САИБ

Сибирская Академия
Информационной Безопасности

ИНТЕРАКТИВНЫЕ КУРСЫ ПО ОСНОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ СОТРУДНИКОВ

ЧЕЛОВЕЧЕСКИЙ ФАКТОР – одна из основных причин взломов компаний при помощи социальной инженерии и широковещательных вирусных атак. Недопонимание важности включения в комплексную систему корпоративной безопасности всех структурных подразделений компании не позволяет достичь нужного уровня эффективности системы защиты корпоративных ресурсов и внутреннего контроля.

Внедряя культуру осведомлённости в области кибербезопасности, мы помогаем клиентам защищать активы компании и выполнять требования, предъявляемые к бизнес-процессам.

Чтобы решать задачи обучения сотрудников было удобно и эффективно, мы предлагаем продуманные курсы, в которых в доступной форме подаётся информация об основах поведения в информационной среде предприятия и сторонних информационных системах для снижения вероятности мошеннических действий.

ПРОГРАММА ПОВЫШЕНИЯ ОСВЕДОМЛЁННОСТИ

САИБ

1. Основы информационной безопасности

Данный курс направлен на обучение базовым правилам безопасности и умение предотвращать возникающие угрозы, находясь в офисе или за его пределами. Вы познакомитесь с оптимальными методами работы, которые помогут обеспечить безопасность данных, устройств, сети и рабочего места.

2. Осторожно, злой фишинг!

Интерактивный курс, разработанный в игровой форме, сценарий которого рассказывает о понятии фишинга, раскрывает основные признаки фишинговых сообщений, демонстрирует методы и примеры реализации атак, а также учит правилам грамотного реагирования на инциденты и позволяет освоить методы своевременного обнаружения фишинговых атак.

3. Основы социальной инженерии

В ходе данного курса вы научитесь распознавать атаки мошенников с использованием социотехники (социальной инженерии), обеспечивать собственную безопасность и помогать в этом своим коллегам по работе и не только.

4. Требования к паролям (Парольная политика)

В ходе данного курса вы научитесь составлять надёжные и безопасные пароли, узнаете, почему важно использовать второй фактор аутентификации, ознакомитесь с источниками скомпрометированных паролей, а также с инструментами хранения и защиты паролей.

5. Конфиденциальные документы: хранение и использование

Содержание курса рассказывает о понятии и особенностях конфиденциальной информации (КИ), определяет состав конфиденциальных документов и учит порядку обращения с ними. Вы научитесь правильно хранить документы, содержащие КИ, а также освоите основные принципы защиты конфиденциальной информации.

6. Обработка персональных данных

Формирование знаний и навыков, необходимых для обеспечения безопасности персональных данных, обрабатываемых в информационных системах организаций (государственных, муниципальных и др.), организующих и осуществляющих обработку персональных данных.

ПРОГРАММА ПОВЫШЕНИЯ ОСВЕДОМЛЁННОСТИ

САИБ

7. Антивирусная защита

В курсе рассматриваются основы теории компьютерных вирусов (понятие и классификация вирусов), современные тенденции развития угроз, связанных с применением программного обеспечения, принципы и технологии, используемые для борьбы с вредоносными программами и другими сетевыми угрозами.

8. Порядок работы с ресурсами Интернет

Данный курс объясняет, как следует работать пользователю в сети Интернет согласно требуемых условий безопасности. Вы узнаете какие опасности поджидают пользователей в сети, а также научитесь определять опасные и безопасные сайты.

9. Установка программного обеспечения и подключение дополнительных устройств на рабочей станции Пользователей

Курс знакомит пользователя с регламентом подключения дополнительных устройств, а также согласованием заявок, списком разрешенного оборудования, порядком регистрации новых устройств.

10. Использование внешних (съёмных) накопителей информации

В этом курсе вы ознакомитесь с принципами распространения вирусов через внешние USB-накопители и узнаете, к чему приводит бесконтрольно использование внешних устройств.

11. Безопасные настройки мобильных устройств (Защита мобильных устройств)

Курс предназначен для пользователей, которые используют мобильные устройства. Пользователь научится защищать свой смартфон, планшет или любое другое мобильное устройство, от злоумышленников и сохранить конфиденциальную информацию в безопасности.

12. Безопасная работа вне офиса

Данный курс позволит рассмотреть удалённый режим работы как новую реальность и угрозу. Вы научитесь обеспечивать безопасность при удалённом подключении при работе вне офиса: узнаете об обязанностях, ограничениях, запретах и правилах безопасной работы в период дистанционного режима исполнения трудовых обязанностей. Будут рассмотрены возможные сценарии действий злоумышленников, разобран порядок действий при возникновении проблем.

ПРОГРАММА ПОВЫШЕНИЯ ОСВЕДОМЛЁННОСТИ

13. Защити данные от хакеров (практический курс)

Тренажёр по информационной безопасности - только практические примеры и тесты типовых инцидентов Кибербезопасности. Тестовые вопросы по разделам - почтовые сервисы, опасные сайты, смартфоны.

14. Проверка знаний по информационной безопасности

Курс состоит из тестирования для проверки остаточных знаний обучающихся, ранее изучивших курсы «Программы повышения осведомлённости». Пользователям предлагается ответить на вопросы по различным темам информационной безопасности, при этом вопросы отбираются случайным образом из банка вопросов. После прохождения тестирования пользователь получает подробную карту с рекомендациями по темам, в которых допустил ошибки и которые требуют повторного прохождения.

15. Обучение персонала правилам безопасной работы на объектах КИИ

Курс предназначен для операторов, диспетчеров производства и сотрудников предприятий в сфере субъектов КИИ, которые осуществляют работу с данными объектами, а так же может быть интересен для иных производственных объектов, которые обеспечивают безопасность любых подсистем безопасности АСУ ТП.

САИБ

Сибирская Академия
Информационной Безопасности

БУДЕМ РАДЫ СОТРУДНИЧЕСТВУ

Сайт: https://saib.biz

Телефон: +7 (383) 309-26-36

Почта: info@saib.biz