Программное обеспечение, указанное в данной статье, находится на вложенном DVD

Защита аккаунтов от взлома

Вредоносные программы, взломы баз данных, звонки в службу поддержки — злоумышленники используют всевозможные способы получения чужих данных для авторизации. Мы, в свою очередь, рассказываем о наиболее надежных мерах защиты.

Чтобы взломать чужой аккаунт, злоумышленники используют самые разнообразные методы, начиная с атак на смартфон и компьютер вредоносным ПО (например, чтобы установить кейлогер) и заканчивая прямыми атаками на веб-службы. В этой статье мы расскажем вам о том, какие меры необходимо предпринять, чтобы обеспечить практически идеальную защиту от киберугроз.

Атаки на веб-сервисы

Мечта любого злоумышленника, жаждущего похитить данные, — доступ к базе данных клиентов веб-сервиса. Ведь в ней хранятся сведения обо всех пользователях: подлинные имена, адреса, даты рождения и нередко даже пароли для входа. В 2013 году хакерам в результате масштабного взлома серверов Yahoo! удалось провернуть подобное и похитить данные всех пользователей — их тогда насчитывалось три миллиарда.

Как службы шифруют данные?

В большинстве случаев для баз данных используется криптография, а пароли пользователей шифруются дополнительно. Но какой именно метод защиты используется, знает только поставщик услуг, поэтому пользователям лучше заранее позаботиться о собственной безопасности самостоятельно.

Как защититься: собственно, универсального лекарства от всех угроз взлома нет, но можно свести к минимуму последствия хакерских атак. В любом случае используйте длинный и надежный пароль. Обычно пароли хранятся в базах данных сервисов в зашифрованном виде, поэтому данные для входа в аккаунт злоумышленники вынуждены расшифровывать отдельно. Соответственно, с короткими ненадежными паролями они справляются быстро. Кроме того, для разных служб используйте разные пароли, а еще лучше — и разные имена пользователя, чтобы злоумышленники поломали голову не только над паролем, но и над правильным именем для входа.

ФОТО: компании-производители; Photographee.eu/Fotolia.com

Правильно используем менеджер паролей

Менеджеры паролей тоже уязвимы. Так, надежность сервиса LastPass злоумышленниками была не раз скомпрометирована. Тем не менее использовать такие сервисы желательно, поскольку они позволяют оптимально синхронизировать доступ к отдельным учетным записям и управлять ими — по крайней мере, это безопаснее, чем использовать один и тот же пароль для нескольких сервисов. Руководствуясь следующими правилами, можно смягчить последствия атак.

Как защититься: обязательно используйте для сервисов типа LastPass самую последнюю версию браузера. Как показывает практика, атаки на сервисы всегда выполнялись через устаревшую версию веб-обозревателя. Кроме того, мастер-пароль нужно регулярно обновлять и выходить из учетной записи после каждого сеанса. Если синхронизация не требуется, вам лучше использовать программу KeePass, которая работает без подключения к Интернету. Но не забывайте постоянно создавать резервные копии баз данных паролей.

Угрозы для устройств

Злоумышленники могут добраться до вашего компьютера с помощью файловых вирусов, загрузок из Интернета и зараженных почтовых писем. Это наиболее многообещающий способ, поскольку огромное количество пользователей по-прежнему не пользуются антивирусными программами или не следят за обновлениями безопасности ОС.

Защита компьютера

Заражение, особенно через почту, — способ далеко не новый, но до сих пор пользующийся удивительной популярностью. В почтовых рассылках злоумышленники используют макровирусы, которые антивирусные программы не сразу обнаруживают, потому что пользователь собственноручно осуществляет их запуск. Письмо внушает пользователю, что во вложении содержится важный документ — например, счет за квартиру. При открытии документа в MS Word пакет Office предупреждает о том, что в документе содержится макрос, но тем не менее многие пользователи нажимают кнопку «Включить макрос». Таким образом злоумышленники получают возможность выполнять команды на компьютере в фоновом режиме.

Атаки с помощью загрузок не менее искусны. К примеру, в сентябре стало известно о взломе популярного инструмента CCleaner: злоумышленники внедрили в него вредоносный код, благодаря которому получили удаленный доступ к устройствам, не защищенным антивирусной программой.

