

**ПОПУЛЯРНЫЕ ИНТЕРНЕТ-СЕРВИСЫ:
УДОБСТВО ИЛИ БЕЗОПАСНОСТЬ?**

**ВКОНТАКТЕ, GOOGLE, MAIL.RU,
ЯНДЕКС, FACEBOOK**

АЛЕКСАНДР НАВАЛИХИН



2011 г.

ОГЛАВЛЕНИЕ

Цели и задачи.....	3
Предварительные замечания.....	4
ВКонтакте.....	5
Google.....	6
Mail.Ru.....	8
Яндекс.....	9
Facebook.....	10
Результаты	11
Исследовательский центр Positive Research.....	12
Об авторе.....	13
Контакты.....	14

1. ЦЕЛИ И ЗАДАЧИ

Сегодня социальные сети и интернет-порталы стали по-настоящему массовыми сервисами, которыми пользуются миллионы людей. При этом многие пользователи регулярно забывают пароли к своим страницам и почтовым ящикам, после чего в службы поддержки приходят тысячи писем с просьбой о помощи. Специально для подобных ситуаций интернет-ресурсы предлагают процедуру восстановления пароля.

Именно процесс восстановления пароля при ближайшем рассмотрении может оказаться слабым местом в системе безопасности популярных онлайн-сервисов.

Цель настоящего исследования – понять, насколько легко получить доступ к учетным записям пользователей социальных сетей и почтовых сервисов исключительно методами социальной инженерии, без специальных знаний и хакерского инструментария.

В ходе исследования эксперты Исследовательского центра Positive Research, инновационного подразделения компании Positive Technologies, провели несколько «социальных атак», объектами которых стали популярные социальные сети ВКонтакте и Facebook, а также сервисы Mail.Ru, Яндекс и Google. Вектор атак был направлен не на пользователей, а на сами сервисы (через процедуры восстановления паролей и виртуальное взаимодействие с сотрудниками службы поддержки).

В результате этих действий эксперты Positive Research смогли получить доступ к учетным записям пользователей нескольких ведущих интернет-сервисов. При этом использовалась только общедоступная информация о пользователе из Интернета.

2. ПРЕДВАРИТЕЛЬНЫЕ ЗАМЕЧАНИЯ

- Действия по восстановлению паролей затрагивали реальные учетные записи пользователей ВКонтакте, Facebook, Google, Mail.Ru и Яндекса. Владельцев этих учетных записей предварительно проинформировали о целях исследования и получили от них согласие на совершение действий с их учетными записями. После завершения проекта полученные реквизиты доступа были возвращены владельцам, никаких дополнительных действий с использованием этих данных не осуществлялось.
- Все интернет-ресурсы, с которыми работали эксперты Исследовательского центра Positive Research, получили уведомления о найденных уязвимостях.
- Каждый из рассмотренных сервисов получил оценку по двум параметрам: уровень защищенности и удобство для пользователя. Оценка выставлялась на основе экспертного мнения.
- Данное исследование не претендует на полноту, поскольку рассматривались лишь наиболее общие и очевидные векторы атак. Исследовательский центр Positive Research продолжает анализировать безопасность социальных сетей и других популярных интернет-сервисов, новости по этой теме будут публиковаться на сайте www.ptsecurity.ru.
- В данном исследовании приведен общий алгоритм работы с учетными записями для получения конфиденциальных данных пользователей. Дальнейшие результаты исследований на эту тему будут раскрыты на международном форуме по практической безопасности Positive Hack Days 30 и 31 мая 2012 года в Москве. Дополнительную информацию можно получить на сайте www.phdays.ru.

3. ВКОНТАКТЕ

О проекте

ВКонтакте – российская социальная сеть. Количество зарегистрированных пользователей – более 100 млн., из которых более 70% проживает в России.

