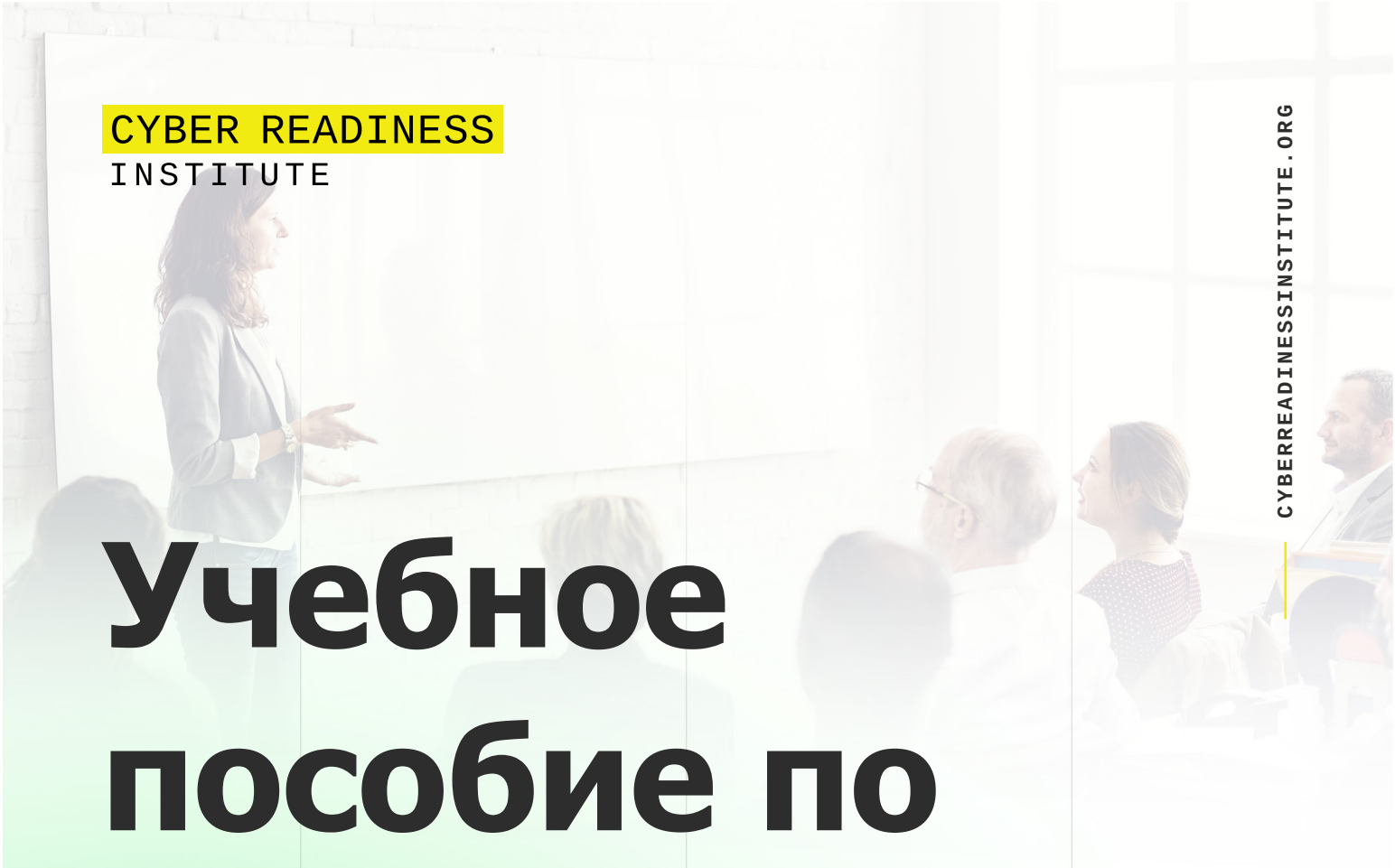
CYBER READINESS
INSTITUTE

CYBERREADINESSINSTITUTE.ORG



Учебное пособие по киберготовности

Все, что вам нужно для проведения тренингов по киберготовности для ваших сотрудников

Это учебное пособие является частью Программы киберготовности Института киберготовности и основано на передовом опыте ведущих экспертов в области кибербезопасности.

Предисловие Кирстен Тодт, управляющего директора Института киберготовности

Примечание для специалиста по киберготовности:

Кирстен Тодт

Управляющий директор Института киберготовности

Ваше путешествие по Программе киберготовности подошло к самому важному моменту — реализации. Теперь пришло время воспользоваться знаниями, которые вы получили в ходе программы, и поделиться ими со своими коллегами. Как специалист по киберготовности вашей организации вы можете содействовать долгосрочным изменениям вашей организации и в глобальной цепочке создания стоимости в целом.

В Учебном пособии по киберготовности мы включили основные ресурсы, которые помогут вам внедрять передовые методы киберготовности в вашей организации и делать это таким образом, чтобы способствовать значимым изменениям. Вы найдете шаблоны электронной почты, которые можно копировать и настраивать, чтобы отправлять сообщения своим коллегам. В пособие вошли контрольные списки, которыми можно поделиться, чтобы все члены вашей организации могли нести ответственность в соответствии с одними и теми же стандартами при решении четырех основных киберпроблем. Наконец, в нем есть ссылки на дополнительные ресурсы как от Института киберготовности, так и от всего сообщества кибербезопасности, в которых вы найдете дополнительные рекомендации для ваших сотрудников.

Внедрение — самый важный шаг в Программе киберготовности, так как это тот момент, когда знание становится действием. Мы приглашаем вас использовать ресурсы этого набора инструментов для создания культуры киберготовности в вашей организации.

Еще раз поздравляю вас с вашим достижением и от имени Института киберготовности желаю вам и вашей организации дальнейших успехов.

О программе

Программа киберготовности — это простой и практичный способ для организаций провести обучение сотрудников по вопросам безопасности и внедрить устойчивые и эффективные методы киберготовности. В этой программе, специально разработанной для малых и средних предприятий, особое внимание уделяется человеческому поведению, и она поможет вам создать рабочую силу, владеющую знаниями, умениями и эффективными методами кибергигиены, которые напрямую влияют на безопасность и жизнеспособность вашего бизнеса.
Узнайте больше на сайте cyberreadiness.org

Оглавление

Введение

Как пользоваться учебным пособием для обучения сотрудников киберготовности

Это пособие предназначено для специалистов по киберготовности и содержит все необходимое для подготовки ваших сотрудников. С помощью этих простых, готовых к использованию учебных материалов вы сможете эффективно обучить своих сотрудников четырем основным киберпроблемам, а также четко изложить новые политики вашей компании, связанные с ними, и протокол плана реагирования на инциденты.

