Безопасный и полезный интернет для продвинутых пользователей

Вы с компьютером – на ты? Вам не надо объяснять, зачем нужен антивирус, и как поступать со спамом? Тогда эти рекомендации помогут сделать интернет еще безопаснее и приятнее.

Смотрите, где вы выходите в интернет

Публичные сети могут являться приманкой для сбора паролей и других персональных данных. Доступ в интернет через подставные публичные сети закончится крупными потерями для пользователя. По возможности, избегайте подключаться к значимым для вас ресурсам через публичные сети. Если все же вы решили подключиться, то используйте vpn-подключение.

Пообщавшись в сети ВКонтакте через публичную сеть, обязательно воспользуйтесь кнопкой «Завершить все сеансы» (вы найдете ее во вкладке «Безопасность блока «Мои настройки»). Это помешает посторонним прочитать вашу переписку или перехватить аккаунт.

Защитите ваш домашний wifi-роутер

Взламывая простые пароли, злоумышленники могут получить доступ к управлению вашим домашним wifi-роутером. Это позволит им незаметно перенаправлять запросы всех устройств, которыми вы пользуетесь дома, таким образом, получив доступ к вашим аккаунтам.

Своевременно обновляйте системное программное обеспечение вашего домашнего wifi-роутера. А также убедитесь, что администраторский веб-интерфейс защищён надёжным паролем и недоступен для внешних пользователей. Не следует держать свою домашнюю wifi-сеть открытой: установите пароль и сообщайте его только тем, кого хорошо знаете.

Смотрите, куда вы вводите пароль

Фишинг – один из самых популярных способов перехвата управления учетными записями. Суть фишинга: обманутый пользователь вводит свои логин и пароль на поддельной странице авторизации в социальной сети, почте или онлайн-банке. Используйте браузеры с встроенной защитой от фишинга или установите в свой браузер соответствующий плагин. Но самое главное, внимательно изучайте страницу авторизации, каждый раз, когда вводите пароль, независимо от типа используемого браузера. Обращайте внимание на адрес страницы, ее оформление и текст. «Кривой» адрес, нестандартное оформление, ошибки в орфографии и пунктуации могут свидетельствовать о попытке обмануть вас. Также убедитесь в том, что страница авторизации использует безопасный протокол — HTTPS, а в адресной строке отсутствуют предупреждения об ошибках.

Включите двухфакторную авторизацию

Большинство популярных сервисов позволяют для входа в учетную запись использовать дополнительную защиту (второй фактор), например, одноразовый пароль (пин-код), который присылается на телефон пользователя. Дополнительный фактор защиты от злоумышленников даже в том в случае, если у них оказались ваши логин и пароль.

Включить двухфакторную авторизацию в сети ВКонтакте можно во вкладке «Безопасность» блока «Мои настройки».

Используйте сложные пароли

Ваши учетные записи в почте и социальной сети находятся под постоянной атакой злоумышленников. Всегда используйте сложные пароли, вне зависимости от того, применяете ли вы двухфакторную авторизацию. Простые пароли легко запомнить, но их и легко взломать.

Будьте осторожны в создании вопросов по восстановлению паролей

Не следует использовать одинаковые вопросы для восстановления паролей к разным аккаунтам. Также не рекомендуется использовать такие привычные вопросы, как имя матери, первая школа, имя питомца и т.д. Всю эту информацию обычно можно легко получить из тех же социальных сетей.

Обращайте внимание на HTTPS

HTTPS-протокол – это сильная защита от подслушивания и перехвата ваших данных в интернете. Внимательно следите за тем, что написано в адресной строке браузера. Строка должна начинаться с «https» и содержать изображение замка. Если при работе с ресурсом «https» вдруг меняется на «http», либо браузер предупреждает о проблемах с сертификатом безопасности, то покиньте этот сайт! Ни в коем случае не вводите пароль и не указывайте никаких персональных данных!

HTTPS – популярный инструмент защиты. Но помните, что у него тоже есть свои уязвимости, которыми пользуются злоумышленники. Учитывайте это при совершении важных действий.

Включить HTTPS в сети ВКонтакте можно во вкладке «Безопасность» блока «Мои настройки», но она скрытая. Чтобы эта опция появилась нужно, находясь в авторизованном режиме, вручную перейти на защищенное соединение. Для этого в начале адресной строки нужно вписать «https». У вас получится такая ссылка: https://vk.com/settings?act=security. Появится опция «Всегда использовать защищенное соединение (HTTPS)». И вам только останется поставить галочку.

