СОВЕТЫ ПО КИБЕРБЕЗОПАСНОСТИ

СОДЕРЖАНИЕ

О РУКОВОДСТВЕ

Среди секс-работников региона все больше тех, кто использует сайты для свиданий, сайты для эскорта, приложения в мобильных телефонах и социальные сети для работы и активизма.

Интернет может дать секс-работникам новые возможности, больше свободы и большую безопасность. Он дает нам возможность работать на себя, принимать осознанные решения и развивать общину. Это место, где можно давать друг другу советы об охране сексуального здоровья и безопасности, делиться информацией и поддерживать друг друга в ходе кризиса. Однако с интернетом связаны и новые угрозы.

Число пользователей растет, но стигма и насилие не снижаются, поэтому мы часто видим, что интернет становится орудием в руках клиентов, полиции и государства. Шантаж, незаконное распространение личных данных в интернете и цифровые атаки стали повседневностью, что в некоторых случаях даже угрожает жизни секс-работников. В странах с авторитарными режимами, где принято следить за гражданами онлайн, риски для секс-работников и активистов вполне реальны. Необходимо объединиться и оценить наш общий опыт, риски и меры, которые мы, как сообщество, можем принять, чтобы защитить себя.

Данное руководство было составлено с опорой на материалы четырех онлайновых тренингов, которые СВАН провела летом 2022 и в ходе которых секс-работники и активисты могли задавать вопросы консультанту по цифровой безопасности, поделиться опытом, потребностями и проблемами с целью повысить цифровую грамотность, оценить онлайновые риски и уязвимые места и научиться простым методам защиты онлайн.

В руководстве вы найдете советы по охране безопасности при работе с наиболее часто используемыми онлайновыми платформами, приложениями для смартфонов и такими устройствами как телефон или компьютеры. Мы надеемся, что это руководство будет полезно вам и вашим общинам, и что этот материал станет еще одним шагом к созданию инструментов для охраны безопасности секс-работников онлайн, созданных секс-работниками.

АКТИВЫ

ШАГ 1 Подумайте, какими активами вы обладаете?

Активом может быть все, что у вас есть, что вы используете в своей рабочей и личной жизни. Это и техника (ноутбуки, компьютеры, смартфоны), и документы (паспорт, водительское удостоверение, рабочий контракт), и аккаунты (почта, мессенджеры, рабочие сайты, банковские сервисы). Перечень активов неисчерпаем, для каждой и каждого из вас он уникальный, только вы можете узнать, какие активы у вас есть.

Запишите все ваши активы на листок или в электронный документ.

ШАГ 2 Что плохое может произойти с вашими активами?

Подумайте о том, что конкретно может случиться с каждым из ваших активов?

Например, почтовый аккаунт могут взломать, прочитать ваши переписки или написать что-то от вашего имени. Ноутбук же могут украсть, его можно и просто потерять, сломать, разбить, залить водой.

Пройдитесь по всему списку своих активов и допишите к каждому из них все, что может с ними произойти. Это и будут ваши риски.

ШАГ 3 Как предотвратить риски?

Для каждого риска попробуйте найти ответы на вопросы:

- Как предотвратить риск? Что сделать, чтоб риск не случился, или уменьшить вероятность наступления риска?
- Как уменьшить последствия? Что стоит сделать заранее, чтоб в случае наступления риска, последствия были минимальны?
- Что делать после наступления риска? Если риск все же произойдет, что стоит сделать сразу после его наступления для минимизации вреда?

ШАГ 4 Рассмотрим пример

Мой актив – аккаунт в Фейсбуке. Что с ним может произойти?

- Я могу потерять доступ к аккаунту, забыв пароль
- Его могут взломать
- Его могут заблокировать из-за массовой атаки ботов с жалобами на мои посты

Для риска «Взлом аккаунта в ФБ» отвечу на свои вопросы:

- Как предотвратить риск? Что сделать, чтоб риск не случился, или уменьшить вероятность наступления риска?
    - Защитить аккаунт. Установить двухфакторную аутентификацию на вход, использовать сложный и уникальный пароль
- Как уменьшить последствия? Что стоит сделать заранее, чтоб в случае наступления риска, последствия были минимальны?
    - Не вести важных переписок внутри фейсбука

- Что делать после наступления риска? Если риск все же произойдет, что стоит сделать сразу после его наступления для минимизации вреда?
    - Оповестить друзей в ФБ о том, что аккаунт был взломан
    - Попытаться восстановить доступ к аккаунту через техподдержку
    - Если в ФБ велась какая-то конфиденциальная переписка – оповестить через альтернативные каналы связи собеседника о том, что аккаунт был взломан и переписку могли увидеть. Возможно, собеседник сможет удалить ее прежде, чем взломщик сможет её прочитать.