Некоторые из ресурсов, представленных в этом пособии, включают:

- Руководство по реализации программы
- План и повестка дня обучения персонала
- Советы по успешному обучению киберготовности
- Руководство по внедрению культуры безопасности на вашем рабочем месте
- Готовые к использованию шаблоны эл. писем для обучения сотрудников
- Загружаемые обучающие видеоролики для сохранения и обмена
- Ссылки на PDF-файлы для распространения и публикации в общей рабочей области

Требования, необходимые до проведения обучения

Прежде чем приступить к реализации схемы обучения персонала в этом пособии, убедитесь, что специалист по киберготовности сделал следующее:

Принял участие в опросе по базовой оценке киберготовности

Базовая оценка киберготовности, которая проводится на этапе «Оценка вашей текущей киберготовности» онлайн-курса обучения, должна быть завершена до его проведения..

Понимание и документирование того, как в вашей организации в настоящее время используют пароли, обновления программного обеспечения, средства защиты от фишинга, а также USB-накопители и съемные носители, является важным первым шагом на пути к киберготовности.

Установление этого базового уровня обеспечивает практический способ измерения успеха вашей организации. В конце концов, вы не можете улучшить то, что не оцениваете.

Индивидуальное руководство по киберготовности

В Руководстве по киберготовности рассматриваются основные причины большинства киберпроблем и приводятся пошаговые инструкции по эффективному решению этих проблем на уровне организации и отдельных сотрудников.

В руководстве систематизированы политики и протоколы, и оно является справочным источником понятий, изложенных в этой учебной программе.

Если специалист по киберготовности завершил базовую оценку и руководство, то вы готовы работать с этим пособием и привести своих сотрудников к киберготовности!

Подготовка к обучению вашей рабочей силы

Руководство по реализации программы

Тренинг по киберготовности разработан таким образом, чтобы быть максимально кратким и действенным для сотрудников. Каждое занятие занимает всего около 10 минут, и каждый урок требует определенных действий со стороны сотрудника либо для установления протоколов, либо для проверки настроек своих систем. Чтобы соблюдение этих политик излишне не влияло на бизнес-операции, мы рекомендуем отправлять сотрудникам одно электронное письмо в неделю в течение 6 недель и заключительное электронное письмо с подведением итогов.

Советы по началу работы

Вы понимаете свою миссию. У вас есть руководство. У вас есть план действий. Теперь настало время произвести впечатление! Целенаправленное проведение этого обучения поможет сделать программу максимально успешной для вашей организации. Некоторые вещи, которые следует учитывать при составлении плана по обучению и привлечению вашей рабочей силы к проблемам киберготовности:

Имейте позитивный настрой

Позитивный подход и образ мышления имеют большое значение для завоевания доверия и одобрения, которые предшествуют соблюдению этих политик и практик. Поймите, что изменения требуют времени и что люди не хотят причинить вред, когда забывают что-то или совершают ошибки.

Хотя вы потратили много времени и обдумали эти вопросы, важно помнить, что большинство сотрудников, вероятно, этого не сделали. Самая захватывающая часть вашей роли — показать людям, как легко им оказывать огромное влияние на вашу организацию.

Составьте план

Относитесь к этому как к кампании, с датой начала и окончания этого процесса и определенными целями. Установите ожидания относительно того, что будет включать в себя обучение и что необходимо изменить в том, как выполняются определенные процессы.

Упрощайте

Постарайтесь сделать так, чтобы людям было как можно проще получать информацию и проходить обучение по этим вопросам. Это может включать в себя сеансы в формате онлайн-семинаров за обеденным столом для начального обучения, сеансы вопросов и ответов, а также последующую переписку по электронной почте для подведения итогов и напоминания на различных общих или групповых совещаниях о практиках киберготовности.

Сделайте это реалистичным

Вы, вероятно, стремитесь добиться успеха и значительных улучшений, но для реализации важно ставить реалистичные цели, чтобы избежать разочарования. Поймите, что люди не будут идеальными поначалу. Поощряйте любой прогресс и позитивные изменения и при необходимости напоминайте.

Поймите, что у людей много дел, и они часто сопротивляются изменениям, чтобы не чувствовать себя подавленными. Поделитесь своей увлеченностью и энтузиазмом по поводу этих изменений, чтобы люди разделили ваше волнение и поняли, что эта программа стоит потраченного времени на ее изучение.

Сделайте это значимым

Покажите людям, насколько они важны для успеха компании. Покажите связь между тем, как поведение и привычки каждого человека напрямую влияют на их собственную безопасность, а также на безопасность их коллег и не только.

Воплотите слова в реальность

Не думайте, что люди запомнят все, что услышат в первый раз. Убедитесь, что используете необходимые ресурсы в наборе справочно-информационных материалов так, чтобы на рабочем месте были напоминания и заметки, которые помогают не забывать эти вопросы.

Публично объявляйте об усилиях, которые люди вложили в эту практику. Сделайте так, чтобы люди чувствовали себя хорошо, участвуя в подобном поведении, а не ощущали контроль, раздражались или беспокоились из-за изменений.

Обзор программы обучения

Вот краткое изложение того, что ваши сотрудники узнают и чего достигнут за короткое время с помощью этого обучения:

Знание четырех основных киберпроблем безопасности бизнеса

- Они узнают о 4-х самых больших источниках кибератак и о том, как простые изменения в поведении могут иметь решающее значение

Понимание основных киберполитик в вашем руководстве по киберготовности

- Они ознакомятся с новыми политиками компании, касающимися этих областей, и поймут, как каждый из них должен решать эти киберпроблемы.

Знание о 3-х шагах в реагировании на инцидент и о том, с кем связаться при инциденте

- Каждый сотрудник должен знать о Плане реагирования на инциденты и как вести себя при киберсобытии, к кому обратиться за поддержкой и когда обращаться за помощью к третьей стороне.

Понимание своей роли в соблюдении кибергигиены

- Они буду осознавать ответственность, которую личные привычки и поведение каждого сотрудника на работе играют в предотвращении компрометации данных компании, раскрытии конфиденциальных данных клиентов наряду с их личной безопасностью.