Используйте блокировщики рекламы

Рекламные объекты на сайтах (баннеры, поп-апы и т.п.) используют Javascript и Flash для перенаправления пользователей на сторонние ресурсы. Они не поддерживают защищенное https-соединение и могут быть местом, где действуют злоумышленники. Вы уменьшите для себя бесполезный трафик и повысите безопасность, если станете использовать блокировщики рекламы. Однако тщательно проверяйте источник используемого блокировщика, не следует устанавливать первый попавшийся блокировщик и прочие «ускорители интернета». Они часто оказываются замаскированными вредоносными программами.

Не подключайте чужие USB-устройства к своему компьютеру

Как правило, USB-устройства (флэшки, внешние диски и т.п.) автоматически распознаются, а программный код, размещённый на них, запускается на компьютере. Эти устройства могут содержать вредоносные программы, которые при запуске обойдут систему защиты вашего компьютера.

Пользуйтесь облачными хранилищами для хранения и передачи файлов, например, Dropbox. А если, все же, используете флэшку, то предварительно проверяйте ее на вирусы. Убедитесь, что флэшка получена от надёжного человека.

Также лучше отключить на своем компьютере автозапуск приложений и медиаконтента. Нужная настройка в Windows расположена по адресу “Панель управления\Оборудование и звук\Автозапуск".

Следите за своими флешками

Разделяйте работу и отдых. Сегодня ёмкие флешки стоят сущие копейки. Используйте разные накопители для дома и школы (офиса). Обменивайтесь файлами с друзьями при помощи одной флешки, а на рабочих компьютерах пользуйтесь другой.

Для защиты от вирусов, а также просто для защиты личных данных, всегда удаляйте с флешки все файлы, после того как скопировали их на компьютер. Можно даже ее отформатировать, это избавит от лишних размышлений о том, какие данные там хранятся, и не заражена ли она вирусами.

Делайте резервное копирование

Бывает, что жесткий диск выходит из строя. Данные могут повреждаться из-за пользовательских ошибок или вирусов. Вероятно, вы знаете, что такое «Ransomware». Это когда вредоносная программа-шифровальщик шифрует пользовательские файлы, а затем злоумышленник вымогает деньги за расшифровку. Помните, что негодяи, которые создают шифровальщики, зарабатывают на том, что ваши файлы существуют только в одном экземпляре. Чтобы сохранить свои данные, регулярно делайте бэкап.

Три коротких примечания о бэкапах:

- Храните хотя бы один бэкап в офлайне и не дома, например на переносном диске у родственников.
- Храните бэкапы в зашифрованном виде, чтобы только вы могли воспользоваться своим бэкапом.
- Есть лишь один бэкап, о котором вы пожалеете. Это тот бэкап, который вы вовремя не сделали.

Одно длинное примечание о шифровальщиках:

Если вы стали жертвой шифровальщика, ни в коем случае не платите выкуп. Файлы вам, скорее всего, не расшифруют, но вы точно воодушевите преступников на продолжение их деятельности. У вас есть шанс восстановить файлы, использовав специальную бесплатную утилиту Лаборатории Касперского Ransomware Decryptor. Также вы можете использовать утилиту Kaspersky WindowsUnlocker. Утилита запускается при загрузке компьютера со специальной программой Kaspersky Rescue Disk.

Если вы пользуетесь Kaspersky Internet Security, то убедитесь в том, что включен компонент System Watcher. Он создает и защищает локальные копии важных файлов так, что шифровальщики не могут получить к ним доступ.

Разлогинивайтесь, когда вы не пользуйтесь ресурсом

Если вы залогинены на каком-либо сайте, но не пользуетесь им, то вы оказываетесь уязвимыми к атакам типа «Межсайтовая подделка запросов» (Cross-

Site Request Forgery или CSRF). При этих атаках злоумышленники от лица пользователя меняют пароли, перечисляют средства или совершают иные вредоносные действия по своему выбору.

Заведите привычку разлогиниваться из любых ресурсов, которыми вы не собираетесь пользоваться в ближайшее время. Эта привычка сэкономит ваши деньги и нервы.

Выключайте компьютер, когда вы им не пользуетесь

Пока ваш компьютер включен, злоумышленник может спокойно предпринимать попытки получить доступ к вашим данным, даже если у вас настроена полнодисковая шифрация. Обесточенный компьютер – лучшая защита.