Защита пользователя

ВКонтакте уделяет достаточно большое внимание обеспечению безопасности пользователей. Для этого используются сложные проверки CAPCHA, отслеживается подозрительная активность, пресекается спам, к странице пользователя есть привязка номера телефона. Также отслеживается и активность пользователей: в журналах регистрации событий фиксируются IP-адреса и названия браузеров, которые использовались для нескольких последних заходов на страницу.

Методика получения пароля

Для нескольких «социальных атак» была выбрана учетная запись среднестатистического пользователя ВКонтакте, на стене которого не были указаны контактные данные (электронная почта и номер телефона). В ходе ряда манипуляций с формой восстановления пароля, контактными данными и переписки со службой поддержки, доступ к странице этого пользователя был получен менее чем за сутки. Дополнительно эксперты провели несколько атак на учетные записи других пользователей, которые также увенчались успехом.

Выявленные проблемы

Слабое место системы безопасности ВКонтакте – недостаточно внимательное отношение службы поддержки к процедуре восстановления пароля. Так, специалисты службы поддержки не обратили внимание на то, что пароль был запрошен с IP-адреса, которым человек до этого никогда не пользовался. Также прошел незамеченным тот факт, что фотография пользователя с документом в руках (обязательное требование ВКонтакте при восстановлении пароля) содержала явные признаки редактирования.

Выводы

Ключевые функции в цепочке проверки данных ВКонтакте доверяет человеку, а это наиболее ненадежное звено, что позволяет злоумышленникам получить доступ к учетным записям пользователей.

4. GOOGLE

О проекте

Google – крупнейшая поисковая система, занимающая первое место по популярности в мире. Предлагает пользователям большое количество дополнительных сервисов: Gmail, Picasa, Code, Maps, Docs, Blogspot, YouTube, Google+, Android и т. д.

Защита пользователя

По утверждению специалистов Google, при принятии решения о восстановлении данных пользователя анализируется большое количество параметров с различными коэффициентами важности.

Для восстановления пароля к учетной записи пользователь заполняет форму, в которой указываются: время начала использования учетной записи, сервисы, подключенные к данной учетной записи, и информация о содержимом почтового ящика (метки, популярные корреспонденты и т. д.). Данная форма дает довольно полное представление о пользователе и призвана точно идентифицировать владельца учетной записи. Однако значительную часть запрашиваемой информации можно получить из открытых источников, в том числе и через сервисы Google.

Методика получения пароля

Как и в случае с социальной сетью ВКонтакте, при попытках получить учетные данные пользователя сервисов Google использовались только средства социальной инженерии, никаких специальных технических уловок не применялось. В результате с помощью манипуляций с формой восстановления пароля был получен доступ не только к учетной записи пользователя в почте Gmail, но и к другим сервисам Google: Picasa, YouTube, Google Analytics и т. д.

Выявленные проблемы

- Google уделяет недостаточное внимание IP-адресам, с которых пользователь заходит на страницу и которые используются при восстановлении пароля к учетной записи Gmail. Тем не менее необходимо отметить, что Google более щепетилен в этом вопросе, чем ВКонтакте.
- Процедура восстановления пароля была запущена в тот момент, когда владелец учетной записи продолжал работать с сервисами Google: общался через GoogleTalk, загружал файлы с Android Market. Сервисы перестали работать внезапно, без каких-либо предупреждений со стороны Google. Причем подобную атаку не смогла остановить даже двухфакторная авторизация с привязкой к мобильному телефону.

Выводы

Универсальная привязка к почтовому ящику всех сервисов Google при взломе учетной записи Gmail открывает злоумышленнику доступ ко всем службам системы, которыми пользуется человек.

Эксперты Исследовательского центра Positive Research сообщили Google о найденных уязвимостях, после чего уязвимости были исправлены.

5. MAIL.RU

О проекте

Почта Mail.Ru – это крупнейший в рунете сервис бесплатной почты, лидер по числу ежемесячных уникальных посетителей

Защита пользователя

Предъявляются стандартные требования: контрольные вопросы, привязка к номеру телефона и т. д. Особого внимания заслуживает интересная особенность: если почтовый ящик активен и им недавно пользовались, восстановить пароль с помощью контрольных вопросов невозможно. В этом случае пользователю предлагается восстановить пароль с помощью альтернативного e-mail или по номеру телефона.