Как защититься: самое главное — актуальность системы Windows. Все обновления безопасности от Microsoft нужно вовремя устанавливать; кроме того, обновлять нужно и инструменты от сторонних разработчиков. Мы рекомендуем утилиту для обновлений драйверов DriverPack Solution. А от таких угроз, как, например, в случае с CCleaner, защититься поможет платное антивирусное решение. Рейтинг лучших продуктов вы можете найти в нашем сводном тесте антивирусов (**https://goo.gl/UUiVad**). А запуск макросов Office разрешайте только для файлов, в отправителях которых вы не сомневаетесь.

Защита смартфона

Тем временем, многие смартфоны не менее уязвимы, чем ПК. И во многих случаях даже более, поскольку подключаются к различным сетям, используют Bluetooth для сопряжения с другими устройствами и не всегда вовремя получают обновления →

5 правил для повышения уровня защиты от угроз

1. Используйте надежный пароль В качестве пароля используйте длинные последовательности более чем из 15 символов и чисел.

2. Установите менеджер паролей Важно следовать правилу: для каждого сервиса — свой пароль. Данные для входа лучше всего хранить в зашифрованном виде в менеджере паролей.

3. Регулярно обновляйте пароли В лучшем случае о необходимости менять данные для входа периодически напоминает сам менеджер паролей. Менять же пароли для важных сервисов (например, для входа на почту) желательно хотя бы раз в квартал.

4. Используйте разные логины Чтобы обеспечить больший уровень безопасности, для каждой учетной записи по возможности используйте разные имена пользователя.

5. Обращайте внимание на добросовестность сервисов Вводите данные (например, адрес или номер счета) на сайтах, вызывающих доверие, а в случае сомнений поищите информацию об этом сервисе

Самые крупные утечки данных прошлых лет

В 2013 году сервис Yahoo! сильно пострадал: в результате взлома были похищены данные трех миллиардов пользователей.

ИСТОЧНИК: Statista, собственные исследования

Сайт haveibeenpwned.com проверяет практически все известные базы данных паролей на наличие вашего аккаунта

Угроза для устройств: 5 важных советов

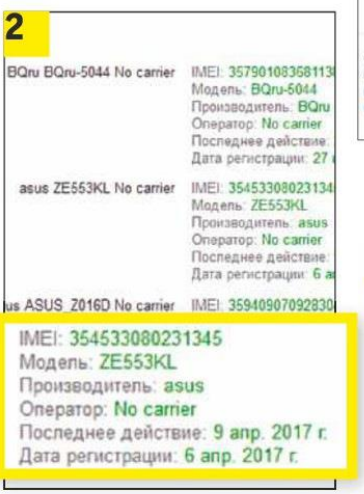
1. Устанавливайте обновления ОС Следите за состоянием Windows и операционной системы смартфона и обязательно устанавливайте все доступные обновления безопасности.

2. Обновляйте приложения и программы Для Windows используйте утилиту DriverPack, чтобы следить за обновлениями драйверов. Для Android и iOS используйте только официальные магазины приложений.

3. Устанавливайте антивирусные инструменты Если вы пользуетесь системами Windows или Android, обязательно установите антивирусную программу.

4. Активируйте двухфакторную защиту По возможности активируйте двухступенчатую аутентификацию (см. таблицу внизу).

5. Проверяйте подключенные устройства Список подключенных к учетной записи устройств находится в настройках аккаунта на сайте производителя и непосредственно в соответствующей системе.



Проверка статуса устройства

Регулярно проверяйте список устройств, использующих ваш аккаунт: это возможно как для Apple 1 , так и Android 2 . Незнакомые устройства немедленно удаляйте

Сервисы с двухступенчатой авторизацией

Дополнительную защиту от атак обеспечивает одноразовый пароль, отправляемый в виде SMS или через приложение.

Сервис	Код через приложение	Код по SMS
Amazon	○	●
Dropbox	●	●
eBay	○	●
Evernote	●	●
GMX	○	○
Google	●	●
LastPass	●	○
«ВКонтакте»	●	●
Office 365	●	●
PayPal	○	●
Mail.ru	○	●
«Яндекс»	●	●
Facebook	○	●

●Да ○Нет

безопасности. Более того, бывает, что даже новейшее обновление безопасности не в состоянии помочь — например, как это случилось с вирусом BlueBorne. С его помощью злоумышленники могли получить доступ к гаджету через Bluetooth. Потенциальной жертве достаточно активировать на смартфоне Bluetooth (например, для подключения смарт-часов), чтобы хакер смог ею воспользоваться. Под угрозой оказались практически все устройства, как на iOS, так и на Android. Apple и Microsoft в настоящее время уже закрыли уязвимость.

