля от электронной почты?



Сталкивались ли вы с рассылкой спама из вашего почтового аккаунта?



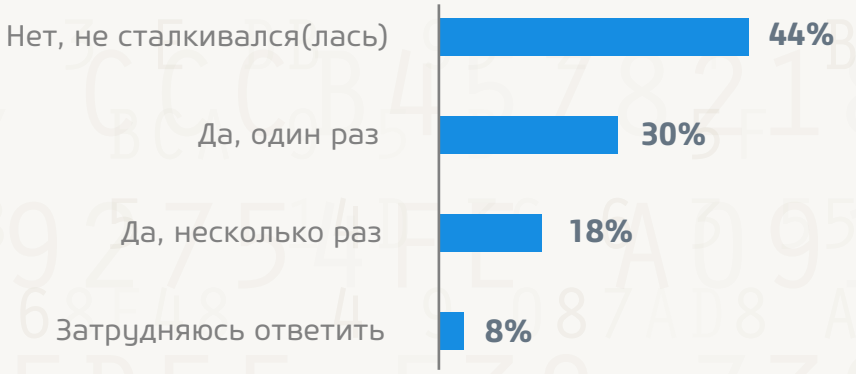
Источник: исследование Mail.Ru Group, 2014 г.

3 Под «мошенничеством» понимается кража пароля от аккаунта и/или рассылка спама от имени пользователя в почте, соцсети, а также мошенничество при онлайн-платежах (например, списание средств с карты)

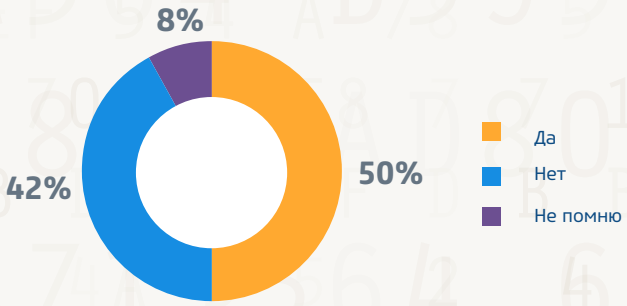
Респонденты чаще сталкиваются с мошенничеством в соцсетях, чем при использовании почты или совершении онлайн-платежей. Почти у половины пользователей социальных сетей (48%) воровали пароли, 58% получали мошеннические сообщения, половина сталкивались с рассылкой спама от своего имени.

Мошенничество в соцсетях

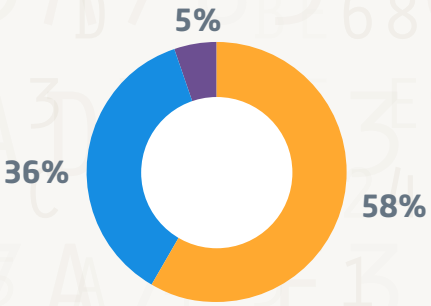
Сталкивались ли вы с кражей пароля от профиля в соцсети?



Сталкивались ли вы с рассылкой спама с вашего аккаунта?



Получали ли вы мошеннические сообщения в соцсети?



Источник: исследование Mail.Ru Group, 2014 г.

Уязвимость пользователей при пользовании онлайн-сервисами

Источник: исследование Mail.Ru Group, 2014 г.

Три основные причины, по которым пользователи становились жертвами мошенничества — использование простых паролей, закачивание вирусов, переходы на мошеннические сайты. При этом при проведении онлайн-платежей использование простого пароля реже становится причиной столкновения с мошенничеством.

Почему вы стали жертвой мошенничества?

	Пользователи почты	Пользователи соцсетей	Пользователи, совершавшие онлайн-платежи
Использовал(а) простой пароль	38%	37%	33%
Скачал(а) вирус	36%	36%	40%
Перешел(шла) по ссылке на мошеннический сайт	33%	33%	34%
Использовал(а) один и тот же пароль на нескольких сервисах	16%	16%	15%
Ответил(а) на мошенническое сообщение	14%	15%	15%
Не разлогинивал(а)ся(сь) при завершении работы в почте, соцсетях	14%	13%	15%

Источник: исследование Mail.Ru Group, 2014 г.