Обучение поддержанию киберготовности и получение возможности для совершенствования

- Ресурсы должны быть легкодоступными, регулярно проверяться и включаться в обучение сотрудников, чтобы обеспечить последовательность и преданность делу поддержания и повышения киберготовности вашей организации.

Усилия, предпринятые в этом обучении, стоят потраченного временин Независимо от текущего уровня киберготовности, эта Программа повысит общую осведомленность о кибербезопасности и поможет предотвратить атаки, а также снизить риск, связанный с наиболее распространенными киберпроблемамин

Проведение тренинга по киберготовности

План обучения

Ниже представлен учебный план киберподготовки для этой программы обучения, которую можно отправить по электронной почте вашему персоналу или использовать для проведения виртуальных или выездных учебных занятий. Мы рекомендуем проводить обучение в формате электронных писем, чтобы уменьшить замедление работы и обеспечить максимальную гибкость для сотрудников, просматривающих эти материалы.

Учебная программа по обучению персонала

	Содержание/Тема	Включенные ресурсы:
Обучающее письмо 1	Наш тренинг по киберготовности начинается!	Электронное сообщение Обзор киберготовности (PDF) Повестка дня тренинга
Обучающее письмо 2	Надежный пароль	Электронное сообщение Видео о надежных паролях Руководство по обновлению ПО (PDF)
Обучающее письмо 3	Обновления ПО	Электронное сообщение Руководство по обновлению ПО (PDF)
Обучающее письмо 4	Осведомленность о фишинге	Электронное сообщение Видео о распознавании фишинга Руководство по предупреждающим признакам фишинга (PDF)
Обучающее письмо 5	Использование UBS-накопителей	Электронное сообщение Руководство по использованию USB-накопителей (PDF)
Обучающее письмо 6	План реагирования на инциденты	Электронное сообщение План реагирования на инциденты (PDF)
Обучающее письмо 7	Обзор главных проблем	Электронное сообщение Обзор 4-х главных киберпроблем
(По желанию) Обучающее письмо 8	Сертификация киберготовности и опрос сотрудников	Видео о том, что означает быть киберготовым Опрос/оценка сотрудников

Шаблоны эл. писем по обучению киберготовности

CYBERREADINESSINSTITUTE.ORG

Обучающее письмо 1

Тема: «Новые политики осведомленности о безопасности и обучение»

Здравствуйте, коллеги!

[НАЗВАНИЕ ОРГАНИЗАЦИИ] начинает киберподготовку! Что это значит для нас:

1. **Новые политики для сотрудников** — Мы добавили в наше руководство несколько новых политик и протоколов, которые содержат процедуры и рекомендации по повышению безопасности здесь: [ВВЕДИТЕ ДАННЫЕ]. Вы можете ознакомиться с этими политиками здесь: [ССЫЛКА]

2. **Обучение сотрудников** — Каждую неделю мы будем уделять несколько минут изучению этих политик и предоставлять вам ресурсы, необходимые для реализации изменений.

Возможно, вам интересно знать, что такое «киберготовность». Быть «киберготовым» означает осознание важности технологических привычек и знание того, на что обращать внимание, чтобы оставаться в безопасности.

Киберпреступники знают, как действует большинство из нас, и они используют эти распространенные привычки, чтобы обойти сложные технологии кибербезопасности. На самом деле, источником большинства кибератак являются несколько видов поведения, которые способствуют тому, чтобы мошенники смогли проникнуть внутрь системы. К счастью, когда мы знаем, что делать и чего не делать, учитывая эти главные четыре киберпроблемы, вероятность того, что методы атаки сработают, резко снижается.

1. Пароли — 63% утечек данных происходят из-за ненадежных или украденных паролей.

2. Обновления ПО — 77% атак использовали бреши в ПО, уже установленном на компьютерах.

3. Фишинг — 91% всех кибератак начинаются с фишингового письма.

4. USB-накопители и съемные носители — 27 % заражений вредоносным ПО исходят от зараженных USB-накопителей.

Устранение этих четырех проблем означает, что конфиденциальные данные, связанные с [НАЗВАНИЕ ОРГАНИЗАЦИИ], клиентами, поставщиками и коллегами, будут в большей безопасности. Поэтому мы собираемся разослать несколько кратких электронных писем, которые предоставят некоторую базовую подготовку по четырем основным киберпроблемам и простым вещам, которые мы все можем сделать, чтобы избежать киберпреступлений и предотвратить их.

Эти электронные письма являются частью обучения по повышению осведомленности о кибербезопасности в рамках Программы киберготовности, и в них рассказывается, как обращаться с паролями, обновлениями ПО и USB-накопителями. Они также включают обучение осведомленности о фишинге. Решение этих четырех ключевых проблем значительно повысит устойчивость вашей организации и ее готовность к киберсобытию.

Обратите внимание, что вы должны соблюдать политики организации и в обязательном порядке пройти обучение. Эти электронные письма и запросы будут занимать всего 10-15 минут вашего времени, и мы просим вас отвечать своему непосредственному руководителю после завершения каждого сеанса обучения.

Первое обучающее электронное письмо будет отправлено [ДД/ММ]. Тем временем, пожалуйста, прочтите программу обучения в формате PDF и обзор программы, чтобы узнать больше об этой подготовке.

Сообщите нам, если у вас возникнут какие-либо вопросы.

[ПОДПИСЬ ЭЛЕКТРОННОГО СООБЩЕНИЯ]

Обучающее письмо 2

Тема: «Основная киберпроблема № 1. Пароли на работе»

Здравствуйте, коллеги!

Это первая часть серии учебных занятий Программы киберготовности!

Основная киберпроблема № 1 — Пароли

Пароль — это дверь в сеть, данные человека или организацию. Мы используем сотни паролей и подключенных устройств в нашей профессиональной и личной жизни. Каждый из них является дверью в нашу компанию. Слабый пароль -- это то же самое, что оставить дверь незапертой.

Каждый из наших паролей является привратником важной информации и систем, которым мы доверяем и за которые несем ответственность. Мы не можем позволить им быть легкой мишенью.

Сложный для взлома пароль -- это первая линия защиты от авантюристичных хакеров. Создание надежного пароля занимает всего несколько секунд, и это обязан делать каждый сотрудник [НАЗВАНИЕ ОРГАНИЗАЦИИ], чтобы максимально защитить наши данные.

