CYBER READINESS
INSTITUTE

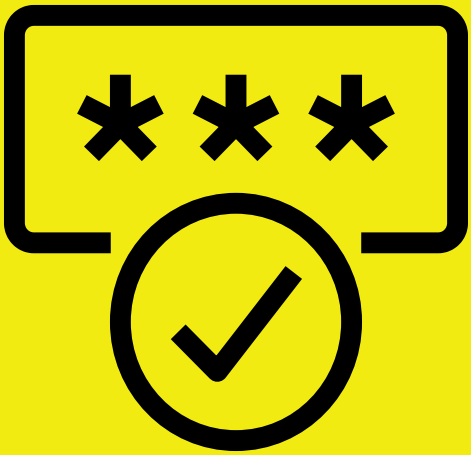
Кибер-готовность Советы и рекомедации

Советы и рекомендации

CYBER READINESS

В большинстве компаний есть рекомендации, которым должны следовать все сотрудники в отношении основных обязанностей таких, как вовремя приходить на работу, какой должна быть офисная одежда или как запросить отпуск. Также следует включить рекомендации по базовой киберготовности. В конце концов, безопасность ваших данных и систем оказывает огромное влияние на ваш бизнес и ваших клиентов. Мы рекомендуем вам использовать следующие советы и рекомендации, чтобы помочь информировать своих сотрудников и привлечь всех членов команды к ответственности для создания культуры киберготовности.

Пароли



Надежные пароли нужны для защиты ваших систем и учетных записей.

Независимо от того, получаете ли вы доступ к рабочей электронной почте, извлекаете файлы из общего жесткого диска или входите в какие-либо онлайн-сервисы, пароль или кодовая фраза, которые вы используете, важны. Вы даже можете добавить еще один уровень безопасности с помощью двухфакторной аутентификации. Двухфакторная система требует от вас ввода уникального кода, который отправляется на ваше мобильное устройство при каждом новом входе в систему. Двухфакторная аутентификация создает важную защитную связь между паролем и человеком.

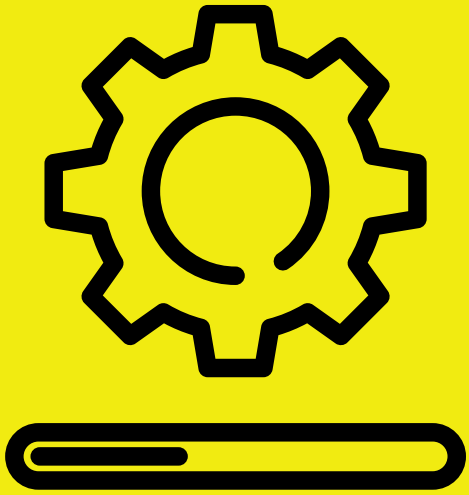
Мы предлагаем вам использовать эти рекомендации для ваших сотрудников:

1. Используйте длинную парольную фразу длиной не менее 15 символов. Например, выберите строчку из любимой телепередачи, фильма или песни.

2. Никогда не используйте одну и ту же парольную фразу для личных и рабочих учетных записей и не сообщайте свои имена пользователей и пароли никому, включая членов команды.

3. Используйте двухфакторную аутентификацию всегда, когда она доступна.

Обновления ПО



Крайне важно поддерживать все ПО и операционные системы в актуальном состоянии. Каждое обновление, выпущенное поставщиком программного обеспечения, может включать важные исправления и патчи, которые защищают ваше ПО и системы от атак. Многие компании назначают одного сотрудника по управлению обновлениями для всех компьютеров компании. Такой подход является предпочтительным. В качестве альтернативы вы можете потребовать, чтобы каждый сотрудник управлял своими собственными обновлениями. В любом случае регулярные обновления крайне важны.

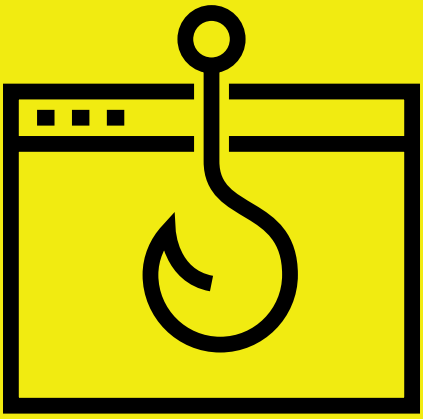
Мы предлагаем следующие рекомендации по обновлениям:

1. Включите функцию автоматического обновления на всех устройствах и в программном обеспечении всякий раз, когда оно предлагается.