Мошенничество в сети: кто с ним сталкивается? Социально-демографический профиль пользователя

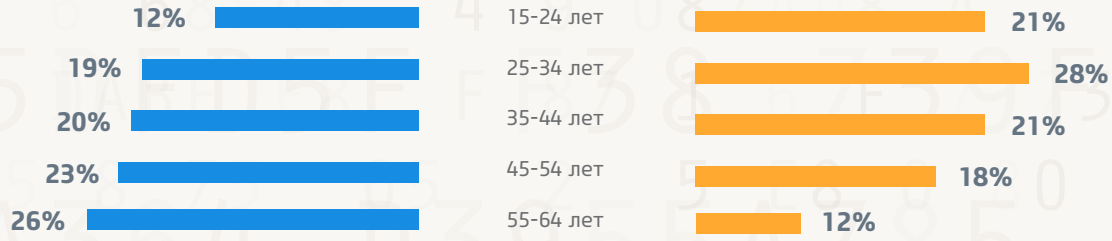
С мошенничеством в сети чаще всего сталкиваются люди в возрасте 15-34 лет, холостые или незамужние. Женщин среди них несколько больше, чем мужчин.

Чаще всего утверждают, что не сталкивались с мошенничеством в сети, люди старше 45 лет. Чаще они женаты (замужем) или состоят в гражданском браке. Мужчин среди них несколько больше, чем женщин.

Пользователи, не сталкивавшиеся с мошенничеством в сети

Пользователи, сталкивавшиеся с мошенничеством в сети

Возраст



Источник: исследование Mail.Ru Group, 2014 г.

Мошенничество в сети: кто с ним сталкивается?
Социально-демографический профиль пользователя

Источник: исследование Mail.Ru Group, 2014 г.

Эксперты о главных причинах взлома пользовательских аккаунтов

Мы спросили экспертов, каковы, на их взгляд, самые распространенные методы взлома пользовательских аккаунтов на сегодняшний день.

Владимир Дубровин
руководитель группы тестирования Mail.Ru Group:

— Чаще всего взлом происходит через троянские программы, которые угоняют аккаунты с компьютеров пользователей. При этом аккаунты администраторов и веб-мастеров сайтов могут быть использованы для размещения вредоносного кода на достаточно популярных ресурсах и заражения через них других пользователей. Еще один частый способ взлома пользовательских аккаунтов — через ошибки в сторонних сайтах и форумах, сделанных на базе популярных бесплатных движков или CMS. Когда в одном из таких движков находятся уязвимости, учетные данные пользователей сразу многих небольших сайтов утекают к злоумышленникам. Учитывая, что многие ленятся придумывать для использования мелкого ресурса что-то уникальное и используют в качестве логина свою электронную почту, а в качестве пароля — пароль от нее, то в результате у злоумышленников скапливаются огромные базы известных пар логин-пароль, с которыми затем они идут по всем почтовым сервисам.

Анна Артамонова
вице-президент Mail.Ru Group, руководитель бизнес-подразделения Почта и портал:

— Один из самых популярных методов интернет-мошенничества — это фишинг. Типичный пример — заставить пользователя ввести пароль на чужом сайте, замаскированном под дизайн страницы авторизации. Но если подделать страницу с такой формой довольно легко, то подделать доменное имя ресурса, которым вы постоянно пользуетесь, невозможно: отличия, пусть даже совсем незначительные (на одну-две буквы), все равно будут. Еще один распространенный метод фишинга — написать пользователю письмо якобы от администрации почтового сервиса с просьбой выслать под каким-то предлогом свой пароль. Если вы получили такое письмо, можете быть абсолютно уверены, что его отправили мошенники. Ни один уважающий себя почтовый сервис не просит пользователей высылать пароли от почтовых ящиков.

Эксперты о главных причинах взлома пользовательских аккуантов

Юрий Наместников
антивирусный эксперт «Лаборатории Касперского»:

— Достаточно распространенные методы взлома аккаунтов — это вирусы и фишинговые схемы. Создание подобных вредоносных программ поставлено на поток, и они мало чем отличаются друг от друга. Огромное количество троянцев несет в себе функционал кражи данных пользователя на различных сайтах, включая социальные сети.