Короткое видео о том, как создавать надежные пароли, которые легко запомнить и использовать:

[ССЫЛКА]

Мы также обновили политику нашей компании в отношении паролей, которая распространяется на всех сотрудников и подрядчиков [НАЗВАНИЕ ОРГАНИЗАЦИИ]. Некоторые основные положения этой политики:

- Используйте пароли или PIN-коды на всех устройствах, включая персональные телефоны и планшеты
- Создавайте свои пароли, используя парольную фразу из 15 символов
- Никогда не используйте один и тот же пароль для деловых или личных целей
- Никогда не используйте и не используйте повторно одну и ту же парольную фразу в двух (или более) системах одновременно.
- Никогда не делитесь учетными записями с несколькими людьми
- Включите многофакторную аутентификацию, если она доступна для любых приложений, используемых на корпоративных устройствах и личных устройствах, используемых для бизнеса.

К письму прилагается контрольный список паролей в формате PDF с пошаговыми инструкциями по внедрению этой новой политики, который вы можете полностью прочитать здесь: [ССЫЛКА].

Обратите внимание, что соблюдение политики и заполнение контрольного списка паролей в формате PDF требуется для всех сотрудников [НАЗВАНИЕ ОРГАНИЗАЦИИ]. Заполнение контрольного списка займет всего 10-15 минут, и вы должны сделать это до [ДД/ММ]. Обязательно сообщите своему руководителю после того, как вы заполните контрольный список.

Если у вас есть какие-либо вопросы, связанные с этим обучением, или о том, как использовать свои пароли и управлять ими, обращайтесь ко мне напрямую, и мы обсудим ваши вопросы.

[**ПОДПИСЬ ЭЛЕКТРОННОГО СООБЩЕНИЯ**]

Обучающее письмо 3

Тема: «Основная киберпроблема №2. Обновления ПО»

Здравствуйте, коллеги!

Это вторая часть серии учебных занятий Программы киберготовности.

Основная киберпроблема № 2 — Обновления программного обеспечения

Вы, по всей вероятности, видели всплывающие уведомления о том, что для вашего компьютера, ноутбука, планшета или мобильного устройства доступно обновление программного обеспечения. Хотя вам скорее всего захочется нажать на «Напомнить позже», это плохая идея. Обновления программного обеспечения устраняют важные бреши в системе безопасности и исправляют критические ошибки, которые были обнаружены. Обновления ПО должны быть установлены немедленно.

Если вы не установите обновления, вы оставите дверь открытой для известных уязвимостей системы безопасности, которые киберпреступники могут и используют для проникновения и проведения атаки. Печально известная атака программы-вымогателя WannaCry воспользовалась выявленной уязвимостью в системе безопасности ОС Windows, которая уже была исправлена в обновлении, выпущенном за два месяца до инцидента. Несмотря на то, что атака затронула только тех, кто не установил обновление, всего за 24 часа более 230 000 систем были скомпрометированы и причинили глобальный ущерб в размере 4 миллиардов долларов США.

Установка обновлений может устранить эти простые точки доступа и защитить от атак вредоносных программ и программ- вымогателей. К счастью, обновления ПО легко выполнить.

Большинство операционных систем и ПО можно настроить на «автоматическое обновление», что может автоматизировать установку обновлений и свести к минимуму прерывание вашей работы. Чтобы убедиться или включить «автоматическое обновление» для приложений, систем и устройств, потребуется всего несколько минут, поэтому сделайте это как можно скорее.

Как и в случае с паролями, мы также пересмотрели политику нашей компании в отношении обновлений ПО. Эти стандарты распространяются на всех сотрудников и подрядчиков [НАЗВАНИЕ ОРГАНИЗАЦИИ].

Некоторые основные положения нашей новой политики:

- **Включите автоматическое обновление на всех ваших устройствах**, включая персональные устройства такие, как мобильные телефоны и планшеты, которые подключаются к сети [НАЗВАНИЕ ОРГАНИЗАЦИИ] , включая системы (например: Windows, OS X, iOS, Android и т. д.).
- **Не игнорируйте уведомления об автоматических обновлениях.** После запроса обновления должны быть установлены в течение 24 часов.

К письму прилагается контрольный список обновлений ПО в формате PDF с пошаговыми инструкциями и ссылками, которые помогут легко выполнить это действие и которые доступны здесь: [ССЫЛКА].

Обратите внимание, что соблюдение политики и заполнение контрольного списка обновлений ПО в формате PDF являются обязательными для всех сотрудников [НАЗВАНИЕ ОРГАНИЗАЦИИ]. Заполнение контрольного списка займет всего 10-15 минут, и вы должны сделать это до [ДД/ММ]. Обязательно сообщите своему руководителю после того, как вы заполните контрольный список.

Если у вас есть какие-либо вопросы, связанные с этим обучением, или о том, как использовать обновления ПО и управлять ими, обращайтесь ко мне напрямую, и мы обсудим ваши вопросы.

[**ПОДПИСЬ ЭЛЕКТРОННОГО СООБЩЕНИЯ**]

Обучающее письмо 4

Тема: «Основная киберпроблема № 4. Фишинг»

Здравствуйте, коллеги!

Готовы к 3-й части серии учебных занятий Программы киберготовности? Осталась всего одна часть до подведения итогов этого тренинга!
Основная киберпроблема № 3 — Фишинг

Фишинг — одна из самых распространенных кибератак. **Любой, у кого есть учетная запись электронной почты или смартфон, может получить фишинговое электронное письмо или текст. Фишинговые атаки используют вводящие в заблуждение сообщения для получения конфиденциальной информации или доступа к сети.** Эти сообщения пытаются заставить людей **нажать на ссылку, загрузить вложение в сообщении или даже напрямую предоставить конфиденциальную информацию, например, банковские реквизиты.**

Большинство из нас знает, что нигерийский принц, отправивший вам электронное письмо с просьбой перевести 5000 долларов США на его банковский счет, является мошенничеством. **Но фишинговые мошенничества часто очень хитроумны, и их трудно обнаружить,** если вы не знаете, что искать. Эти сообщения **зачастую хорошо замаскированы под реальные сообщения, которые человек может получить на законных основаниях.**

Фактически, **9 из 10 кибератак начинаются с фишинга,** так как то, что они делают, работает очень хорошо. Методы, которые мошенники используют для фишинговых атак, постоянно развиваются, **при этом в большинстве фишинговых сообщений используется несколько уловок**, которым вы можете научиться, чтобы вас не обманули.