АТАКИ

ШАГ 1 Фишинг

Фишинг – ловля на живца. Ловить будут вас. Цель – получение ваших персональных данных, логинов, паролей.

Фишинговые письма обычно выглядят привлекательно или эмоционально. Я выделяю 3 типа фишинговых писем:

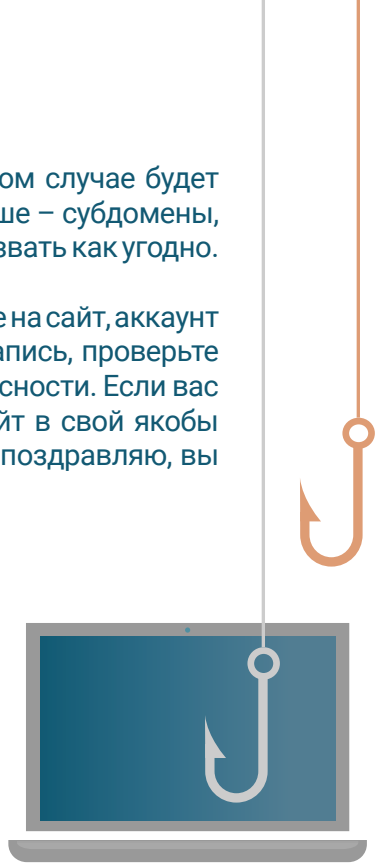
1. Угроза вашему аккаунту

Такое письмо содержит явные угрозы вашему аккаунту, текст письма может выглядеть примерно так: «Ваш аккаунт был взломан, чтобы защитить его – немедленно перейдите по ссылке».

Обычно ссылка из письма ведет на сайт – копию того, аккаунт на котором у вас якобы взломали, однако адрес сайта будет отличаться. Например, вместо google.com вы можете увидеть в адресной строке что-то такое:

google.com.this.site.is.real.novirusesthere.com. Доменом в таком случае будет не google.com, а bovirusesthere.com, а все, что написано раньше – субдомены, которые можно сделать на любом сайте, и которые можно назвать как угодно.

Не переходите по ссылке из письма, а самостоятельно зайдите на сайт, аккаунт на котором якобы был взломан. Зайдите в свою учетную запись, проверьте историю входов в аккаунт, историю действий в сфере безопасности. Если вас беспокоит это – смените пароль. Однако если, зайдя на сайт в свой якобы взломанный аккаунт, вы не увидите никаких оповещений – поздравляю, вы только что успешно избежали фишинговой атаки!



2. Вы выиграли миллион долларов!

Такие письма обычно направлены на кражу ваших денег. В некоторых случаях у вас попросят оплатить налоги, залоговый или комиссионный платеж, это может называться как угодно. Если вы не участвовали в лотерее – вы не могли в ней выиграть. Так что на этом пункте останавливаться на долго не будем.

3. Рабочее письмо со вложением

Вы можете получить вполне легитимное письмо с каким-то неоплаченным счетом, с каким-то документом, да с чем угодно. Письмо может выглядеть правдоподобно, но вы, вероятно, не вспомните адресата. В этом случае во вложении в письме может оказаться вирус.

Внимательно посмотрите на название файла во вложении, а не только на его иконку. Если файл заканчивается на .exe, .msi, .vbs, .reg, .dll – такой файл может быть вредоносным.

Если же файл выглядит реалистичным – попробуйте открыть его в режиме предпросмотра (например, используя почту Гугл вы можете открывать почти все форматы документов).

Если вам все же нужно загрузить файл на компьютер и открыть его, и если его расширение безопасно – проверьте файл на вирусы встроенным антивирусом. В качестве альтернативы вы можете использовать онлайн сервис VirusTotal. Загрузите файл, и он будет проверен множеством антивирусов.

ШАГ 2 Вирусы

Одна из самых привычных атак – вирусы. Многие из вас с ними сталкивались. Вирусы могут по-разному вредить вашей системе. Некоторые вирусы шифруют ваши файлы, некоторые – перехватывают управление вашим компьютером, некоторые тихо и незаметно следят за всем, что вы делаете.

Как мы можем подхватить вирус?

