Теплица социальных технологий

Что такое цифровая безопасность: термины и технологии

Наталья Баранова

https://te-st.org/2018/05/25/digital-security-terms/

Статья обновлена 18 января 2022

В этом материале мы расскажем, что такое цифровая безопасность, какие термины нужно знать, чтобы разбираться в этой теме. Также дадим рекомендации по базовой и дополнительной безопасности, которые помогут защитить данные на ваших устройствах и в Интернете.

Цифровая безопасность – это комплекс мер, направленных на защиту конфиденциальности, целостности и доступности информации от вирусных атак и несанкционированного вмешательства.

Сегодня у многих организаций крайне развитая IT-инфраструктура. Поэтому шансы, что хотя бы один компьютер может заразить всю сеть, увеличиваются. В этом случае каждому сотруднику важно соблюдать цифровую безопасность. Иначе репутация всей организации может оказаться под угрозой. Стоит помнить, что любое устройство, как служебное, так и личное, может стать каналом атаки и угрозой.

Теплица рекомендует регулярно делать аудит безопасности и повышать личную компьютерную грамотность.

Категории защиты

1. Базовая безопасность. Это первостепенные действия по защите компьютера.

- Установка лицензионных операционных систем и программного обеспечения. Нелицензионная ОС может содержать вредоносные закладки, а также не позволять делать обновление. Если вы не хотите покупать OS, можно воспользоваться бесплатными аналогами на базе Linux: Ubuntu, Linux Mint, Fedora.
- Регулярное обновление операционной системы. Обновления зачастую содержат исправление брешей в безопасности.
- Установка антивируса для пользователей Windows. Антивирус снизит риск заражения компьютера широко распространенными вредоносными программами. Пользователям MacOS или Linux антивирус не требуется.
- Синхронизация локальных папок с Облаком. Оперативный бэкап в «облако» наиболее критичных для работы файлов (архив ключей доступа, приватные ключи PGP). Если есть оперативный бэкап, то в случае необходимости можно сразу продолжить работу без необходимости полного восстановления из бэкапа. Не рекомендуем использовать российские облачные хранилища, например, Яндекс.диск.
- Полнодисковое шифрование. Рекомендуем воспользоваться: FileVault для Mac OS X, BitLocker или VeraCrypt для Windows.
- Создание резервной копии диска.

2. Цифровая гигиена. В эту категорию входят действия не обязательные, но крайне желательные.

- Двухфакторная авторизация для почты и социальных сетей.
- Использование PGP.
- Использование сложных и разнообразных паролей.
- Локальное шифрование.
- Установка пароля на вход в BIOS, или пароля EFI для macOS. Это защитит компьютер от запуска с LiveCD (ОС размещенная на USB или компакт-диске). Запустив систему с LiveCD, вы получаете доступ к жесткому диску и можете изменить загрузчик ОС на свой.
- Пароль на вход в систему, что позволит защитить вашу ОС от постороннего доступа, в то время как вы отлучились на минутку.
- Нельзя подключать к вашему устройству чужие флешки, мобильные телефоны, SD-карты, USB-устройства и прочие носители информации. Также стоит отключить автозапуск для внешних устройств. На внешних носителях и устройствах может быть вредоносное ПО, которое самопроизвольно запустится на вашем компьютере.
- Не следует давать свой компьютер посторонним (пусть даже доверенным лицам) или детям. Они могут установить нежелательное ПО. Если необходимо это сделать, то лучше создать гостевой аккаунт без права установки новых программ и дать им туда доступ.
- Если ваше устройство было скомпрометировано (изъято спецслужбами в ходе обыска или досмотра на таможне или украдено и затем найдено), то использовать такое устройство после его возврата уже небезопасно. Есть вероятность, что на устройство могли установить шпионскую программу или чип.
- Не устанавливайте потенциально вредоносное ПО: для подбора ключей к программам (keygen) или иное ПО для взлома официальных программ. Зачастую такое ПО является «приманкой» для внедрения вредоносных программ.
- На мобильных телефонах не рекомендуется устанавливать программы из неофициальных магазинов приложений. В официальных магазинах программы проходят проверку безопасности.