Посмотрите этот короткий видеоклип, чтобы узнать, как распознать фишинг в ваших сообщениях. [ССЫЛКА НА ВИДЕО]

Политика и практика нашей компании в отношении осведомленности о фишинге были обновлены и будут применяться ко всем сотрудникам и подрядчикам [НАЗВАНИЕ ОРГАНИЗАЦИИ].

Некоторые основные положения этой новой политики:

- Не предоставляйте личную информацию по электронной почте и не предпринимайте никаких действий, открывая вложения, нажимая на ссылку или вводя информацию во всплывающем окне.
- Всегда проверяйте личность отправителя, прежде чем нажать на любое вложение в электронном письме.
- Прочитайте полный адрес электронной почты отправителя и проверьте его на наличие грамматических или орфографических ошибок.
- Если какое-либо электронное письмо выглядит необоснованным, не открывайте никакие вложения и не следуйте инструкциям в электронном письме.
- При получении документа из внешнего источника открывайте его только в режиме чтения/защищенном режиме.
- Сообщайте о любых подозрительных электронных письмах [ИМЯ СПЕЦИАЛИСТА ПО КИБЕРГОТОВНОСТИ] или ИТ-персоналу.

К письму прилагается контрольный список осведомленности о фишинге в формате PDF с советами по фишингу из тренинга, с которым вы можете ознакомиться здесь :[ССЫЛКА]. Обратите внимание, что соблюдение политики и заполнение обучающего видео и PDF-файла о фишинге требуется для всех сотрудников [НАЗВАНИЕ ОРГАНИЗАЦИИ]. Заполнение контрольного списка займет всего 10-15 минут, и вы должны сделать это до [ДД/ММ]. Обязательно сообщите своему руководителю после того, как вы заполните контрольный список.

Если у вас есть какие-либо вопросы, связанные с этим обучением, или о том, как использовать обновления ПО и управлять ими, обращайтесь ко мне напрямую, и мы обсудим ваши вопросы.

[**ПОДПИСЬ ЭЛЕКТРОННОГО СООБЩЕНИЯ**]

Обучающее письмо 5

Тема: «Основная киберпроблема № 4. USB и съемные носители»

Здравствуйте, коллеги!

Сегодня мы рассмотрим последнюю основную киберпроблему в нашей серии учебных занятий Программы киберготовности!

Основная киберпроблема №4 — USB и съемные носители

USB — это популярный и простой способ хранения и передачи файлов, но они также являются легкой мишенью для вредоносных программ.

Хакеры могут заразить USB вредоносным ПО таким, как вирусы, программы-шпионы, программы-рутеры и т. д., которые могут нанести непоправимый ущерб. Человек, найдя «потерянный» USB на парковке, может подключить его к своему компьютеру, чтобы посмотреть, что на нем, и вернуть его владельцу, не зная о риске.

USB — это не единственный вид съемных носителей, они также могут включать в себя:

- Оптические диски (диски Blu-Ray, DVD, CD-ROM)
- Карты памяти (карта Compact Flash, карта Secure Digital, Memory Stick)
- Zip-диски/дискеты
- USB-накопители
- Внешние жесткие диски (DE, EIDE, SCSSI и SSD)
- Цифровые камеры
- Смартфоны
- Другие внешние/стыковочные устройства, которые содержат съемные носители

Мы обновили политику нашей компании в отношении USB/съемных носителей, которая будет применяться ко всем сотрудникам и подрядчикам [НАЗВАНИЕ ОРГАНИЗАЦИИ]. Некоторые основные положения этой новой политики:

- **[НАЗВАНИЕ ОРГАНИЗАЦИИ] запрещает всем сотрудникам использовать USB-накопители и съемные носители,** за исключением редких и заранее разрешенных случаев.
- **Сотрудники должны использовать исключительно облачные приложения и/или безопасное шифрование электронной почты** для обмена и хранения всех файлов.
- **Использование любых съемных носителей должно быть немедленно прекращено,** и они должны быть просканированы перед передачей файлов в облако для хранения.

Прилагаемый контрольный список по USB в формате PDF содержит основные сведения о работе со съемными носителями, доступ к которым можно получить здесь: [ССЫЛКА].

Обратите внимание, что соблюдение политики и заполнение обучающего видео и контрольного списка по USB в формате PDF являются обязательными для всех сотрудников [НАЗВАНИЕ ОРГАНИЗАЦИИ]. Заполнение контрольного списка займет всего 10-15 минут, и вы должны сделать это до [ДД/ММ]. Обязательно сообщите своему руководителю после того, как вы заполните контрольный список.

Если у вас есть какие-либо вопросы, связанные с этим обучением, или о том, как использовать обновления ПО и управлять ими, обращайтесь ко мне напрямую, и мы обсудим ваши вопросы.

На следующей неделе мы расскажем о нашем новом Плане реагирования на инциденты. Он поможет нам подготовиться к киберсобытиям и проблемам, которые могут произойти, и научиться принимать ответные меры против них.

[**ПОДПИСЬ ЭЛЕКТРОННОГО СООБЩЕНИЯ**]

Обучающее письмо 6

Тема: «Наш план реагирования на киберинциденты»

Здравствуйте, коллеги!

Сегодня мы расскажем о нашем плане реагирования на киберинциденты!

Это послужит дорожной картой для нашей компании в целом и для каждого человека, чтобы знать, что делать и как действовать в случае возникновения киберпроблемы.

Методы кибергигиены, которые мы изучили во время этого тренинга, и наши новые политики киберготовности имеют большое значение для снижения риска нарушения правил безопасности. Но даже при наличии наилучших мер важно учитывать, что в какой-то момент нам, вероятно, придется иметь дело с инцидентом безопасности.

Наш план реагирования на инциденты позволяет быстро реагировать на все возникающие проблемы, решать их и извлекать из них уроки. Кризис может быть хаотичным и стрессовым, но наличие пошагового плана гарантирует то, что наша реакция на нарушение будет стратегической и эффективной, а не реактивной или бесполезной.