1. Из письма. Этот способ мы рассмотрели ранее.
2. Из чата в мессенджере. К чатам применимы все правила безопасности как для обычной почты.
3. Вместе с пиратским ПО. Качая пиратское ПО, вы добровольно соглашаетесь, что вирус, который взломает нужную вам программу, будет запущен. Как поведет себя взломщик дальше? Он только взломает программу, или глубоко засядет в систему? Ответа у меня нет, поэтому я рекомендую всегда использовать только легальное ПО.
4. На флешке. Вы можете найти флешку на улице или вам может дать ее доверенный человек, в любом случае каждую флешку, которую вы вставляете в компьютер, стоит просканировать антивирусом. Кроме того, при подключении флешки ОС предложит вам несколько действий на выбор: открыть флешку в проводнике, отформатировать флешку или запустить актозапуск. Никогда не соглашайтесь на автозапуск флешки, так как в программе автозапуска может прятаться вирус. Откройте флешку в проводнике и дальше исследуйте нужные вам файлы.

Как защититься от вирусов?

Установите и всегда обновляйте антивирус. Никогда не используйте взломанные пиратские версии антивирусов, если не хотите покупать какой-то из них – просто включайте Защитник Windows.

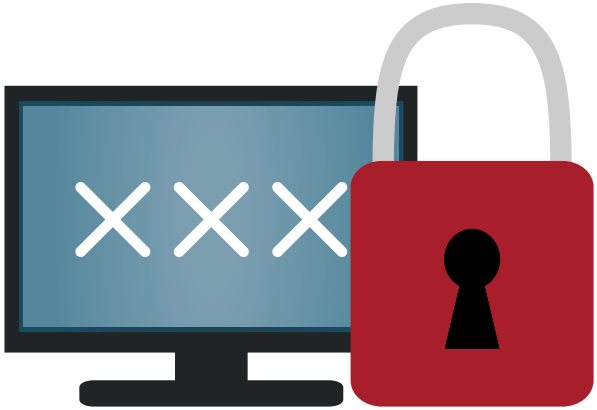
ШАГ 3 Удаленные атаки с использованием «Уязвимостей нулевого дня»

Такие атаки чаще всего совершаются против конкретных людей с конкретной целью. Гражданские активисты, видные политики, деятели искусства – такие люди становились жертвами атак. Вероятно, вы никогда не столкнетесь с такой атакой. Однако, если ваш уровень рисков таков, что, по-вашему, против вас могут совершать прямые атаки – обратитесь за консультацией к специалистам по кибербезопасности. Вы можете обратиться к составителю данного документа Генри Демьяновичу, его контакты указаны на последней странице.

ЗАЩИТА АККАУНТОВ

ШАГ 1 Какие аккаунты нужно защищать?

Защищать стоит все свои аккаунты на сколько это возможно. И рабочие, и личные. Стоит разделать рабочие и личные аккаунты, использовать разные пароли для них.



ШАГ 2 Пароль

Несколько признаков надежного пароля:

- Длинный (от 8 символов)
- Разнообразный (включает большие, малые буквы, цифры)
- Уникальный (разные пароли для разных сайтов)
- Не связанный с вами (не используйте в паролях дату рождения, никнейм, кличку собаки и т. д.)

В современных реалиях регулярно менять пароли не нужно. Вам стоит поменять свой пароль только в том случае, если он был или мог быть скомпрометирован, то есть его могли узнать.

ШАГ 3 Хранение паролей

Как вы уже знаете, для безопасности стоит использовать уникальные пароли для каждого сайта, но ведь запомнить уникальные пароли практически невозможно. Что же делать? Использовать парольный менеджер.

Если вы используете iPhone, скорее всего вы уже встречались со встроенным парольным менеджером, который предлагает сохранять пароли из приложений и сайтов, а также умеет генерировать сложные пароли при регистрации.

Если же вы предпочитаете Android, то могли видеть в работе Google Smart Lock.

Кроме того, все популярные браузеры предлагают вам сохранять пароли в них.

Кроме указанных выше есть специальные менеджеры паролей, они позволяют хранить все пароли в одном приложении, но получать доступ к ним на любом устройстве. Я, например, использую BitWarden.

Как видите, способов хранения паролей достаточно много, вы можете выбрать любой из них. Каждый из них лучше, чем запоминание.

Однако, если вы все же решили запоминать пароли – используйте по меньшей мере 2 а лучше 3 разных пароля: 1 основной, для личной жизни, почты, банков. 2 – для работы, рабочих аккаунтов и сайтов. 3 – для «мусорных» сайтов, сайтов, где нужно зарегистрироваться для чего-то разового или не очень важного, например для загрузки электронной книги.

ШАГ 4 Двухфакторная аутентификация

Большинство сайтов позволяют настроить двухфакторную аутентификацию. Иногда это называют двухэтапной проверкой. Первым фактором выступает ваш пароль. Вторым фактором может выступить что-то из списка:

- Pop-up уведомление с текстом «Вы входите в свой аккаунт, подтвердите вход»
- Одноразовый СМС-код
- OTP-код из приложения Google Authenticator (или аналогичного)
- USB-ключ (выглядит как флешка)
- Резервные коды восстановления (генерируются после настройки в качестве второго фактора любого другого фактора)

Вы можете выбрать любой удобный для вас второй фактор, однако следует знать некоторые особенности каждого из них.