Фишинговые приемы тоже хорошо известны, и принципиально за последние несколько лет ничего не изменилось. Некоторые из них нацелены именно на получение доступа к почтовому аккаунту или к аккаунтам в соцсетях.

Один из излюбленных инструментов фишеров — рассылки от лица друзей жертвы, например, в социальных сетях. Получая такое сообщение от своего друга, человек чаще всего открывает сообщение и переходит по ссылке, так как он доверяет отправителю. В итоге на его компьютер при наличии уязвимых версий программного обеспечения, например устаревшего браузера, автоматически может загрузиться вредоносная программа.

Арсен Исрапилов
директор по маркетингу и развитию бизнеса социальной сети Одноклассники:

— Исходя из атак и угроз, которые мы анализируем, самые распространенные методы взлома пользовательских аккаунтов — это фишинг и вирусы. Стоимость брутфорса достаточно высока, при этом необходимо знать логин и платить за разгадывание CAPTCHA. В социальных сетях крайне распространены схемы из разряда социальной инженерии и мошенничества: пользователю предлагается получить какой-то подарок или услугу даром на стороннем сайте, на котором необходимо что-то загрузить, ввести логин и пароль или код из SMS. В частности, мошенники часто предлагают пользователям Одноклассников получить бесплатно виртуальную валюту.

Андрей Прозоров
ведущий эксперт компании InfoWatch по информационной безопасности:

— Чаще всего данные пользователей оказываются скомпрометированными в результате заражения компьютера вредоносным ПО. Применительно к соцсетям это может быть вирус, использующий элементы социальной инженерии и направленный на кражу аккаунтов. Однако это уже другой тип угрозы, механизм работы которой рассчитан на невнимательность или доверчивость самого пользователя. Так что в отношении интернет-сервисов «слабым звеном» обычно является именно человек.

Сергей Вишняков
представитель хакерского сообщества, независимый исследователь:

— Если рассматривать самые популярные методы атак с целью получения доступа к закрытой информации, самой эффективной часто является социальная инженерия. В этом случае атака не направлена на компьютер или мобильное устройство пользователя — она направлена на самого пользователя. Есть мнение, что это самый надёжный способ проникновения в любую сеть. Социальная инженерия как метод атаки прекратит своё существование только в том случае, если человечество перестанет существовать. Используя человеческие ресурсы для воплощения своих планов, злоумышленники могут получить доступ абсолютно к любой информации.

Эксперты о методах защиты аккаунтов

Мы попросили экспертов дать пользователям онлайн-сервисов рекомендации, которые помогли бы им защититься от злоумышленников в сети. Большинство из них сходятся в том, что необходимо создавать надежные пароли, внимательно следить за наличием значка безопасного соединения в адресной строке браузера, обновлять программное обеспечение компьютера и использовать антивирус.

Анна Артамонова
вице-президент Mail.Ru Group, руководитель бизнес-подразделения Почта и портал:

— Часто бывает, что у юзера хорошо защищен основной ящик — тот, который он наиболее активно использует в данный момент. При этом у него есть несколько дополнительных аккаунтов, которыми он пользуется редко или считает «старыми», «бывшими» и, соответственно, не пользуется ими вообще, поэтому ему кажется, что нет смысла вкладываться в их защиту — то есть привязывать номер телефона, придумывать сложный пароль и регулярно его менять. Однако может оказаться, что именно к дополнительному ящику привязаны многие важные с точки зрения личных данных сервисы, например, Apple ID или аккаунты в платных играх. Так что я бы посоветовала, во-первых, навести порядок в ваших аккаунтах: вспомнить, какие почтовые ящики у вас есть и для чего нужен каждый из них, а во-вторых, хорошо защищать те, в которых хранятся важные для вас данные. Хотя в идеале, конечно, лучше защищать все — хотя бы для того, чтобы вашим друзьям не рассылали спам от вашего имени.