Наше реагирование на инциденты состоит из трех основных элементово:

1. **Подготовка**
    - Всегда следите за актуальностью резервных копий и синхронизируйте облачные учетные записи
    - Всегда будьте начеку в случае подозрительной или странной активности
2. **Реагирование**
    - Всегда обращайтесь к [СПЕЦИАЛИСТ ПО КИБЕРГОТОВНОСТИгКОНТАКТНОЕ ЛИЦО ПО ИТ], если происходит что-то странное, или что-то кажется неправильным (компьютер завис после открытия файла и т. д.)
    - Немедленно прекратите использование устройстваготключите устройство от сети
3. **Восстановление**
    - Сообщите всем затронутым сторонам
    - Сбросьте все пароли и идентификаторы
    - Переустановите ПО, синхронизированные учетные записи и резервные копии данных по мере необходимости

Мы обновили справочное пособие нашей компании, включив в него этот План реагирования на инциденты, который необходимо просмотреть и использовать для всех сотрудников и подрядчиков [НАЗВАНИЕ ОРГАНИЗАЦИИ] и доступ к которому вы можете найти здесь [ССЫЛКА].

Обратите внимание, что проверка и соблюдение политики являются обязательными для всех сотрудников [НАЗВАНИЕ ОРГАНИЗАЦИИ]. Это займет всего й минут и должно быть завершено до [ММгДД]. Обязательно сообщите своему руководителю после того, как просмотрите План реагирования на инциденты.

Если у вас есть какие-либо вопросы, связанные с нашим Планом реагирования на инциденты, обращайтесь ко мне напрямую, и мы обсудим ваши вопросы. На следующей неделе мы кратко подведем итоги того, чему научились в ходе этой программы, а затем [НАЗВАНИЕ ОРГАНИЗАЦИИ] официально получит сертификат киберготовности!

[**ПОДПИСЬ ЭЛЕКТРОННОГО СООБЩЕНИЯ**]

Обучающее письмо 7

Тема: «Обзор киберготовности»

Здравствуйте, коллеги!

Мы завершили серию учебных занятий Программы киберготовности! Давайте кратко рассмотрим то, что мы узнали на пути к киберготовности.

4 основные киберпроблемы

Проблема № 1 — Пароли

- Пароли — это двери в нашу сеть и данные, а слабые пароли — это простой способ для хакеров получить доступ к ним. Использование слабых паролей для учетных записей пользователей и рабочих устройств может поставить под угрозу всю сеть.
- Используйте парольные фразы для каждой учетной записи и включите многофакторную аутентиикацию для всех учетных записей, приложений или устройств, которыми вы пользуетесь.

Проблема № 2 — Обновления ПО

- Обновления ПО устраняют уязвимости в системе безопасности и добавляют новые функции для ваших устройств, ликвидируя слабые места в системе безопасности и защищая от кражи ваших данных вредоносными программами.
- Установите для всех устройств автоматическое обновление, чтобы обеспечить загрузку обновлений ПО, как только они станут доступны.

Проблема № 3 — Осведомленность о фишинге

- Фишинг нацелен на отдельных лиц, обманным путем заставляя их нажать на ссылку или загрузить вложение. Эти ссылки или вложения могут заразить устройство вредоносным ПО или позволить хакеру получить доступ к системам или учетным записям человека.
- Знание того, как выявлять и иметь дело с попытками фишинга, помогает защититься от любых атакующих сообщений, которые проходят через спам-фильтры электронной почты.

Проблема № 4 — USB-накопители и съемные носители

- USB-накопители и другие съемные носители могут быть заражены вредоносным ПО, и об этом нельзя узнать, пока не станет слишком поздно.
- Часто люди подключают неизвестный USB-накопитель к своему компьютеру, чтобы посмотреть, что на нем, и заражают всю сеть. Избегайте использования USB-накопителей и съемных носителей без предварительного разрешения и используйте безопасные решения такие, как облако и зашифрованная электронная почта для обмена файлами и хранения.

План реагирования на инциденты

1. Подготовка — Всегда будьте начеку и следите за тем, чтобы резервные копии были актуальными, а облачные учетные записи синхронизировались.
2. Реагирование — Всегда сообщайте, если что-то не так, немедленно прекратите использование устройства / отключите его от сети.
3. Восстановление — Сбросьте все пароли и идентификаторы после взлома.
4. Цените время и усилия каждого, потраченные на прохождение этого тренинга, поскольку мы продолжаем повышать нашу киберготовность!

Как всегда, если у вас возникнут какие-либо вопросы, обращайтесь ко мне напрямую, чтобы обсудить ваши вопросы.

[**ПОДПИСЬ ЭЛЕКТРОННОГО СООБЩЕНИЯ**]

Ресурсы программы обучения

Повестка дня тренинга киберготовности

Краткое изложение того, чему вы научитесь и чего достигнете за короткое время на этом тренинге:

Знание четырех основных киберпроблем для безопасности бизнеса

- Узнайте о 4-х важнейших источниках кибератак и о том, как простые изменения в поведении могут иметь решающее значение.

Понимание основных киберполитик, изложенных в руководстве по киберготовности

- Изучите новые политики компании, касающиеся киберпроблем, и узнайте, как следует их решать..

Знание 3-х шагов в реагировании на инцидент и того, к кому обращаться

- Каждый сотрудник должен быть осведомлен о Плане реагирования на инциденты компании и должен знать, что делать в ответ на киберсобытие, к кому обращаться за поддержкой и когда обращаться за помощью к третьей стороне.

Понимание своей роли в соблюдении кибергигиены

- Поймите ответственность, которую личные привычки и поведение каждого сотрудника на работе играют в предотвращении компрометации данных компании, раскрытия конфиденциальных данных клиентов наряду с их личной безопасностью.

Знание того, как поддерживать киберготовность и получить возможность совершенствоваться

- Учебные ресурсы следует внимательно читать и периодически пересматривать, чтобы быть последовательным и приверженным делу поддержания и повышения киберготовности вашей организации.

Усилия, предпринятые во время этого обучения, стоят потраченного времени. Эта программа повысит нашу общую осведомленность о кибербезопасности, поможет предотвратить атаки и снизить риск, связанный с наиболее распространенными киберпроблемами.

Контрольный список использования паролей

Всегда используйте надежный пароль или парольную фразу

- **Всегда меняйте пароли по умолчанию** перед первым использованием
- **Используйте парольную фразу длиной не менее 15 символов для создания своих паролей.** Парольная фраза является частью предложения, например, «юavVacationYosemite» или предложение, например «Мне нравится баскетбол».
- **Проверяйте надежность паролей** перед использованием

Используйте разные пароли для каждой учетной записи

- Убедитесь, что **для каждой учетной записи используется другой надежный пароль**/ парольная фраза, которая л**ибо полностью обезличенал либо сгенерирована случайным образом**.
- **НЕ используйте** формулы для создания «уникальных» паролей для ваших учетных записей. Их легко запомнить, но так же легко взломать ((PasswordFB, PasswordYT, PasswordGmail и т. д.)