Дополнительная безопасность

- **Закройте видеокамеру ноутбука.** Применяя вредоносное ПО, злоумышленники могут

использовать камеру и микрофон для слежки за вами. Камеру лучше заклеивать, когда вы ею не пользуетесь.
- **Создайте полную резервную копию.** Рекомендуется перед проведением операций по полнодисковому шифрованию или иным действиям с ОС, которые могут вывести ее из строя, сделать полную резервную копию (бэкап). Бэкапы должны быть зашифрованы. В случае утери или кражи компьютера бэкапы очень экономят время по восстановлению работы. Крайне рекомендуется делать распределенный бэкап и не хранить все бэкапы на одном устройстве и месте. Стоит использовать CloneZilla, DejaDupe, Time Machine или альтернативы.
- **Локальное шифрование.** В случае хранения на персональном компьютере чувствительных материалов (таких как пароли доступа, финансовые и административные материалы, а также персональные данные третьих лиц (касается, прежде всего, бухгалтерии), связанных с работой в вашей организации, эти файлы должны храниться в запароленной и зашифрованной папке. Рекомендуется использовать VeraCrypt или аналоги.

Работа в Сети

- Нельзя подключаться к открытым (то есть таким, на которые не установлен пароль) Wi-Fi сетям без использования VPN (OpenVPN, Cloak или другого). Трафик по открытым беспроводным сетям можно легко перехватить.
- Нельзя вводить пароли к ресурсам организации, если не установлено защищенное соединение по HTTPS. Убедитесь перед вводом пароля, что в начале адреса сайта указан текст https://
- Использовать сложный пароль. Все пароли, используемые сотрудником вашей организации для электронной почты, доступа к административной панели сайта, социальных сетей и т.п., должны содержать цифры, большие и малые буквы алфавита и знаки препинания. По возможности стоит также добавить специальные символы. Для хранения и генерации паролей стоит использовать менеджеры паролей.
- Не использовать один пароль везде. Используйте генератор паролей для создания и хранения уникальных паролей для каждого сайта. Общий пароль, если «утечет», может стать частью словарей паролей, которые злоумышленники используют для подбора паролей к разным сайтам.
- Не стоит вводить пароли вручную в публичных местах, где их могут подсмотреть или записать на камеру! Используйте в таких случаях менеджер паролей и вводите пароли при помощи копирования или функции автозаполнения.

Почта, онлайн-документы и мессенджеры

- Двухфакторная авторизация для почты. Не должна быть привязана к SIM-карте, необходимо привязывать к одноразовым кодам или к верификации с помощью телефона и программы Authenticator.
- Использование PGP для чувствительной переписки. В случае если вы отправляете персональную информацию о себе или третьих лицах (паспортные данные, именные билеты), пароли, пересылаете базы данных.
- Двухфакторная авторизация для социальных сетей. Также не стоит привязывать к SIM-карте.

Термины, которые стоит знать

Шифрование данных – обратимое преобразование информации в целях сокрытия от не авторизованных лиц с предоставлением в это же время авторизованным пользователям доступа к ней.

HTTPS – это зашифрованный способ передачи информации. В отличие от обычного

соединения по HTTP, ваши данные будут зашифрованы перед отправкой. Соединение по HTTPS убережет вас от подмены сайта его копией.

Полная резервная копия диска – процесс, который помогает восстановить операционную систему после атаки, со всем набором программ и настроек.

VPN (от англ. Virtual Private Network – виртуальная частная сеть) – это технология, которая позволяет проложить виртуальный кабель через Интернет в вашу удаленную сеть (сервер).

Двухфакторная идентификация – это дополнительный уровень безопасности ваших аккаунтов. Он гарантирует, что доступ к вашей учетной записи сможете получить только вы, даже если пароль известен кому-либо еще.