Простые шаги для обеспечения безопасности

Сегодня, когда многие, если не большинство из нас, вынуждены сидеть и работать из дома, огромное значение приобретают знания простейших методов обеспечения информационной безопасности. Несмотря на наличие надежных технологий, самым слабым звеном в обеспечении безопасности остается человек. Давайте ответим себе на следующие вопросы:

1. Вы используете надежные пароли? Всегда? И всегда разные?
2. Все члены вашей семьи (включая детей) используют для работы (игр) на компьютере свои собственные учетные записи? С минимальными правами? И при этом используете надежные пароли?
3. Вы давно меняли пароли? Все? И к Wi-Fi?
4. Вы используете лицензионное ПО? Вовремя его обновляете? Все? Не только ПО от Microsoft?
5. Вы используете лицензионный антивирус? Как часто вы проверяете ваш ПК? Смартфон?
6. Вы используете QR-код? А при этом вы его проверяете?
7. Как давно вы обновляли ваш смартфон? А приложения?
8. Вы давно проверяли права ваших приложений на смартфоне? Знаете ли вы о том, какие права требуют ваши приложения? Проверяли?
9. Вы используете VPN? Особенно при соединении через бесплатный Wi-Fi?

Я могу задавать много подобных вопросов. Но в данной статье просто постараюсь рассказать почему это необходимо. Специалисты ИТ просто усмехнутся, мол, что тут рассказывать, все ж очевидно. Верно, очевидно. Но задумайтесь, а вы сами выполняете эти правила? А ваши близкие? Жены, дети, родители? Вы с ними говорили об этом? Как давно? Точно?

На самом деле хочу, чтобы вы понимали. Хороший, даже блестящий инженер и хороший преподаватель, рассказывающий сложные вещи простым языком – это совершенно разные люди. Более того, хороших рассказчиков, увы, не просто мало, а очень мало. В данной статье я постараюсь простым языком рассказать о сложном. Получится или нет? Я не знаю. Попробую.

Прежде всего хочу, чтобы вы понимали. Даже самая лучшая технология не сможет вас защитить сама по себе. Байки о волшебных средствах из коробки – это не более чем рассказы специалистов по рекламе. К любой технологии должен прикладываться специалист, который умеет настроить то или иное аппаратное (программное) средство. Иначе это просто бесполезное вложение денег! Давно известно, что проще всего атаковать вас, а не ваш компьютер (смартфон). Живой пример. Сколько на сегодня зараженных смартфонов (планшетов) под Android, а ведь самораспространяющихся вирусов в обычном понимании под эту ОС не существует. За каждым заражением стоит пользователь, который это установил. Его кто-то заставлял? Нет конечно. Вспомните нашумевшую игру Angry Birds. Славная игрушка, верно? А кто задумывался что эта игра 1200 раз в неделю передавала данные о вашем местоположении? Или приложение «Фонарик», которому нужны данные о вашем местоположении? И никто не задумывается зачем??? Просто соглашаются. А спроси, ценят ли свою приватность, все побегут кричать «Да!». Неужели?

Вы используете надежные пароли? Всегда? И всегда разные?

Извините, но не верю. Большинство пользователей либо используют простые пароли, вспомним, к числу самых популярных паролей до сих пор относится «1234567» или имя пользователя. Увы, пользователи ленятся запоминать длинные и сложные пароли. Уже почти 10 лет Google

использует двухфакторную аутентификацию. И что? Сейчас, по данным Google, данную технологию использует не более 10% пользователей.

Почему люди продолжают использовать простые пароли?

Чаще всего пользователи считают, что вряд ли смогут противостоять кибермошенникам, ведь они компьютерные гении.

Но самое главное, то, что более половины пользователей использует один и тот же пароль для нескольких сервисов. К чему это приводит? Взламывается одна учетная запись и в результате под угрозой все ваши учетные записи. Вы к этому готовы?