Включите многофакторную аутентификацию (MFA)

- Включите многофакторную аутентификацию (MFA) во всех своих учетных записях, где это возможно.

Советы по безопасности пароля

- Удалите учетные записи и удалите приложения, которые вы больше не используете.
- **Убедитесьл что во всех ваших учетных записях используются надежные пароли** и что пароли не используются более одного раза.
- Проверьте настройки безопасности на подключенных устройствах, учетных записях и приложениях, чтобы увидеть текущие настройки или настройки по умолчанию.
- **Проверьте надежность ваших текущих паролей** и при необходимости обновите их.
- **Никогда и никому не сообщайте пароли компании.** Всегда применяйте новые пароли до и после любой поездки, если на устройстве используются данные компании.

Контрольный список обновлений ПО

Загрузите и включите автоматические обновления

Убедитесь, что все ваши системы, приложения и устройства исправлены и настроены для автоматического обновления.

- **Продукты Apple** — Продукты и ПО для iPhone, iPad, Apple Watch или macOS
- **Продукты Android** — Любые устройства, приложения или системы на базе Android (могут включать в себя смартфоны, ноутбуки, планшеты, смарт-часы, бытовую технику, автомобили, системы умного дома и мониторинга безопасности, камеры, смарт-телевизоры, игровые приставки)
- **Продукты Microsoft** — Операционные системы Windows: ноутбуки, настольные компьютеры, планшеты,смартфоны, игровые приставки и др.
- **Другие приложения/платформы/устройства** — Применение исправлений и настройка автоматических обновлений для всех других устройств и приложений (например, пакет Office365 на Mac)

Сделайте своевременные обновления программного обеспечения стандартной практикой

Мы добавили в руководство для сотрудников политику в отношении ПО из Программы киберготовности, в которой изложены требования, связанные с обновлениями ПО и другими важными проблемами безопасности.

- Включите уведомления об автоматических обновлениях и не игнорируйте их.
- Устанавливайте обновления ПО как можно скорее, в идеале в течение 24 часов.
- Всегда обновляйте рабочие и персональные устройства, которые вы используете для работы.

Контрольный список осведомленности о фишинге

Будьте начеку и используйте этот контрольный список, чтобы быстро определить, может ли странное сообщение быть фишинговой атакой.

4 способа обнаружить фишинг

1. Проверьте адресные строки

- Давал ли я свой адрес электронной почты этой компании раньше?
- Есть ли у меня учетная запись в этой компании?
- Соответствует ли личность отправителя цели электронного письма?
- Указана ли моя электронная почта как адрес отправителя?
- Кому адресовано письмо: неизвестному получателю или большому количеству получателей, с которыми вы не знакомы?

2. Проверьте содержание

- Ссылки, указанные в тексте письма, выглядят действительными?
- Есть ли орфографические ошибки и опечатки? Какова грамматика и подходит ли тон?
- Обещают ли мне большие деньги за небольшие усилия с моей стороны или без них?
- Просят ли меня внести предоплату за сомнительную деятельность, комиссию за обработку или оплатить расходы, чтобы ускорить процесс?
- Просит ли кто-нибудь меня указать номер моего банковского счета, другую личную финансовую информацию или пароли? («Подтвердите свою учетную запись» или «Нажмите на ссылку ниже, чтобы получить доступ к своей учетной записи».)

3. Проанализируйте цель письма

- Действительно ли проблема так актуальна, как утверждает отправитель?
  - «Если вы не ответите в течение 48 часов, ваша учетная запись будет закрыта».
  - «Невыполнение этого требования может автоматически привести к деактивации вашей учетной записи».
- Почему отправитель запрашивает конфиденциальную информацию? Как я могу определить, является ли предлагаемая деятельность законной и подлинной?

4. Будьте осторожны с вложениями

- Не открывайте непредусмотренные вложения.
- Не открывайте вложения от незнакомых людей. Прежде всего удостоверьтесь, что вы знаете отправителя.
- Не открывайте необычные вложения.
- Не открывайте вложения, которые отправлены со странными сообщениями.

Контрольный список использования USB и съемных носителей

Следуйте этим рекомендациям по использованию и управлению съемными носителями и устройствами на работе.

Когда использовать:

- **НЕ используйте USB-накопители без предварительного разрешения** для работы или на работе.
- По возможности **избегайте использования съемных носителей.**
  - Если вы в настоящее время используете USэ-накопители в своей роли, обратитесь к нужным людям, чтобы безопасно перенести любые конфиденциальные данные на защищенный диск и сразу же удалить данные с устройства после завершения..
- **Никогда не подключайте к компьютеру неизвестные мультимедийные устройства**, которые вы нашли. Передайте любой неизвестный накопитель службе безопасности или ИТ-персоналу.

Как защитить:

- **Отключите функции автозапуска и автовоспроизведения** для всех съемных носителей или устройств. Эти функции запускаются автоматически при подключении к USB-порту или накопителю.
- **Убедитесь, что на вашем компьютере установлены** антивирусные решения для активного поиска вредоносных программ при подключении съемных носителей или устройств любого типа.
- **Убедитесь, что все съемные носители и устройства зашифрованы.** Это сделает любые данные бесполезными для неавторизованных пользователей в случае потери или кражи устройства.
- **Всегда применяйте новые пароли до и после любой поездки**, когда данные компании используются на съемных носителях или устройствах. Никогда никому не сообщайте пароли, используемые для съемных носителей или устройств.
- **Храните личные и деловые данные отдельно.** Не храните рабочие данные на каком-либо личном устройстве и наоборот.

Поддержание киберготовности

Оценка и поддержание киберготовности

Поздравляем! Теперь ваши сотрудники осведомлены о четырех основных проблемах киберготовности и полностью оснащены методами и политиками, которые снижают риск кибератак! Если вы еще этого не сделали, уделите минуту, чтобы признать и оценить эти усилия и то положительное влияние, которое они окажут на вашу организацию.

Повторная оценка после обучения

Теперь пришло время пересмотреть степень киберготовности вашей организации, чтобы вы могли увидеть влияние программы и определить области, которые необходимо улучшить и укрепить с сотрудниками.

Проведите оценку после обучения в онлайн-программе подготовки специалистов по киберготовности и сравните ее с первоначальным исходным уровнем, чтобы определить прогресс и области для улучшения.