Юрий Наместников
антивирусный эксперт «Лаборатории Касперского»:

— Не доверяйте сообщениям от незнакомых пользователей и организаций, не кликайте по присланным ссылкам и не открывайте вложения. Если вы стали получать подозрительные письма и сообщения от ваших друзей, постарайтесь связаться с ними другим способом: скорее всего, их почтовый аккаунт или аккаунт в социальной сети попал в руки мошенников, и вашим друзьям необходимо как можно быстрее сменить пароль для доступа к нему. Самостоятельно вводите адреса важных сайтов в строке. После загрузки страницы обязательно проверьте наличие защищенного соединения HTTPS (его можно определить по иконке в виде замочка в адресной строке браузера). Отсутствие защищенного соединения даже при правильном адресе страницы говорит о том, что вы, скорее всего, находитесь на мошенническом ресурсе. Установите современное защитное решение и поддерживайте его антивирусные базы в актуальном состоянии.

Денис Аникин

технический директор Почты Mail.Ru:

— Говоря о защите аккаунта, принято в первую очередь советовать регулярно менять пароль, делать его сложным, не использовать на других сервисах и т.п. Однако как показывает практика, пароль не всегда является достаточным барьером для киберпреступников, поскольку его, например, можно украсть с помощью фишинга или вируса. Именно поэтому мы запустили в Почте и на портале Mail.Ru двухфакторную аутентификацию. Теперь, чтобы взломать ящик пользователя, подключившего у себя это решение, злоумышленнику придется не только узнать его пароль, но и получить доступ к мобильному телефону – а это уже в разы сложнее. Реализовать двухфакторную аутентификацию нас просили в основном продвинутые пользователи, но я очень надеюсь, что она станет популярна и у более широкой аудитории.

Сергей Вишняков

представитель хакерского сообщества, независимый исследователь:

— Есть целый сегмент пользователей, которые утверждают, что «им нечего скрывать». На мой взгляд, они разрушают понятие безопасности интернет-сервисов и развязывают руки киберпреступникам и мошенникам. Пользователи, разделяющие такое мнение, даже не догадываются, что подвергают опасности не только себя, но и других. Например, если пользователь, пренебрегающий правилами интернет-безопасности, заходит в интернет с точки доступа, трафик с которой прослушивает злоумышленник, то перехвачены будут не только его данные, но и данные тех, с кем он общается.

Что касается рекомендаций, основное — использовать стойкий пароль, который будет содержать цифры и буквы в разном регистре, а как максимум еще и специальные символы. Пароли лучше всего запоминать, но если это невозможно, храните их так, чтобы они не попали в руки злоумышленникам. Способов масса: от специализированных сервисов и ПО до зашифрованных контейнеров. Используйте плагины для браузеров AdBlock, которые обезопасят вас от баннеров, всплывающих окон, флеш-объектов и скриптов для выполнения сценариев в браузере.

Эксперты о безопасности в интернете

Владимир Дубровин

руководитель группы тестирования Mail.Ru Group:

— Желательно менять пароль не реже чем раз в три месяца и придумывать отдельный для каждого сервиса. Часто бывает так, что пользователь использует один и тот же пароль для почты и каких-то других интернет-ресурсов, в том числе форумов, торрент-трекеров, мелких онлайн-магазинов, которые пренебрегают защитой — и хакеры, зная об этом, атакуют именно их. Но поскольку на практике иметь абсолютно уникальный пароль для каждого сервиса — это все-таки сложно реализуемо, нужно придумать его хотя бы для почтового ящика, который наиболее критичен с точки зрения необходимости защиты.

Андрей Прозоров

ведущий эксперт компании InfoWatch по информационной безопасности:

— Первое и главное — не используйте простой или «золотой» пароль (одинаковый пароль для нескольких аккаунтов). Если боитесь что-то забыть, используйте менеджеры паролей. Второе — будьте внимательны и относитесь с подозрением к каждой ссылке, по которой вас просит пройти якобы друг из социальной сети. Третье — используйте антивирусы. Четвертое — к публичному WiFi надо относиться с большой осторожностью. Данные, которые вы отправляете на какой-либо сайт в интернете (в том числе логин и пароль) могут быть легко перехвачены злоумышленником. Как минимум надо быть уверенным, что вы подключаетесь к официальной WiFi-точке и что трафик идет по защищенному каналу HTTPS.

Илья Сачков

генеральный директор компании Group-IB:

— На данный момент однин из лучших способов защиты аккаунта – это выбор онлайн-сервисов с двухфакторной аутентификацией (например, через СМС) и привязка к железу (к компьютеру, телефону, приложению). К сожалению, не все онлайн сервисы предоставляют такую возможность.