Запомните несколько правил:

1. Один сервис – один пароль. Пароли не должны повторяться!
2. Никому и никогда не сообщайте свои пароли.
3. Храните пароль так, чтобы его не могли увидеть посторонние.
4. При первом подозрении, что ваш пароль стал известен посторонним, срочно смените его и сообщите об этом ответственному за безопасность в вашей компании.
5. Всегда используйте только сложные уникальные пароли.
6. Если вы подозреваете, что ваш аккаунт пытаются взломать, немедленно смените пароль от почты.
7. Пароль от электронной почты можно вводить:
   7.1. на сайте почтового сервиса;
   7.2. в мобильном приложении почтового сервиса;
   7.3. в почтовой программе для десктопа;
   7.4. И больше — нигде.
8. Используйте менеджер паролей
9. Резервное копирование и восстановление

Как видите, ничего особо сложного. Список этих правил рекомендую распечатать и использовать всегда и везде.

Все члены вашей семьи (включая детей) используют для работы (игр) на компьютере свои собственные учетные записи?

Чаще всего на домашних компьютерах все работают и играют под одной и той же учетной записью, да еще и с правами администратора. К чему это может привести? Как минимум к тому, что в случае заражения зловред тоже получит права администратора. А если ваш ребенок (или вы сами) случайно удалите проект, над которым работала ваша жена (или вы сами), то, боюсь, скандал в семье неминуем. А ведь это вполне реально. Либо ваш ребенок принесет домой (загрузит из Интернета) зараженную игру. Вы к этому готовы? Боюсь нет! Так что лучше подумать заранее.

Вы давно меняли пароли? Все? И к Wi-Fi?

Задумайтесь, вы регулярно меняете пароли? На самом деле есть одно негласное правило. Чем проще пароль вы используете, тем чаще вы должны его менять. Как часто? Я не знаю. Я меняю пароли дома раз в два месяца. Естественно, на работе это необходимо делать чаще. Пароль к Wi-Fi необходимо так же регулярно менять. Поверьте, ваши усилия оправдаются.

Вы используете лицензионное ПО? Вовремя его обновляете? Все? Не только ПО от Microsoft?

О необходимости использования лицензионного ПО написано огромное количество статей. И тем не менее, люди упорно предпочитают халяву. Вы задумывались, взломали операционную систему, которую вам устанавливали только ради вас? Из благотворительности? Неужели? Взломщик ведь при этом преследовал свои цели. И делал это не из благотворительности, верно? Его труд должен быть оплачен. Вы платите? Нет. Значит в вашу операционную систему вполне может быть встроен троян для сбора информации, верно? Вы думаете, ваша информация ничего не стоит? Вы не правы.

А вспомните, как давно вы обновляли ваш приложения? Многие пользователи боятся обновлений. Особенно операционной системы или Office. Боятся прежде всего потому что эти приложения не лицензионны и могут просто перестать работать. Результат предсказуем. Компьютер просто оказывается взломанным. Но если программное обеспечение от Microsoft еще чаще всего обновляется, то стороннее ПО не обновляется совсем. Как быть?

Проще всего периодически посещать сайты производителей вашего программного обеспечения. Однако есть еще более простой способ.

Если вы используете антивирусное программное обеспечение от Kaspersky, например, Kaspersky Security Cloud, то вы можете воспользоваться опцией «Обновление программ». Фактически это ПО будет периодически сканировать ваш компьютер и предлагать вам обновить то или иное ваше программное обеспечение. Вместе с тем стоит помнить, что некоторые программы сами указывают что есть обновление и вам просто нужно его установить.

Вы используете лицензионный антивирус? Как часто вы проверяете ваш ПК? Смартфон?

Смешные вопросы? Ну зачем платить за антивирус, если есть бесплатная версия. Все верно. Есть. Только вопрос. Если вы не покупаете, а используете бесплатную, то чем вы расплачиваетесь? Ну не верю я в благородство и желание помочь. Может быть я не прав, но что-то никогда я в магазине не видел не то, что бесплатного мяса, но даже бесплатного хлеба. А чем программисты хуже? Ведь тоже кушать хотят и причем каждый день.

Вспомните историю с бесплатным антивирусом AVG. Помните? Когда разработчики заявили, что собирают и продают ваши личные данные, чтобы ваш антивирус был бесплатным. И как? Нравится? Мне – нет! А смартфон вы проверяете? Часто? Задумайтесь!