Google для Android тоже выпустила патч — правда, только для новых устройств, и прежде он должен пройти проверку качества у производителя смартфона. А пока нет обновления, Android не защищена. Более того, уязвим не только Bluetooth, но и Wi-Fi. Совсем недавно Apple закрыла баг новой iOS 11 в чипе беспроводной сети, через который злоумышленники могли поместить вредоносное ПО в смартфоны.

Как защититься: как и для Windows, самый лучший способ защиты от злоумышленников — это вовремя обновлять ПО. Для Apple iOS следовать этому совету еще относительно просто, потому что патчи доступны и для более старых устройств. А пользователи Android нередко оказываются беззащитны. Поэтому на Android всегда требуется дополнительно устанавливать антивирусную программу.

Если устройство или аккаунт уже попали в руки злоумышленников — хакеры уже используют вашу учетную запись. Проверьте список подключенных устройств, использованных для входа в аккаунт. Для iOS это меню «Настройки»: коснитесь своего имени iCloud, чтобы внизу посмотреть список подключенных устройств. Если увидите незнакомое устройство, коснитесь его и выберите «Удалить из аккаунта». На Android-гаджетах откройте **https://myaccount.google.com**, поищите незнакомое вам устройство и нажмите «Что-то не так?», чтобы закрыть для него доступ к аккаунту. Пользователям обеих операционных систем — и iOS, и Android — в случае обнаружения незнакомого оборудования немедленно следует изменить пароль.

Еще больший уровень безопасности при входе в аккаунт обеспечивает двухступенчатая аутентификация. Каждый раз во время осуществления входа после ввода пароля пользователю отправляется одноразовый код (или в виде SMS на смартфон, или прямо в приложении, в зависимости от сервиса). Список сервисов, которые предлагают эту дополнительную защиту, представлен в таблице слева.

Социальная инженерия как лазейка для злоумышленников

Доступ к чужим аккаунтам хакеры обеспечивают себе не только рассылкой вредоносного ПО или атаками на веб-серверы служб. В некоторых случаях им помогают сами жертвы, сами того не ведая. В очень целенаправленных атаках злоумышленники даже выдают себя за пользователей и обращаются в службы поддержки, чтобы узнать пароль. Но этому можно помешать.

Взлом аккаунтов с помощью фишинга

Этот простой, но результативный метод заключается в следующем. Злоумышленники рассылают электронные письма якобы от имени банков или веб-служб со ссылкой на подложный сайт. Цель — заставить пользователей перейти по ссылке в письме, который переведет их на подложную веб-страницу. И письма, и подложные сайты внешне очень трудно отличить от настоящих. Как только пользователь введет свой логин и пароль на подложном сайте, они автоматически попадают в руки хакеров.

Как защититься: чтобы понять, что перед вами фишинговое письмо, нужно сначала изучить его содержание. Банки и веб-сервисы никогда не запрашивают никаких PIN- или одноразовых TAN-кодов. Но иногда тексты таких писем формулируются настолько хорошо, что содержание не вызывает сомнений — письмо может выдаваться, например, за подтверждение заказа в онлайн-магазине или что-нибудь в этом духе.

Если содержание письма у вас подозрений не вызывает, проверьте отправителя. Но не просто посмотрите на поле с адресом — он тоже может быть подложным. Откройте исходное сообщение через свойства письма. В Outlook, например, для этого нужно кликнуть правой кнопкой мыши по письму и выбрать «Параметры сообщения». Настоящий отправитель отображается в поле «Заголовки Интернета». Порядок действий для веб-клиентов аналогичный. Если имя отправителя не соответствует названию веб-сервиса, будьте осторожны: высока вероятность того, что вы имеете дело с фишингом.

Но в некоторых нечастых случаях даже здесь злоумышленникам уже удалось клонировать имя отправителя письма. Поэтому в завершение нужно проверить ссылку, содержащуюся в письме. Правой кнопкой мыши скопируйте ее в буфер обмена и затем нажмите «Добавить» в адресной строке браузера, чтобы увидеть ссылку полностью, не открывая ее. Если ссылка ведет не к сервису, а совершенно на другой сайт, удалите письмо. В противном случае откройте сайт и проверьте сертификат. Если он действителен, скорее всего, это настоящий сайт сервиса.