2. Регулярно обновляйте все операционные системы, ПО и приложения для компьютеров, телефонов и планшетов, как только вы получите уведомление о готовности обновления.

3. Регулярно проверяйте, установлены ли все обновления, и нет ли пропущенных обновлений.

Фишинг



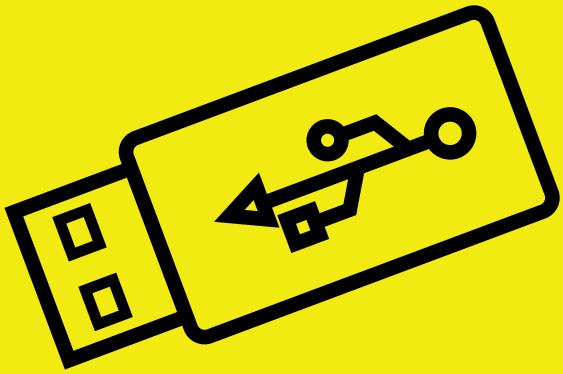
На сегодняшний день фишинг является одной из самых распространенных и опасных киберпроблем. Часто фишинговое письмо может выглядеть как настоящее, безопасное сообщение. Но открыв его, вы загрузите программные вирусы или предоставите злоумышленникам доступ к вашим данным. Все получают фишинговые письма. Вот почему важно знать, на что обращать внимание. Осведомленность — лучшая защита от фишинга.

Вот несколько советов, которые помогут:

1. Проверьте адрес электронной почты отправителя и любую другую идентифицирующую информацию такую, как логотип компании, почтовый адрес и контактные данные, на предмет любых несоответствий или признаков того, что это может быть подделка.

2. Если вы не знакомы с отправителем электронной почты, не нажимайте на ссылки и не загружайте вложения в электронном письме.

3. Если ответите на письмо, не предоставляйте никакой личной информации.



USB-накопители и съемные носители

USB-накопители удобны для обмена файлами между компьютерами, но их также можно использовать для переноса вирусов и вредоносных программ. Невозможно определить, где был накопитель или кто мог его скомпрометировать. Лучший способ избежать риска, связанного с USB-накопителями и другими съемными носителями, — полностью отказаться от их использования. Однако введение прямого запрета на использование USB-накопителей может быть проблематичным.

Поэтому мы предлагаем всем сотрудникам следовать приведенным ниже рекомендациям:

1. Предложите простые в использовании альтернативы USB-накопителям, например, облачные службы обмена файлами, чтобы USB-накопители не были нужны.

2. Никогда не принимайте и не используйте непроверенные сторонние USB-накопители.

3. Самое главное, полагайтесь на здравый смысл. Если вы не знаете, откуда взялся накопитель, не подключайте его.

Реагирование на инциденты

Киберготовность заключается в принятии правильных шагов для снижения риска, а также готовность в случае, если инцидент все же произойдет. Наличие плана реагирования на инциденты — важный шаг к киберготовности. Относитесь к этому, как к противопожарной тренировке: если случится чрезвычайная ситуация, важно иметь план, в котором каждый знает свою роль.

Дополнительную информацию о реагировании на инциденты вы найдете в Программе киберготовности, но, как минимум, обратите внимание на эти три аспекта:

1. Подготовка: убедитесь, что все сотрудники регулярно делают резервные копии своей работы и данных.

2. Реагирование: если произойдет атака или проблема, немедленно отключите атакованное устройство от сети компании. Все сотрудники должны пройти этот шаг.

3. Восстановление: восстановите потерянные данные из резервной копии, уведомите всех жертв атаки, а также сбросьте идентификатор и пароль скомпрометированного устройства.

ГОТОВЫ ПОДНЯТЬ СВОИ НАВЫКИ
НА НОВЫЙ УРОВЕНЬ?

УЗНАЙТЕ БОЛЬШЕ О ПРОГРАММЕ КИБЕРГОТОВНОСТИ

Программа киберготовности — это бесплатный онлайн-ресурс, представляющий собой практические шаги, которые вы можете выполнять для оценки и повышения своей киберготовности. Она проста в использовании и легко отслеживает ваш прогресс. Вы можете работать в своем собственном темпе. После завершения вы получите сертификат киберготовности, чтобы продемонстрировать клиентам и поставщикам, что вы предприняли шаги для создания культуры киберготовности в вашей организации.

Подробнее:

BeCyberReady.com