Pop-up уведомление будет доступно только на смартфонах, на которых произведен вход в аккаунт. Этот способ работает с аккаунтами Google, Facebook и некоторыми другими. Большинство сайтов и приложений не поддерживают такой метод

СМС-код – стандартный второй фактор, его поддерживает большинство сервисов, однако стоит понимать, что СМС возможно перехватить, и если у злоумышленника будет цель взломать персонально вас несмотря на цену атаки, или если оппонентом будет государство – СМС-код не сможет вас защитить.

OTP-ключ, наверное, самый распространенный и самый надежный способ двухфакторной аутентификации. Вы можете выбрать одно из множества приложений для генерации ключей, но важно помнить, что стандартный Google Authenticator не

позволяет вам делать резервную копию ваших кодов доступа. Это значит, что вы потеряете доступ к своим аккаунтам, если случайно удалите Google Authenticator со смартфона, или если потеряете доступ к самому смартфону. Чтобы этого избежать я использую Aegis. Это приложение позволяет делать резервные копии ваших кодов, защитить копии паролем, да и доступ к кодам также надежно защищен.

USB-ключ – отличный способ входа. Microsoft предлагает вовсе отказаться от пароля в пользу USB-ключа. Ключ может работать и с компьютером, и со смартфоном. Существуют также беспроводные NFC ключи. Особенность ключа в том, что он физически один, и чтоб получить доступ к аккаунту, нужно держать его в руках. Если ваш ключ лежит в надежном месте – никто никак не сможет получить доступ к аккаунту, даже имея ваш пароль. Но и вы не сможете получить доступ к своему аккаунту пока не возьмете ключ в руки.

Резервные коды – последний рубеж, который может спасти вас в критической ситуации. Резервные коды следует распечатать на бумаге и отложить в надежное место. Когда-то, когда вы потеряете доступ к своему второму фактору, и вам потребуется восстановить доступ к аккаунту, они могут вас спасти.

Надежный пароль и настроенная двухфакторная аутентификация – залог безопасности ваших аккаунтов.

ШАГ 5 Беспарольные аккаунты

На некоторые сайты и в некоторые приложения вы можете входить без пароля. Вы можете зайти, используя свой Google или Facebook аккаунт. Вход в таком случае произойдет буквально одной кнопкой. Опасность такого входа состоит в том, что вы можете ненароком передать сайту намного больше информации о вас, чем он просит. Внимательно читайте, какие доступы получит сайт при авторизации через Google или Facebook. Обычно, сайт получит ваше имя, почту, возможно аватарку, возможно дату рождения. Если же сайт требует больше информации – это повод задуматься о его надежности.

В целом использование Google или Facebook аккаунтов для авторизации на других сайтах значительно более надежно, чем регистрация на них с паролем. Ведь вам достаточно защитить только свой Google или Facebook, а не все аккаунты на всех сайтах.

ЗАЩИТА НОУТБУКА

ШАГ 1 Установка пароля на вход

Пароль на вход в ноутбук защитит вас от краткосрочного доступа к ноутбуку третьих лиц. Если вы оставите ноутбук без пароля на 5 минут, кто-то может зайти в него и быстро посмотреть что-то, например историю браузера.

Пароль не защитит вас в случае кражи или долгосрочного доступа к вашему ноутбуку.

ШАГ 2 Использование шифрования BitLocker

Для защиты всей информации на вашем ноутбуке вы можете установить шифрование диска BitLocker. Оно доступно в Pro версии ОС Windows 7, 8, 8.1, 10.

На более старых ноутбуках вам потребуется придумать пароль, который нужно будет вводить дополнительно к паролю на вход в систему. На более новых ноутбуках пароль придумывать не придется.

При включении BitLocker система предложит вам сохранить или распечатать ключ восстановления. Обязательно сохраните его где-либо. В случае чего этот ключ поможет вам восстановить доступ ко всем вашим файлам.

ШАГ 3 Включение Защитника Windows

Вирусы в последнее время почти не атакуют простых пользователей, их активность спадает, однако они все еще существуют, и все еще опасны. Защитник Windows – достаточно хороший антивирус, встроенный в систему. Его вполне достаточно для стандартной защиты системы от стандартных угроз. В большинстве случаев покупка или использование бесплатных антивирусов не имеет смысла, к тому же ни один из них не будет так глубоко интегрирован в систему, как встроенный в неё Защитник.

