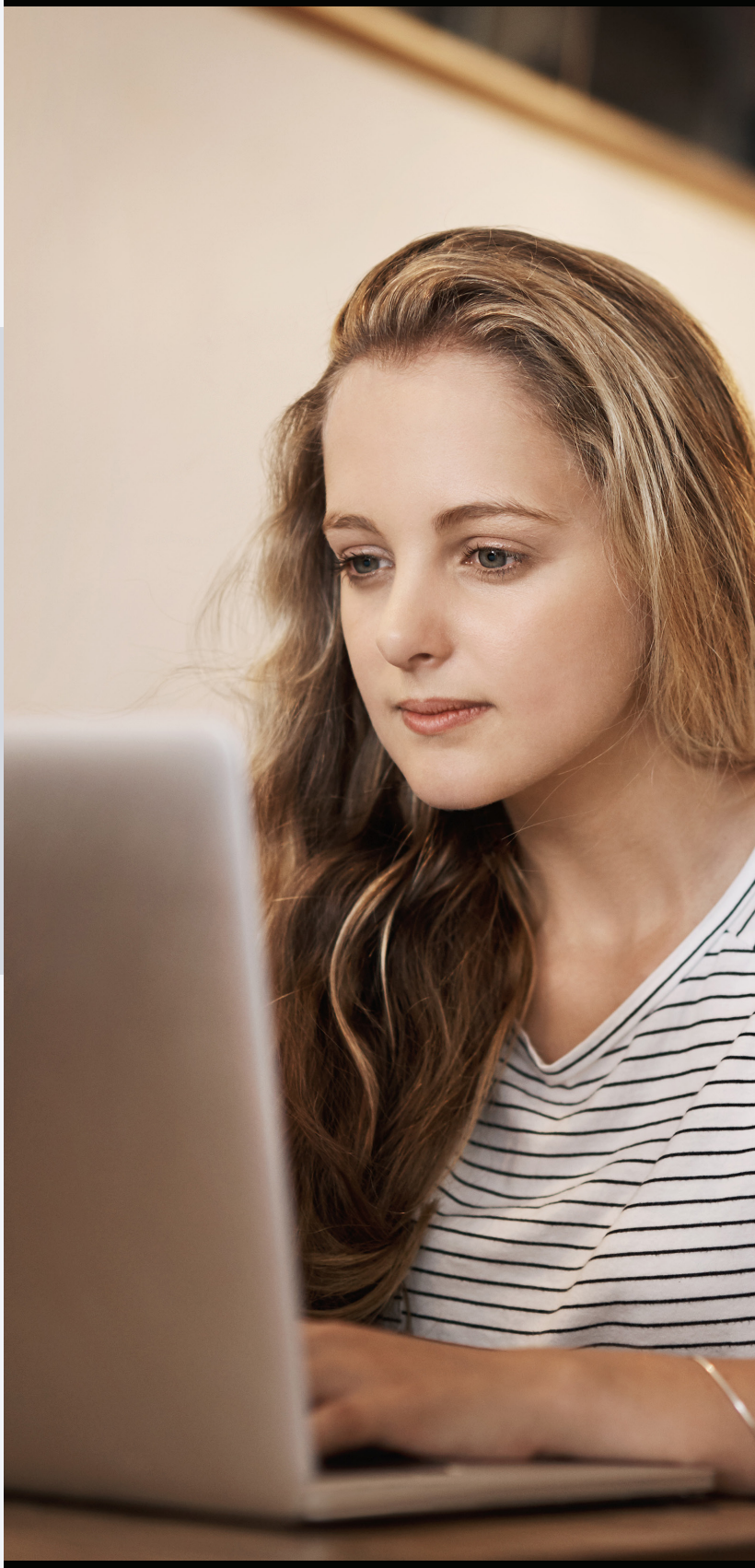
Укрепляем самое слабое звено в первой линии обороны: ваших сотрудников.

IBM Security



Чтобы надежно защитить организацию от киберугроз, нужно запретить сотрудникам открывать электронные письма. Впрочем, такой запрет нерационален, поэтому лучше заняться обучением персонала.

IBM Security Awareness and Training Services

IBM Security предлагает услуги разработки комплексной программы и непрерывной адаптации учебных планов, связанные с осведомленностью о рисках безопасности и фишинге. Эти услуги необходимы для формирования корпоративной культуры осведомленности о рисках. Мы предлагаем программу обучения непрерывной осведомленности, адаптированную согласно потребностям вашей организации.

Фишинг был и остается основным вектором атаки. Наши услуги помогают сотрудникам подготовиться к борьбе с фишингом и социальной инженерией. В процессе подготовки ваших сотрудников мы используем электронное обучение и геймификацию, применяем имитационные модели фишинга и социальной инженерии. Наши опытные консультанты помогут адаптировать платформу к вашим потребностям, предложат методы обучения, показатели, отчетность и средства управления программой, оптимизированные под ваши требования.

Начните сегодня!

Узнайте подробнее о преимуществах программы Security Awareness and Training Program.

Чтобы связаться с подразделением IBM Security Services, перейдите по ссылке **ibm.biz/BdqYUF.**

IBM

Комплексная программа обучения, посвященная осведомленности и обеспечению безопасности поможет смягчить организационные риски.

Пять шагов по развертыванию программы.

1. Четкое определение

- **Определение целей программы**
- **Определение целевой аудитории (охват)**
- **Определение КПЭ**
- **Определение требований к программе и нормативно-правовому соответствию**

2. Разработка

- **Разработка платформы осведомленности о киберугрозах**
- **Создание плана обеспечения осведомленности**
- **Разработка информационных продуктов и учебных руководств**
- **Получение поддержки со стороны руководства компании**

3. Оценка

- **Оценка текущего уровня знаний в области информационной безопасности**
- **Оценка текущего уровня понимания сотрудниками своей роли и своих возможностей в сфере информационной безопасности**

4. Развертывание

- **Проведение интеграции и адаптации согласно индивидуальным требованиям**
- **Проведение тренингов, кампаний, викторин и опросов**
- **Компьютерное обучение и активация клиентов (тенантов)**

5. Измерение

- **Отслеживание и измерение эффективности программы**
- **Создание отчетов по результатам оценки и обучения**
- **Предоставление сопоставимых результатов с использованием эталонных кампаний**

Особенности

- Целевая команда специалистов, занятая непрерывной реализацией программы
- Адаптация и индивидуализация согласно потребностям клиента
- Снижение зависимости от навыков штатных сотрудников
- Официальная программа обучению осведомленности и обеспечению безопасности
- Текущее управление программой

Преимущества

- Помогает сократить количество инцидентов
- Помогает снизить совокупные издержки инцидентов
- Единообразный подход к внедрению в масштабах организации
- Связывает фишинговые тесты в реальном времени с целевым обучением
- Помогает увеличить осведомленность о безопасности и улучшить ее обеспечение, а также изменить поведение сотрудников