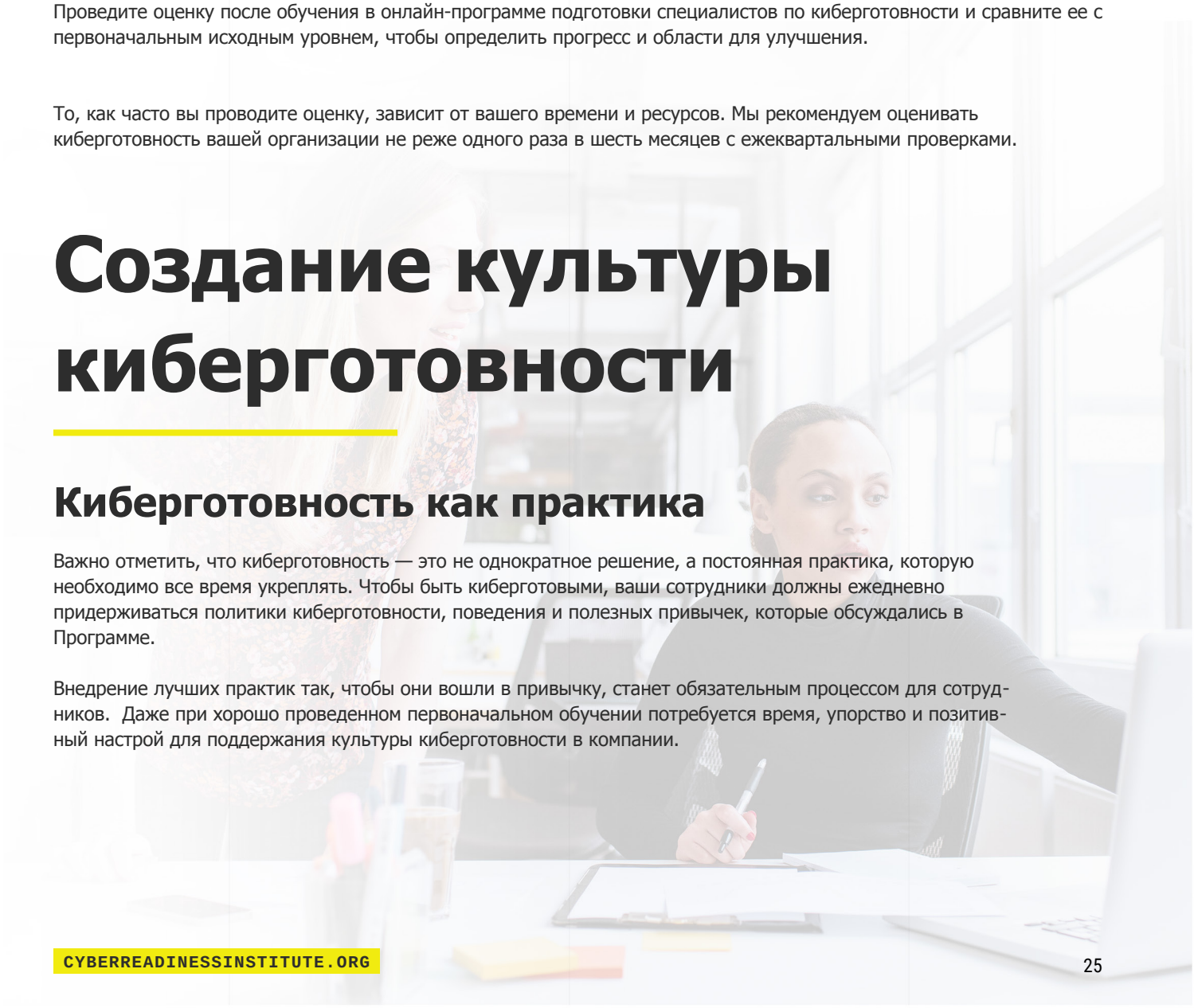
То, как часто вы проводите оценку, зависит от вашего времени и ресурсов. Мы рекомендуем оценивать киберготовность вашей организации не реже одного раза в шесть месяцев с ежеквартальными проверками.

Создание культуры киберготовности

Киберготовность как практика

Важно отметить, что киберготовность — это не однократное решение, а постоянная практика, которую необходимо все время укреплять. Чтобы быть киберготовыми, ваши сотрудники должны ежедневно придерживаться политики киберготовности, поведения и полезных привычек, которые обсуждались в Программе.

Внедрение лучших практик так, чтобы они вошли в привычку, станет обязательным процессом для сотрудников. Даже при хорошо проведенном первоначальном обучении потребуется время, упорство и позитивный настрой для поддержания культуры киберготовности в компании.



Советы по повышению уровня киберготовности

- Сделайте эту практику частью процесса адаптации новых сотрудников, чтобы по мере роста рабочей силы повышалась ваша киберготовность.
- Проводите опрос не реже двух раз в год, чтобы оценить осведомленность и согласованность в вашей организации.
- Периодически проверяйте и оценивайте киберготовность своих сотрудников, а также напоминайте им правила киберготовности посредством периодических занятий по переподготовке, либо с помощью кампаний по электронной почте не реже двух раз в год.
- Используйте и внедряйте руководства и ресурсы Института киберготовности, чтобы помочь вашей организации постоянно повышать уровень безопасности.

Полезные ресурсы по кибербезопасности

Пособия Института киберготовности

- Создание культуры киберготовности для удаленной рабочей силы
- ЧАВО в облаке
- Основы защиты данных для удаленных сотрудников
- Руководство по программамнвымогателям
- Защита удаленной рабочей силы
- Как сделать удаленных сотрудникн ов киберготовыми
- Три главных правила и три главных зан прета для удаленных сотрудников

Справочные ссылки

- 5 причин тогол почему вы должны использовать облачное ханилище каждый день
- Как работает облачное хранилище
- Надежная защита информации в облаке
- Использование парольной фразы
- Киберустойчивость и финансовые организации: набор инструментов для наращивания потенциала
- 3 шага для предотвращения фишинга
- Кибербезопасность: 10 советовл как подготовиться к большим и маленьким угрозам

Об Институте киберготовности

Институт киберготовности (CRI) — это инициатива, объединяющая лидеров бизнеса из разных секторов и географических регионов для обмена ресурсами и знаниями, которые помогут в разработке бесплатных инструментов кибербезопасности в малых и средних предприятиях. Повышение киберготовности малого и среднего бизнеса повышает безопасность глобальных цепочек создания стоимости.
Узнайте больше на сайте **CyberReadinessInstitute.org**