Хорошим тоном со стороны интернет-компании является проверка аномалий пользовательской сессии: смена геолокации, конфигурации браузера, операционной системы, проверка учетной записи в ботнетах и т.п. То есть когда, например, ваша почтовая служба понимает, что вы живете в Москве и пользуетесь PC, а через 5 минут заходите почему-то из Нью-Йорка с макинтоша. Если это возможно, включайте sms или email-уведомление об использовании вашего аккаунта и периодически заходите в статистику пользования аккаунтом, где можно посмотреть историю ваших подключений.

Эксперты о дальнейшем развитии систем безопасности интернет-сервисов и о том, сохранят ли актуальность сегодняшние методы атак

В целом эксперты единодушны во мнении, что в будущем, как и на сегодняшний момент, обеспечение безопасности онлайн будет складываться из двух основных факторов. Первый — сознательный подход со стороны пользователей; второй — постоянная работа самих сервисов над усилением мер безопасности.

Анна Артамонова
вице-президент Mail.Ru Group, руководитель бизнес-подразделения Почта и портал:

— Уровень безопасности интернет-сервисов можно повышать практически до бесконечности, но это неизбежно повлечет за собой определенное неудобство для пользователей. А удобством, как показывает наш опыт, большинство жертвовать просто не готово. Поэтому интернет-сервисы продолжат искать компромисс между защищенностью и удобством юзеров. Мы стремимся к тому, чтобы обеспечить высокий уровень защиты даже тем, кто не умеет или не хочет заботиться о своей безопасности. Например, работа в Почте и на главной странице Mail.Ru по умолчанию идет по протоколу HTTPS — перейти на HTTP нельзя даже вручную. Недавно мы перестали предлагать новым пользователям возможность выбрать ответ на секретный вопрос как метод восстановления доступа к ящику, поскольку по сути ответ на секретный вопрос – это еще один пароль, а значит – потенциально уязвимое место. Помимо этого, мы используем HTTP only cookie, Secure Cookie, content security policy и разделение пользовательских сессий при доступе к различным проектам единого информационного портала Mail.Ru. А также целый ряд «фич», о которых мы не хотим рассказывать публично, чтобы не облегчать жизнь злоумышленникам.

Юрий Наместников
антивирусный эксперт «Лаборатории Касперского»

— Есть два основных направления развития безопасности интернет-сервисов: техническое и пользовательское. Техническое направление — это применение современных методов защиты. Нельзя один раз создать систему и считать ее полностью защищенной на протяжении многих лет, нужно постоянно совершенствовать способы защиты. Работа с пользователями является не менее важной составляющей безопасности. Какой бы современной ни была защита системы, всегда остается человеческий фактор. Еще пару лет назад крупные сервисы не считали взаимодействие с пользователями своим приоритетом, однако в последнее время работа в этом направлении заметно улучшилась.

Эксперты о дальнейшем развитии систем безопасности интернет-сервисов и о том, сохранят ли актуальность сегодняшние методы атак

Денис Аникин
технический директор Почты Mail.Ru:

— Одно из слабых мест в защите интернет-сервисов — это пароль. На уровень его сложности можно влиять: например, сегодня любой уважающий себя почтовый сервис дает пользователям рекомендации-подсказки, как составить надежный пароль, и не разрешает заводить легкие. Однако нельзя идти по пути его бесконечного усложнения, поскольку, если пароль сделать слишком сложным, пользователь обязательно его забудет. Соответственно, один из возможных вариантов — это отказ от пароля. Мы, например, уже сделали такой шаг, запустив в домене my.com первую в мире беспарольную почту, привязанную к мобильному телефону.

Сергей Вишняков
представитель хакерского сообщества, независимый исследователь:

— Единственная атака, которая останется актуальной на весь период жизни человечества — это социальная инженерия.

Владимир Дубровин
руководитель группы тестирования Mail.Ru Group:

— Взлом становится сложнее и дороже. Скорее всего, взломщики будут более «тщательно» использовать информацию, которую можно добыть из взломанных ящиков. Можно предположить, что будет больше атак с использованием персональной информации из ящика электронной почты — шантаж (в том числе шантаж не только самого пользователя, но и тех, о ком он ведет переписку), фишинговые и вирусные атаки на контакты пользователя.

