12 главных советов по кибербезопасности

Вот 12 простых советов по обеспечению безопасности вашей личной информации. Не забудьте поделиться этими советами со своими сотрудниками. Таким образом, вы также можете защитить свою организацию.

1. Будьте осторожны со ссылками.

Ссылки в электронных письмах – это распространенный инструмент, используемый хакерами, чтобы обманом заставить людей отказаться от своей защищенной информации. Это часто бывает в форме банковских выписок, бронирования авиабилетов, электронных писем для восстановления пароля и т. д.

Если пользователь нажимает на одну из этих ссылок, он попадает на поддельный сайт, который очень похож на своего реального аналога. Сайт попросит их войти в систему или ввести личную информацию. Как только хакер получит эту информацию, он получит доступ к учетной записи пользователя.

Так что помните о ссылках в своих письмах. Если что-то выглядит подозрительно, не нажимайте на это. Фактически, самый безопасный вариант — посетить сайт провайдера напрямую, а не использовать ссылку по электронной почте.

2. Меняйте пароли.

Хотя проще запомнить один пароль для всех ваших учетных записей, он не самый безопасный. Лучше всего менять пароль для каждого используемого сайта и учетной записи. Таким образом, если компания, которую вы используете, будет взломана, украденные учетные данные не будут работать на других сайтах. Если вам интересно, как вы могли бы запомнить все эти пароли, вы не одиноки. Но это подводит нас к третьему совету.

3. Используйте диспетчер паролей.

Менеджер паролей — это программа или программа, которая хранит все ваши пароли в одном месте. У вас есть один пароль «мастер-ключ» для разблокировки доступа к этим паролям. С менеджером паролей вам не придется беспокоиться о запоминании каждого из ваших паролей. Это также избавит вас от необходимости записывать пароли (чего никогда не следует делать!)

LastPass, KeePass, Dashlane, 1Password и Roboform – хорошие программы. Многие предлагают бесплатные версии, а некоторые совершенно бесплатны. И, если вы используете Dropbox, OneDrive, Google Drive или тому подобное, вы можете сохранить базу паролей на своем облачном диске, и она будет доступна где угодно.

4. Настройте многофакторную аутентификацию.

Без настройки многофакторной аутентификации (MFA) пользователь может получить доступ к своей учетной записи, используя только имя пользователя и пароль. Но MFA добавляет еще один уровень защиты. Для проверки личности пользователя при входе в систему требуется более одного метода аутентификации.

Один из примеров MFA – это когда пользователь входит на веб-сайт и должен ввести дополнительный одноразовый пароль. Этот одноразовый пароль обычно отправляется на адрес электронной почты или на телефон пользователя. Настройка MFA создает многоуровневую защиту, затрудняя несанкционированный доступ к вашей информации.

5. Не используйте дебетовые карты в Интернете.

Еще один важный совет по кибербезопасности касается онлайн-платежей. При совершении онлайн-платежей избегайте использования дебетовых карт. Или что-нибудь, что напрямую связано с вашим банковским счетом.

Вместо этого используйте параметры, которые обеспечивают дополнительный уровень защиты между хакерами и вашими банковскими счетами. Это может быть

кредитная карта со страховкой или какой-либо способ оплаты онлайн, например PayPal.

6. Не сохраняйте информацию о платеже.

Многие веб-сайты позволяют сохранять информацию о кредитной карте, чтобы сделать будущие покупки быстрее и проще. Не делай этого. Нарушения случаются постоянно. Красть нечего, если ваша кредитная карта не сохранена на сайте. Это может показаться проблемой, но мы обещаем, что это не так плохо, как кража вашей информации.

7. Держите свои системы в актуальном состоянии.

Ваше программное обеспечение, операционная система и браузер всегда должны быть в актуальном состоянии. Если в вашей компании используется брандмауэр, программное обеспечение и прошивка брандмауэра также должны быть обновлены. Чем старше система, тем больше времени у хакеров для поиска уязвимостей. Обновляя свои системы, вы предотвратите использование вредоносными программами или хакерами этих слабых мест в системе безопасности.

Итак, в следующий раз, когда вы увидите всплывающее окно с обновлением системы, не игнорируйте его!

8. Избегайте неизвестных сайтов.

В наш век социальных сетей легко поделиться ссылкой в Интернете. Но будьте осторожны при посещении новых сайтов. Возможно, на этих сайтах проводятся «атаки на скачивание» , которые могут угрожать вашим данным.

При атаке с использованием закачки через диск пользователю даже не нужно нажимать на что-либо, чтобы компьютер мог заразиться. Достаточно просто посетить сайт, чтобы передать вредоносный код. Итак, лучше всего придерживаться хорошо зарекомендовавших себя сайтов, которым вы доверяете. Хотя эти сайты тоже можно взломать, это маловероятно.

9. Будьте осторожны в социальных сетях.

Социальные сети — отличный способ поддерживать связь с друзьями и семьей. Но помните, чем вы делитесь в Интернете. Преступники и хакеры могут узнать много информации о вас, наблюдая за вашим общедоступным профилем. И точно так же, как вы не стали бы делиться всей своей личной информацией с незнакомцем, вы не должны делиться ею в Интернете.

10. Установите антивирусное программное обеспечение.

Вирусы, шпионское ПО, вредоносное ПО, фишинговые атаки и многое другое. Есть так много способов , которыми ваши данные могут быть скомпрометированы. Установка антивирусного программного обеспечения на ваше устройство поможет бороться с этими атаками. Убедитесь, что программное обеспечение активно и в актуальном состоянии, и что оно должно предотвращать угрозы цифровой безопасности еще до того, как они возникнут.

11. Избегайте ненужных загрузок.

Загрузки — это основная тактика, которую используют хакеры для получения доступа к вашей сети. Чтобы защитить ваш компьютер и ваши данные, ограничьте количество скачиваний. Следует избегать любого ненужного программного обеспечения или расширений браузера. А в организации сотрудникам требуется авторизация перед загрузкой чего-либо из Интернета.

Если вы считаете, что загрузка безопасна, всегда выбирайте индивидуальную установку и внимательно смотрите. Если какие-либо надстройки или расширения появляются во время автоматической установки, отклоните их.

12. Будьте чрезмерно подозрительны.

Хотя многие вещи в Интернете безопасны, лучше перестраховаться. Будьте в курсе любых ссылок, которые вы нажимаете, программного обеспечения, которое вы загружаете, и сайтов, которые вы посещаете. Немного здоровой паранойи по отношению к электронной почте, социальным сетям и Интернету может помочь вам уловить вещи, которые в противном случае ускользнули бы от вас.

Подробнее: https://www.securitylab.ru/blog/personal/bezmaly/350620.php