ШАГ 4 Проверка настроек приватности

Windows 10 качественно защищает нашу приватность. Вы можете узнать, какие приложения получали доступ к вашей камере и микрофону. Вы легко можете узнать, если какая-то программа или незамеченный вирус следит за вами. Для этого зайдите в Настройки > Конфиденциальность и в левом меню выберите «Микрофон» или «Камера». Вы увидите приложения из магазина Windows, которым разрешен и запрещен доступ к камере и микрофону. Чуть ниже вы увидите список всех приложений (в том числе и не из магазина), которые получали доступ к камере или микрофону. Если вы заметите там что-то лишнее – это повод обратиться за консультацией к специалисту по кибербезопасности. Возможно, кто-то подслушивал или подсматривал за вами.

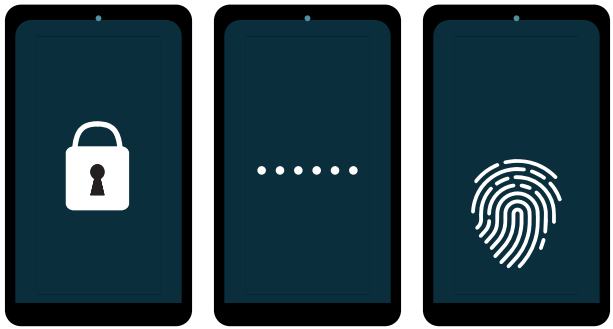
Отдельно важно знать о веб-камере. Если на вашем ноутбуке есть индикатор работы камеры, и он исправен (горит, когда камера работает) – вы можете быть уверены, что за вами никто не подсматривает. Сейчас невозможно получить доступ к камере ноутбука и программно отключить индикатор работы. Он гарантировано будет гореть, когда камера будет работать, если только полностью не выйдет из строя.

ЗАЩИТА СМАРТФОНА

ШАГ 1 Установка пароля или ПИН-кода на вход

Не используйте графический ключ для входа в систему, так как этот способ входа самый небезопасный. Его можно подсмотреть, угадать, восстановить по следам на экране. Большинство людей используют один из 20–30 стандартных паттернов рисунков, которые легко подобрать. Используйте пароль или ПИН-код.

Вы также можете использовать отпечатки пальцев для входа. Но не рекомендую использовать вход по лицу, так как в некоторых смартфонах можно использовать ваше фото для обхода этой защиты.



ШАГ 2 Проверка настроек приватности

В настройках вашего смартфона есть пункт «Защита приватности» или аналогичный, в зависимости от системы. В нем вы можете увидеть, какие программы имеют доступ к вашей камере, микрофону, геолокации. В некоторых версиях Android вы также можете увидеть, когда в последний раз приложение получало доступ.

Если вы видите в списке приложения, которых там быть не должно – удалите их, а также обратитесь за консультацией к специалисту.

ШАГ 3 Программное обеспечение – только из официальных источников

Всегда устанавливайте программы только из официальных магазинов приложений, таких как Play Market, App Gallery, Galaxy Store, F-Droid. Никогда не пытайтесь найти нужное вам приложение в гугле «скачать *приложение* бесплатно apk», ведь в таком случае вы почти гарантированно заразите свой смартфон вредоносной программой.

Вредоносной программой, но не вирусом. Дело в том, что вирусов в том же смысле, что и на ПК, на смартфонах почти нет. Вместо этого вы можете установить вредоносную программу, которая при установке потребует доступ ко всему, к чему сможет дотянуться – к файлам, камере, микрофону, звонкам, контактам. Так вредоносные программы могут шпионить за вами, подсовывать вам свою рекламу.

Устанавливая ПО только из надежных источников, вы с большой вероятностью обезопасите себя.

ШАГ 4 Экстренный сброс смартфона с полной очисткой

Иногда бывает необходимость срочно сбросить смартфон, удалив все данные на нем. Вы можете воспользоваться для этого программой Locker, которую нужно установить из магазина приложений F-Droid.

Программа потребует права администратора устройства – дайте их ей, ведь только так она сможет произвести полный сброс. Сброс произойдет при неверном введении ПИН-кода несколько раз (количество задается в настройках). Вы также можете выключить или отключить уведомление о том, что при неверном вводе кода телефон будет сброшен.

ЗАЩИТА ДАННЫХ

ШАГ 1 Защита от утери

Для того, чтобы не потерять доступ к своим данным, нужно регулярно делать резервную копию всей важной для вас информации.

Вы можете просто регулярно, например раз в неделю, делать копию важных файлов на внешний носитель. Вы можете использовать флешку, внешний жесткий диск или облачное хранилище. В любом случае главное – регулярность.