Эксперты о дальнейшем развитии систем безопасности интернет-сервисов и о том, сохранят ли актуальность сегодняшние методы атак

Арсен Исрапилов
директор по маркетингу и развитию бизнеса социальной сети Одноклассники:

— Само собой, системы безопасности интернет-сервисов развиваются каждый день, становясь все надежнее. Но надо понимать, что сервис не может защитить пользователя на сто процентов. Пользователь и сам должен думать о защите своего профиля, в первую очередь — придумать сложный пароль, который будет невозможно угадать и подобрать. Гадать, что будет спустя пять-десять лет, не хочется — посмотрим. Ведь эволюционируют не только системы безопасности, но и методы взлома.

Илья Сачков
генеральный директор компании Group-IB:

— В будущем пароли станут рудиментом — вместо них придет биометрия, биопараменты (ритм сердца), голос и многое другое.

Выводы

В целом можно констатировать, что пользователи по-прежнему недостаточно внимательно следят за своей безопасностью в интернете.

Так, почти две трети пользователей онлайн-сервисов когда-либо становились жертвами мошенничества (64%). Среди причин пострадавшие чаще всего называют простой пароль, скачанный вирус или переход на мошеннический сайт. Почти в два раза реже пользователи отмечают, что пострадали из-за использования одного пароля на нескольких сервисах или из-за того, что ответили на мошенническое сообщение. Среди жертв мошенничества на онлайн-сервисах больше пользователей в возрасте 15-34 лет, не состоящих в браке, и женщин.

При вводе личных данных (например, логина или пароля) почти половина пользователей онлайн-сервисов (почты, социальных сетей) не проверяют наличие безопасного соединения.

Каждый пятый пользователь никогда не менял пароль от основного почтового ящика, и каждый третий — от дополнительного. К смене пароля в социальных сетях пользователи прибегают редко: 38% меняют пароль не чаще раза в год, а 18% вообще никогда не меняли пароль.

Почти четверть пользователей электронной почты применяют пароль от основного почтового ящика на других ресурсах, из них 62% — в социальных сетях, 27% — в онлайн-магазинах и 25% — в дополнительном почтовом ящике.

К безопасности дополнительного ящика пользователи склонны относиться менее бережно по сравнению с основным: реже меняют пароль, реже используют привязку номера телефона, предпочитая секретный вопрос для восстановления аккаунта.

Всего четверть пользователей используют наиболее безопасный пароль, состоящий из символов, букв и цифр. У 43% пользователей длина пароля не превышает восьми символов, пароль состоит из букв и цифр (без использования специальных символов). Чуть больше трети пользователей (37%) используют в пароле только строчные буквы. Если говорить о цифрах, используемых в пароле, 16% выбирают дату рождения — свою или близких. Что касается буквенных элементов пароля, каждый шестой пользователь выбирает русское слово, набранное латинскими буквами, 8% — фамилию, имя или отчество, 7% — несколько слов подряд.

Однако исследование выявило и позитивные тенденции.

Так, например, 51% пользователей утверждают, что используют разные пароли для всех аккаунтов, у 36% заведены разные пароли для наиболее важных учетных записей.

29% пользователей используют в качестве пароля произвольный набор букв и 27% - выдуманное ими самими слово.

43% респондентов используют пароли длиной от 6 до 8 символов. Чуть более четверти (27%) — от 9 до 10 символов. Однако можно предположить, что в основном это связано с тем, что сегодня многие онлайн-сервисы не позволяют пользователю ввести короткий и слишком простой пароль (так, при регистрации в Почте Mail.Ru или при создании нового профиля в Одноклассниках пользователь не сможет ввести пароль меньше шести символов и состоящий только из букв).

Выводы

Для восстановления пароля от основного ящика большинство пользователей (68%) используют привязку к номеру телефона.

Пользователи с осторожностью относятся к ссылкам, пришедшим на основной электронный ящик: почти три четверти опрошенных (74%) в таких случаях всегда внимательно проверяют адрес, прежде чем перейти по ссылке.