CRI HYBRID WORKFORCE GUIDE

CYBER READINESS INSTITUTE

Киберготовность для гибридных рабочих мест — **Правила, которым будут следовать сотрудники**

Компании всех масштабов теперь осознают, что на рабочих местах будут новые реалии, которые станут носить постоянный характер. Многие компании отправляют лишь небольшой процент своей рабочей силы обратно в физический офис, а это означает, что гибридная рабочая среда, в которой некоторые сотрудники работают дома, а некоторые — в офисе, станет реальностью.

Новая реальность требует от компаний разработки и внедрения устойчивых политик кибербезопасности для гибридных рабочих мест. В первые месяцы пандемии многим компаниям пришлось решать вопрос непрерывности бизнеса, и они сделали правила безопасности менее строгими, чтобы дать людям возможность эффективно работать из удаленных мест. Настало время заменить эти нестрогие правила безопасности гибридными правилами, обеспечивающими одинаковый уровень безопасности во всех рабочих средах. Институт киберготовности (CRI) помогает малым и средним предприятиям (МСП) устанавливать правила и процедуры безопасности в гибридной среде.

Люди — Какие изменения в поведении необходимы для продуктивной работы и киберготовности?

Процесс — Какие изменения в правилах и процедурах необходимы для определения четких ожиданий от поведения сотрудников и обеспечения их успешной работы?

Технологии — Какие новые технологии необходимы для повышения кибербезопасности, когда сотрудники работают удаленно или периодически меняют рабочее место между домом и офисом?

Институт киберготовности уделяет особое внимание поведению людей. См. пункты «Люди» и «Процессы» структуры, описанной выше. Мы также предоставим рекомендации по технологиям в гибридной рабочей среде.
Ниже приведены важные советы, которые помогут управляющим расставить приоритеты в том, что нужно сделать для обеспечения безопасной гибридной среды.

Убедитесь, что каждый сотрудник прошел обучение и знаком с правилами

вашей организации в отношении следующего:

- **Пароли.** Строгая аутентификация включает использование 16-символьных паролей и многофакторную аутентификацию, когда это возможно.
- **Фишинг.** Частое и актуальное обучение по фишинговым операциям, включая примеры недавних попыток фишинга дома и на работе, особенно в связи с COVID-19.
- **Использование USB-накопителей.** Предоставьте четкие рекомендации по работе с документами компании из нескольких мест. Этот подход мог бы включать создание облачной системы обмена файлами и обучение.
- **Обновление ПО.** Объясните, что обновления должны быть немедленно загружены на устройство, используемое для доступа к сети компании.

Все предприятия должны стараться выдавать рабочие ноутбуки всем сотрудникам, работающим из дома, чтобы избежать использования личных устройств для работы. Если это невозможно с финансовой точки зрения, поработайте со своими сотрудниками над созданием отдельной учетной записи пользователя на их личном устройстве.

Учитывая возросшую зависимость от платформ видеосвязи, убедитесь, что вы пользуетесь платформами с действующими протоколами безопасности, включая использование отдельного пароля для каждой встречи.

Устанавливайте проактивную и регулярную связь с вашей командой, в том числе осуществляйте:

- Еженедельные звонки персонала
- Регулярные проверки 1:1 по расписанию

Следите за дополнительными инструкциями в нашей подборке материалов по гибридным рабочим местам, поскольку мы проясняем вопрос по кибербезопасности в новой реальности и рабочей среде, давая советы руководителям и сотрудникам.

Об Институте киберготовности

Институт кибербезопасности — это некоммерческая инициатива, объединяющая лидеров бизнеса из разных секторов и географических регионов с целью обмена ресурсами и знаниями, которые используются для разработки бесплатных инструментов кибербезопасности в малых и средних предприятиях (МСП). Наши ресурсы для удаленной работы доступны на испанском и французском языках. Самостоятельная онлайн-программа киберготовности доступна на китайском, английском, французском, испанском, португальском, арабском и японском языках. Чтобы узнать больше, посетите сайт www.BeCyberReady.com.