На ноутбуке или компьютере вы можете использовать специальные приложения, позволяющие создать облачную папку прямо на вашем диске. В таком случае всё, что вам будет нужно – это сохранять абсолютно все важные файлы внутри этой облачной папки. Такая папка сохраняется на вашем компьютере, все файлы будут доступны без интернета, но в то же время она всегда синхронизируется с облаком, делая резервную копию всех файлов автоматически.

Лучшим решением в этой сфере будет OneDrive, встроенный в Windows. Вы можете использовать 5 бесплатных гигабайт или купить 1000 гигабайт в облаке за 6 долларов в месяц. OneDrive позволяет не только создать облачную папку на вашем диске, но и автоматически синхронизировать папки «Документы», «Рабочий стол» и «Картинки».

Вы также можете использовать любой другой облачный сервис, начиная с Google Drive и заканчивая собственной копией OwnCloud, запущенной на вашем персональном сервере (либо на сервере организации).

ШАГ 2 Защита от кражи и компрометации

Для защиты информации от кражи, стоит позаботиться о безопасности устройств, на которых информация хранится.

Если вы храните информацию на ноутбуке – защитите свой ноутбук, установите пароль на вход и включите шифрование диска BitLocker.

Если информация в облаке – защитите свой облачный аккаунт, используйте надежный пароль, настройте двухфакторную аутентификацию.

Если информация на флешке – зашифруйте флешку или саму информацию! Вы можете использовать BitLocker (в таком случае флешку можно будет использовать только с компьютерами на ОС Windows). Вы также можете использовать специальную программу для шифрования флешки или некоторых файлов – VeraCrypt. В таком случае вы сможете получить доступ к вашим файлам на любом устройстве, на котором установлена эта программа.

Важно помнить о том, что если вы шифруете файлы, то и их резервные копии должны быть зашифрованы. В то же время вам не обязательно шифровать файлы перед сохранением их копии в облако, вам достаточно защитить свой облачный аккаунт.

ШАГ 3 Восстановление данных

Не все данные можно восстановить. Иногда данные теряются навсегда.

Вы можете восстановить любые данные, которые были сохранены в облачных хранилищах Microsoft OneDrive и Google Drive. Вы можете восстановить даже файлы, удаленный из корзины (на это в зависимости от сервиса у вас будет от 14 до 120 дней).

Если вы используете для хранения данных HDD диски – вы, вероятно, можете восстановить недавно удаленные данные с них. Однако вы не сможете восстановить никакие данные с SSD диска, который, вероятно, установлен в вашем ноутбуке или компьютере.

Только резервная копия всех важных для вас данных может спасти вас.

Всегда сохраняйте все важные файлы минимум в 2 разных местах, но не забывайте защитить каждое из них.

ЗАЩИТА ТАЙНЫ ПЕРЕПИСКИ

ШАГ 1 Электронная почта

Большинство из вас использует один из самых популярных почтовых сервисов – Google Mail. Некоторые из вас используют другие сервисы (Yahoo, Hotmail, etc.). Давайте поймем кто и что может знать о наших письмах.

Все стандартные сервисы электронной почты шифруют соединение с вашим браузером либо с почтовым клиентом. Это значит, что все письма, которые вы отправляете и получаете, могут видеть только вы, ваш собеседник и сам почтовый сервис. Посторонние могут получить доступ к вашей переписке двумя способами: взломав ваш аккаунт либо получив юридический ордер на просмотр вашей переписки, который будет обязан выполнить ваш почтовый оператор. Вы уже знаете, как защитить свой аккаунт, но как защитить переписку от почтового сервиса?

Существует 2 пути для защиты. Шифрование почты на стороне «клиента» или использование зашифрованной почты.

Первый способ трудоемкий и кратко процесс общения с собеседником выглядит так:

1. Вы и ваш собеседник генерируете себе связки ключей: публичный и приватный. Вы можете воспользоваться браузерным расширением Mailvelope или вы можете сгенерировать ключи в почтовом клиенте Mozilla Thunderbird. mail client.
2. Вы с собеседником обмениваетесь своими ПУБЛИЧНЫМИ ключами и импортируете их в свои почтовые клиенты (либо в браузерное расширение Mailvelope)
3. При создании письма вы включаете режим шифрования
4. Вы обмениваетесь зашифрованными письмами

В таком случае если вы зайдете в свой почтовый аккаунт на любом другом устройстве, зашифрованная переписка будет выглядеть как бессмысленный набор текста либо как обмен текстовыми файлами с бессмысленным набором текста в них. Ни вы (без вашего ключа), ни почтовый сервис, ни кто-либо другой не сможет прочитать вашу переписку. Однако в открытом видео станутся некоторые данные, такие как адреса отправителя и получателя, какая-то сервисная информация.