Атаки с применением социального воздействия

В угоне аккаунта пользователю необязательно участвовать волей-неволей. Для получения доступа к учетной записи хакеры все свободнее используют доступную в Интернете информацию. Для таких прицельных атак злоумышленники могут, например, тщательно просматривать записи в Facebook или Instagram, чтобы на основании собранной информации попытаться ответить на контрольные вопросы почтового сервиса и задать новый пароль. То же самое касается и веб-хостингов: например, сервиса GoDaddy. Когда пользователь обращается по горячей линии в службу поддержки, он аутентифицируется с помощью четырехзначного PIN-кода. Если код простой — например, дата рождения, — то злоумышленнику отгадать его будет легко, и так же легко ему будет позвонить в службу поддержки и изменить данные учетной записи.

Как защититься: для сервисов, которые предоставляют возможность сбросить пароль по контрольному вопросу, используйте непредсказуемые пары вопросов и ответов. Например, на вопрос «О чем я сейчас думаю?» ответом установите комбинацию букв и цифр. Главное — сами не забудьте свой ответ после того, как дали вашей фантазии разгуляться.

То же самое касается PIN-кодов для телефонов. Обратите внимание на то, чтобы последовательность цифр не соответствовала какой-либо комбинации, легко угадываемой по вашей повседневной жизни, и чтобы символы в ней не повторялись (например, не стоит использовать код банковской карты везде, где только можно, в качестве PIN). Кроме того, ограничьте возможность просмотра ваших профилей в Facebook, Instagram и других социальных сетях. На большинстве сервисов в настройках можно запретить вывод профиля в результатах поиска Google — для Facebook, например, этот параметр находится в меню «Настройки | Конфиденциальность».

Следуйте рекомендациям по безопасности, предложенным в этой статье, и злоумышленникам будет очень трудно добраться до информации на вашем аккаунте.

Социальные атаки: 5 важных советов

1. Запретите отображение данных профиля в поисковиках Отмените в Facebook и других сетях разрешение выводить в результатах поиска Google личные сведения.

2. Активируйте защиту PIN-кода для горячих линий службы поддержки В качестве кода авторизации для обращений на горячую линию используйте случайный набор цифр, а не дату рождения.

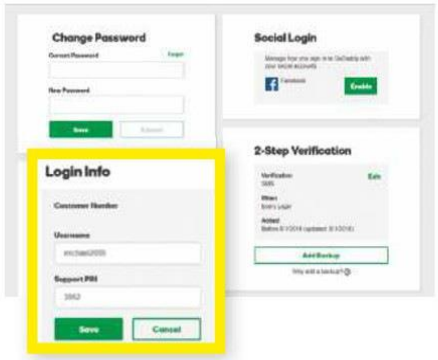
3. Обращайте внимание на имя отправителя Если вы получите письмо с подозрительным содержанием, проверьте в свойствах письма имя отправителя: отображаемый адресат может оказаться подложным.

4. Проверяйте ссылки, содержащиеся в письмах Копируйте ссылки из подозрительных писем в буфер и вставляйте в адресную строку браузера, не переходя по ним.

5. Проверяйте сертификаты сайтов На сайтах, запрашивающих данные для авторизации, обращайте внимание на SSL-сертификаты — они должны быть корректными и действительными.

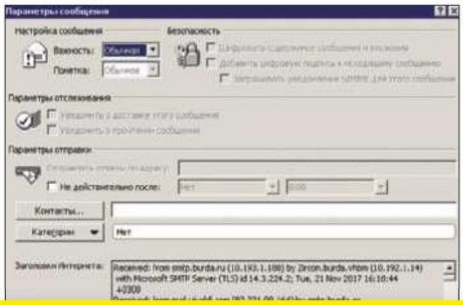
Контрольные вопросы с нелогичными ответами

Для контрольных вопросов никогда не устанавливайте ответом реальный текст. Лучше задайте последовательность из букв и цифр



PIN-код для службы поддержки

Чтобы хакер не выдал себя за вас в службе поддержки, используйте PIN-код, который отгадать не так просто, как дату рождения



Проверка отправителя

В «Параметрах сообщения» Outlook можно получить подробную информацию о том, откуда пришло письмо