Методика получения пароля

В случае с Mail.Ru общедоступной информации, которую можно найти в Интернете, оказалось недостаточно для получения пароля. Эксперты Positive Research использовали другие приемы социальной инженерии: в ходе знакомства с человеком в виртуальном пространстве (в социальной сети ВКонтакте) у него удалось получить всю необходимую для восстановления пароля информацию: ответы на контрольные вопросы, контакты и т. д.

Выявленные проблемы

При восстановлении пользовательских паролей Mail.Ru недостаточно использовать только общедоступную информацию человека. Доступ к учетной записи можно получить, только после предоставления необходимой информации самим пользователем.

Выводы

Mail.Ru проявляет открытость к своим пользователям, компания готова пойти навстречу во многих вопросах. Но в результате на первый план выходит ответственность самих пользователей и уровень их интернет-образования.

6. ЯНДЕКС

О проекте

Яндекс – крупнейшая российская поисковая система и интернет-портал. Помимо поиска Яндекс предоставляет пользователям большое количество сервисов, в том числе бесплатную электронную почту.

Защита пользователя

Предусмотрены стандартные способы восстановления пароля: привязка к номеру телефона, контрольные вопросы, возможность взаимодействия со службой поддержки, альтернативные почтовые адреса. Отдельно следует отметить детализированную форму обратной связи. Чем больше пользователь знает о своем почтовом ящике, тем больше шансов на восстановление доступа.

Методика получения пароля

Для получения доступа к учетной записи Яндекса эксперты Positive Research использовали уже проверенный подход. В ходе виртуального общения пользователь сам сообщил необходимую для восстановления пароля информацию (в том числе указал, как давно пользуется сервисами Яндекса). Однако возникло непреодолимое препятствие – служба поддержки потребовала личный визит пользователя в офис компании с паспортом в течение ограниченного срока. Доступ к учетной записи получить не удалось.

Выявленные проблемы

Надежная защита, помешавшая исследователям получить пароль к «Яндекс.Почте», может создать серьезные сложности как злоумышленникам, так и добросовестным, но забывчивым пользователям. Если злоумышленники действительно взломают почтовый ящик, к которому, в частности, привязана учетная запись в платежной системе «Яндекс.Деньги», то служба поддержки потребует личного присутствия в офисе компании с паспортом.

Выводы

Обязательное посещение офиса – достаточно жесткое требование даже для лояльных пользователей.

7. FACEBOOK

О проекте

Facebook – крупнейшая в мире социальная сеть. Количество ее активных пользователей превышает 800 млн. человек.

Защита пользователя

Схема защиты Facebook не совсем стандартная: есть привязка к электронной почте и телефону, также можно воспользоваться списком друзей для восстановления доступа к странице. Причем предполагается, что этих людей пользователь знает в реальном мире.

Методика получения пароля

Для получения доступа к учетной записи Facebook был выбран способ восстановления пароля с помощью друзей. Однако все манипуляции с созданием виртуальных друзей и контактов ни к чему не привели. При попытке «создать друга» для восстановления забытого пароля исследователи столкнулись с жесткими требованиями к самому понятию «друг». Для Facebook это учетная запись, которой его владелец активно пользуется уже некоторое время. Кроме истории, Facebook предъявляет серьезные требования к интенсивности коммуникации между друзьями. За 2 недели активности в этой социальной сети экспертам Positive Research так и не удалось попасть в список доверенных друзей.

Выявленные проблемы

Возможности пользователя Facebook, забывшего пароль, в принципе ограничены. Если по какой-то причине пользователь теряет доступ к почте и забывает ответ на секретный вопрос, Facebook сообщает, что ничем не может помочь и советует зарегистрироваться заново.