В качестве альтернативы вы можете использовать любой сервис безопасной почты, например Protonmail.

Подобные сервисы делают всю роботу по шифрованию «под капотом», что облегчает вам жизнь. Однако важно помнить, что взломав ваш аккаунт на подобном сервисе, злоумышленник сможет увидеть всю переписку, в отличии от первого варианта, при котором злоумышленник увидит бессмысленный набор символов.

ШАГ 2 Мессенджеры

Рассмотрим 3 популярных мессенджера: Telegram, WhatsApp, Signal.

Signal – один из самых защищенных мессенджеров в мире, однако он также один из самых неудобных мессенджеров. В нем вы найдете базовый функционал, переписки, звонки, стикеры и смайлы. Вы можете настраивать автоматическое удаление сообщений.

WhatsApp – технически аналог Signal, ведь у них один и тот же алгоритм шифрования. В обоих мессенджерах ваша переписка – это ваша ответственность, она хранится на ваших устройствах, но WhatsApp позволяет вам делать резервные копии.

Telegram – куда более удобный мессенджер, однако может ли он быть таким же безопасным?

Вы можете использовать секретные чаты в Telegram, они по сути совпадают с обычными чатами в Signal и WhatsApp. Они хранятся только на ваших устройствах (на одном конкретном устройстве, с которого чат был начат), и к ним нельзя получить доступ даже взломав аккаунт.

Возможностей этих трех мессенджеров хватит вам для того, чтобы быть в безопасности, а ваши переписки оставались конфиденциальными. Но важно понимать, что мессенджеры не предлагают вам анонимность – все они связывают ваш профиль с вашим номером телефона.

Существуют мессенджеры, не требующие ваш номер телефона, однако количество людей, использующих их крайне мало, и вряд ли вам удастся перевести на них всех людей из своего круга общения.

Каждый из этих мессенджеров можно защитить. Вы можете включить пин-код для входа в мессенджер на конкретном устройстве либо вы можете включить двухфакторную аутентификацию – дополнительный пароль, без которого зайти в ваш аккаунт не удастся даже имея вашу сим-карту.

ПРОГРАММЫ

ШАГ 1 Программы для смартфона

Для поиска программ на смартфон используйте встроенный в систему магазин приложений (App Store, Play Market, App Gallery, Galaxy Store, etc.)

Вы также можете использовать магазин свободного ПО F-Droid для Android.

ШАГ 2 Программы для ноутбука и компьютера

Для начала воспользуйтесь встроенным в систему магазином приложений (Windows Store, Mac app store), возможно нужная вам программа есть там.

Если нужной программы нет в стандартном магазине приложений – посетите официальный сайт издателя программы. Чтоб найти официальный сайт, загуглите название программы без дополнительных слов (например «скачать бесплатно»). Вероятно, одним из первых результатов и будет официальный сайт. Если вы не уверены – найдите нужную вам программу в Википедии, на странице с информацией о программе будет ссылка на официальный сайт издателя.

Если программа платная – чаще всего вы можете загрузить ознакомительную пробную версию з ограниченным функционалом, либо версию с полным функционалом, но доступную ограниченный срок.

Не загружайте программы из непроверенных источников, так как такие программы могут иметь скрытый вредоносный функционал, они также могут заразить вашу систему вирусами.

ШАГ 3 Установка программ

Будьте внимательны при установке программ. Всегда выбирайте «подробный» режим установки там, где это возможно. Во время установки внимательно читайте всю информацию на каждом шаге. Очень часто на некоторых шагах вы встретите автоматически поставленные галочки согласия с установкой дополнительного, мусорного ПО. Всегда отключайте такие галочки, не соглашайтесь на установку всякого хлама в систему. С помощью таких грязных трюков в вашу систему может попасть нежелательное ПО, всякие рекламные баннеры, лишние браузеры или дополнения к ним. Чаще всего среди этого хлама не будет вирусов, но сами по себе эти дополнительные программы – мусор, который захламляет систему, мешает вам эффективно использовать ваш компьютер.

ШАГ 4 Обновление программного обеспечения

Для поддержания высокого уровня безопасности системы стоит всегда обновлять систему, программы, драйверы до последней актуальной версии. Регулярно в программах или операционных системах находят дыры в безопасности. Издатель

ПО вносит необходимые исправления, как только ему становится известно о дыре. Все исправления поступают к вам в виде обновлений. Иногда обновления добавляют функционал, иногда исправляют ошибки, но иногда закрывают дыры в безопасности. Всегда используйте последнюю актуальную версию системы, ПО и драйверов, чтоб максимально снизить риски использования уязвимостей в программной и аппаратнйо части вашего устройства.