Вы используете QR-код? А при этом вы его проверяете?

Сегодня все чаще многие пользователи используют QR-код. Однако понимают ли пользователи, что использование такой технологии несет в себе огромный риск. Ведь на совсем небольшом экране смартфона вы не видите адресную строку, куда именно вы перешли. В связи с этим я бы рекомендовал использовать QR-сканер, который проверяет вашу ссылку до того, как вы по ней перейдете. Если вы спросите, какой сканер использую я, мне легко ответить – QR-scanner от Kaspersky. Это ПО бесплатное и существуют версии как для iOS, так и для Android.

Как давно вы обновляли ваш смартфон? А приложения?

Проблема обновления смартфона, увы, с каждым днем становится все острее. И если для iPhone это менее острая проблема, сегодня обновляются версии, начиная с iPhone 6 до последних выпусков, то с Android все куда сложнее. Увы, стоит признать, что максимальное время жизни

смартфона под управлением ОС Android – два года. Причем не с момента покупки вашего смартфона, а с момента выхода вашей версии ОС. Увы, стоит признать, что смартфонов под управлением последней и предпоследней версии ОС в марте 2020 на рынке Российской Федерации всего 48% (по данным [1]).

Вы давно проверяли права ваших приложений на смартфоне? Знаете ли вы о том, какие права требуют ваши приложения? Проверяли?

Увы, права приложений, чаще всего никто не проверяет. Информацию о вас так или иначе собирают практически все мобильные (впрочем, не только мобильные) операционные системы, это известно давно. С не меньшим успехом информацию о вас собирают мобильные приложения. «Удалённые» пользователем записи истории браузера Safari на самом деле не исчезают из «облака», а остаются в iCloud в течение длительного времени. Данные журнала этого же браузера синхронизируются регулярно и не зависят от настроек резервных копий, что позволяет вести наблюдение за тем, какие сайты посещает пользователь, с минимальной задержкой. Причем Apple оказалась единственной компанией, которая продолжает хранить на своих серверах записи из истории браузера даже после того, как пользователь их удалит.

Вспомним такое приложение как «Фонарик».

Приложения-фонарики для Android запрашивают в среднем 25 разрешений для доступа к разным функциям и данным смартфонов.:

- 408 таких приложений запрашивают до 10 разрешений
- 267 — от 11 до 49 разрешений
- 262 приложения запрашивают от 50 до 77 разрешений.
- 77 программ запросили доступ к записи звука.
- 180 приложений просили доступ к данным контактов.
- 21 приложению-фонарику был необходим доступ к возможности записывать контакты.

Всего компания Avast изучила 937 приложений. [2]

А ведь опасных прав не просто много, а очень много. К ним можно отнести:

- SMS
- Календарь
- Камера
- Контакты
- Местоположение
- Телефон
- И т.д.

Вы используете VPN? Особенно при соединении через бесплатный Wi-Fi?

Отдельно хотелось бы остановиться на использовании бесплатного Wi-Fi. Очень интересно наблюдать, как люди пользуются открытыми беспроводными сетями. Неужели вы думаете, что вас никто не слушает? Или вас некому слушать? Вы уверены? А ведь слушая, можно получить не только пароли от почты, но в некоторых случаях даже пароли от интернет-банка. Если уж вам так нужно использовать открытый Wi-Fi, используйте VPN.

Резервное копирование и восстановление

Независимо от того, насколько вы осторожны, вас, увы, все еще можно взломать. Если это так, то часто единственный способ — восстановить всю вашу личную информацию из резервной копии. Убедитесь, что вы делаете регулярные резервные копии любой важной информации и убедитесь, что вы можете восстановить свои данные из них. Большинство операционных систем и мобильных устройств поддерживают автоматическое резервное копирование либо на внешних дисках, либо в облаке.

Заключение

Безусловно, это далеко не все что вы должны сделать. Но с чего-то ведь нужно начинать, верно?

Литература

1. http://gs.statcounter.com/
2. https://tech.informator.ua/2019/09/10/prilozheniya-fonariki-dlya-android-ulichili-v-nezakonnom-sbore-lichnyh-dannyh/