Выводы

Facebook демонстрирует наиболее взвешенный подход, который сочетает заботу об удобстве и безопасности пользователя. Человеку не придется выезжать в офис с паспортом в руках, при этом он надежно защищен от «социальных атак».

8. РЕЗУЛЬТАТЫ

- Процедура восстановления пароля оказалась недостаточно продуманным процессом в большинстве интернет-сервисов, проверенных в ходе исследования.
- Решая вопросы безопасности, интернет-сервисам приходится искать «золотую середину». Слишком мягкие правила и лояльность по отношению к пользователям приводят к тому, что учетные записи легко взламываются, а слишком жесткие правила могут оттолкнуть пользователей и создать им лишние неудобства. Проведенное исследование показало, что массовые интернет-проекты по-разному решают эту дилемму: одни стараются ограничить пользователей или требуют удостоверения личности, другие предоставляют больше свободы в ущерб безопасности.
- Онлайн-сервисы выдвигают немалое количество требований, которые должен выполнить пользователь при восстановлении пароля к своей учетной записи, но служба поддержки не всегда требует их выполнения на 100%. Это облегчает задачу злоумышленникам, которым удается обмануть техподдержку и восстановить чужие пароли.
- Сами пользователи продолжают вести себя в Интернете довольно легкомысленно. Они охотно делятся с первым встречным ответами на контрольные вопросы и прочей информацией, которая без труда позволяет получить доступ к их почте или учетным записям в социальных сетях.

Проект по оценке устойчивости популярных интернет-сервисов по отношению к «социальным атакам» продолжается, его результаты будут представлены на международном форуме по практической безопасности Positive Hack Days 30 и 31 мая 2012 года в Москве.

9. ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР POSITIVE RESEARCH

Исследовательский центр Positive Research – один из крупнейших в Европе исследовательских центров в области информационной безопасности. Центр является инновационным подразделением компании Positive Technologies, одной из ведущих компаний-практиков на российском рынке информационной безопасности.

В задачи Исследовательского центра входит анализ передовых тенденций в области информационной безопасности и их использование в развитии продуктов и сервисов компании. Эксперты центра занимаются проведением исследовательских, конструкторских и аналитических работ, анализом угроз и уязвимостей, содействуют в устранении ошибок в различных системах и приложениях.

С 2004 года с помощью экспертов Positive Research лидеры ИТ-отрасли, среди которых Microsoft, Cisco, Google, Avaya, Citrix, VmWare, TrendMicro, устранили несколько сотен уязвимостей и недочетов систем безопасности.

Деятельность Исследовательского центра неоднократно отмечалась благодарностями со стороны производителей программного обеспечения и систем защиты информации.

10. ОБ АВТОРЕ



Александр Навалихин – ведущий эксперт исследовательского центра Positive Research.

Окончил РХТУ им. Д. И. Менделеева, факультет компьютерных систем и технологий.

Ключевые компетенции: Unix-администрирование, безопасность веб-приложений, программирование на PHP, Perl и Python.

В Positive Research Александр возглавляет исследовательскую группу, занимающуюся вопросами социальной инженерии.

11. КОНТАКТЫ

Мария Широкова

Менеджер по связям с общественностью

Positive Technologies

Тел.: (495) 744-01-44

Моб.: +7 (903) 550-67-58

pr@ptsecurity.ru

Евгения Тарасова

Руководитель пресс-службы

Positive Technologies

Тел.: (495) 744-01-44

Моб.: +7 (903) 616-79-58

ETarasova@ptsecurity.ru

ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР POSITIVE RESEARCH

КОМПАНИЯ POSITIVE TECHNOLOGIES

107241 / МОСКВА / ЩЕЛКОВСКОЕ ШОССЕ / Д. 23 А

ТЕЛ.: +7 (495) 744 01 44 / ФАКС: +7 (495) 744 01 87

WWW.PTSECURITY.RU / WWW.MAXPATROL.RU / WWW.SECURITYLAB.RU