БЕЗОПАСНЫЙ ИНТЕРНЕТ

ШАГ 1 Используйте доверенные сети

Доверенными вы можете считать сети, которые настраивали сами, или которые настраивались для вас. Ваши домашняя и рабочие сети можно считать доверенными.

ШАГ 2 HTTPS Everywhere.

При серфинге в интернете убедитесь, что все сайты, с которыми вы взаимодействуете, поддерживают протокол связи HTTPS. Для этого обратите внимание на адресную строку. Возле адреса сайта должен стоять замочек. Этот замочек означает, что между вами и сайтом установлено зашифрованное соединение, никто кроме вас и сервера не сможет узнать, что конкретно вы делаете на сайте, какие данные передаете или качаете.

Вы можете установить в свой браузер расширение HTTPS Everywhere, оно предупредит вас о том, что какой-то сайт не использует HTTPS протокол и такой сайт нельзя назвать безопасным.

Важно понимать, что «замочек» на сайте не означает автоматически, что сайт хороший и безопасный. Замочек означает только лишь то, что между вами и сайтом установлено безопасное защищенное соединение.

ШАГ 3 VPN

VPN – виртуальная приватная сеть. Используя VPN – вы создаете защищенный зашифрованный туннель между вами и VPN сервисом. Никто на пути от вас до сервера VPN не сможет не только перехватить ваш трафик, но и узнать, куда вы направляетесь. VPN скрывает от посторонних глаз пункт вашего назначения – сайт или сервер приложения, на которое вы заходите. Он также скрывает ото всех всё, что вы передаете внутри туннеля: сообщения, данные, файлы.

Вы можете использовать VPN находясь в неизвестных сетях, например в отеле, в ресторане или на городской площади. Ваш трафик, передаваемый через VPN, не получится ни перехватить, ни расшифровать.

Однако важно понимать, от чего не спасет VPN. Он не спасет вас от угроз на стороне вашего устройства (вирусы, вредоносные программы), не спасет он и от угроз на стороне сайта, на который вы заходите. Некоторые сайты могут быть уязвимы к взлому и через них можно попытаться взломать вас. VPN не спасет вас от этого, тут поможет антивирус.

ШАГ 4 Выбирайте сайты, которые посещаете

Большинство всем известных сайтов и веб порталов с миллионами посещений в день безопасны для вас. Угрозы могут таиться на малоизвестных сайтах, которые вы можете найти случайно.

Например, вам нужно скачать электронную книгу. Вы гуглите эту книгу по названию и попадаете на сайт, который впервые видите. Будьте внимательны, ведь такой сайт может угрожать вашей безопасности.

На таком сайте могут быть вирусы. С ними справится ваш антивирус, так что не стоит сильно беспокоиться.

Часто самая большая красивая зеленая кнопка «Скачать» загрузит на ваш компьютер какой-то мусор. Ненужную программу, основной функционал которой – показывать вам рекламу. Такие программы могут обходить антивирус, так как они не являются вирусами. Внимательно смотрите на расширение файла, который загружаете. Если вы собирались скачать электронную книгу, а загрузился файл *.exe – вероятно это не книга, а вредоносная программа.

ПОСЛЕСЛОВИЕ

Цифровая безопасность – это не установка антивируса. Это постоянный и длительный процесс. Процесс, переходящий в привычку. Безусловно, можно прямо сейчас проверить все ваши устройства и аккаунты, убедиться, что они в безопасности, зашифровать всю важную информацию и сделать резервные копии. Но если сделать это один раз – результат вас не обрадует. Ложное чувство безопасности, созданное во время защиты, может повлечь беспечность и открыть брешь в системе вашей безопасности. Вы можете думать «У меня все настроено» и перестать следить за своими действиями, ведь вы уже в безопасности. Именно тогда вас можно атаковать, и именно тогда вы наиболее уязвимы.

Безопасность – это процесс, который нельзя прерывать. Вы должны взращивать в себе привычки безопасного поведения, например всегда закрывать крышку ноутбука, когда отходите от него, или всегда смотреть на адресную строку, когда заходите на какой-то, даже привычный, сайт.

Абсолютной безопасности не существует. Борьба добра со злом, хакеров со специалистами по кибербезопасности, будет продолжаться вечно. Новые угрозы, как и новые решения, появляются постоянно. Держите руку на пульсе ситуации, и будьте на шаг впереди! Только так можно контролировать состояние своей цифровой безопасности.

Автор: Генри Демьянович, hnrdem@gmail.com, Telegram: @hnrdem


SWAN
SEX WORKERS' RIGHTS
ADVOCACY NETWORK