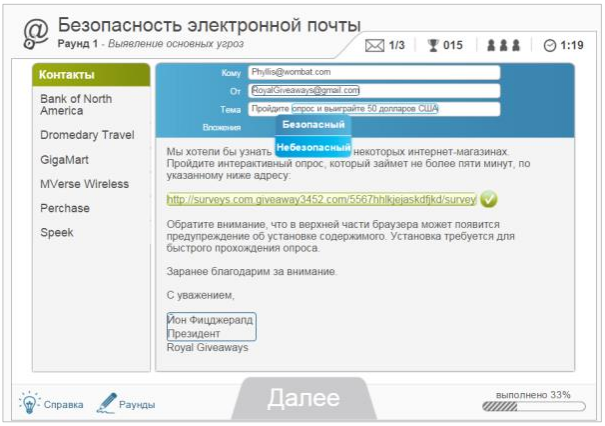
KASPERSKY lab

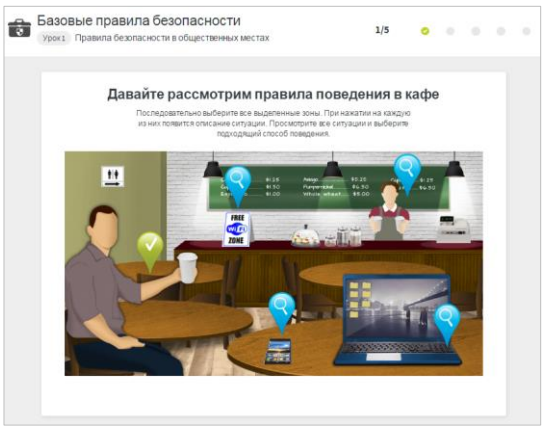
ОНЛАЙН-ПЛАТФОРМА ОБУЧЕНИЯ НАВЫКАМ КИБЕРБЕЗОПАСНОСТИ

ОБЛАЧНАЯ ПЛАТФОРМА ОБУЧЕНИЯ НАВЫКАМ – МОДУЛЬНЫЙ ИНТЕРАКТИВНЫЙ ТРЕНИНГ ДЛЯ ВСЕХ СОТРУДНИКОВ КОМПАНИИ.

Эффективное обучение техническим знаниям и навыкам кибербезопасности большого количества сотрудников организации является насущной необходимостью, поэтому доступ к онлайн-платформе является неоценимым для рассмотрения различных сценариев и ситуаций, понимания потенциальных угроз и способов защиты от них. Ключевые функции онлайн-платформы:

- **Обучающие модули**: Навыки антифишинга, Защита и уничтожение данных, Безопасность в социальных сетях, Физическая безопасность, Безопасность мобильных устройств, Безопасность мобильных приложений, Безопасный просмотр веб-сайтов, Безопасность за пределами офиса, Социальная инженерия, Распознавание мошеннических URL-адресов, Безопасность электронной почты, Пароли.
- **Оценка знаний**: для определения глубины навыков и необходимости обучения пользователей. Оценка знаний покрывает многочисленные домены безопасности, включает заранее подготовленные или случайные опросы, возможность создавать собственные вопросы и выбора длительности оценки.
- **Имитация фишинговых атак**: Готовые шаблоны фишинговых писем, основанные на реальных случаях фишинга, с возможностью настройки и дополнения. Когда сотрудник получает письмо и переходит по ссылке, он видит специальную обучающую страницу – важный этап обучения, и автоматически записывается на соответствующий обучающий модуль.
- **Аналитика и отчеты**: Контроль прохождения тренингов и результатов программ оценки, данные о развитии навыков в различных областях безопасности, как в целом по организации, так и на индивидуальном уровне.





Онлайн-обучение позволяет сотрудникам практиковаться и учиться с помощью интерактивного обучающего портала.

На основе обучающей платформы и руководства по Лучшим Практикам от ЛК, компания может реализовать эффективный, постоянно действующий и измеримый план обучения навыкам кибербезопасности, переводя сотрудников от простых заданий к более сложным, варьируя темы обучения для соответствия изменяющемуся ландшафту угроз и опыту людей.

Интерактивные обучающие модули

- **Основы информационной безопасности** – Определяйте наиболее распространенные проблемы безопасности при выполнении служебных обязанностей и в свободное время.
- **Основы информационной безопасности для руководителей** – Роль менеджеров в распознавании и избегании угроз.
- **Защита данных** – Используйте портативные устройства безопасно, надлежащим образом удаляйте секретные данные
- **Безопасность электронной почты** – Узнайте, как определить фишинговые сообщения электронной почты, опасные вложения и другие обманные сообщения электронной почты.
- **Пароли** – Узнайте, как создать надежные пароли и управлять ими.
- **Безопасное чтение интернета** – Соблюдайте осторожность при работе в интернете, избегая опасных действий и попадания в распространенные ловушки.
- **Безопасность личных данных** – защитите конфиденциальную информацию о вас, вашем работодателе и ваших клиентах.
- **Безопасность мобильных устройств** – Используйте важные физические и технические средства для защиты устройств и данных.
- **Безопасность мобильных приложений** – Узнайте, как оценить безопасность мобильных приложений.
- **Безопасное использование социальных сетей** – Узнайте, как безопасно и ответственно использовать социальные сети.
- **Безопасность за пределами офиса** – Избегайте распространенных ошибок при работе дома или в дороге.
- **Социальная инженерия** – Распознавайте и предотвращайте мошенничество с использованием социотехники.
- **Физическая безопасность** – Узнайте, как защитить людей и их собственность
- **Безопасность платежей в интернете –** Определите признаки опасности и повысьте уровень безопасности данных кредитной карты.
- **Охраняемая медицинская информация –** Узнайте, как и почему следует защищать охраняемую информацию о состоянии здоровья (PHI).
- **URL Training** – Научитесь выявлять мошеннические URL-адреса.
- **Anti-Phishing Phil** – Игровой модуль, который учит определять фишинговые атаки, распознавая поддельные URL-адреса.
- **Anti-Phishing Phyllis** – Игровой модуль, учащий выявлять фишинговые сообщения электронной почты по комплексу признаков.

Доступные конфигурации

Мы предлагаем три основные конфигурации платформы (см. Сравнительную таблицу ниже):

1. Anti-Phishing Suite – Если ваша главная задача – снизить число фишинговых атак,
2. Multi-topic Suite – Если защита от фишинга важна, но не менее важны и другие области безопасности,
3. Полная версия – Все вышеперечисленное, включая возможность управлять обучением и расставлять приоритеты в изучении отдельных вопросов безопасности.

	Anti-Phishing	Multi-topic	Полная версия
Симулированные фишинговые атаки	Да	Да	Да
Автоназначение обучающих модулей	Да	Да	Да
Назначение обучающих модулей в ручном режиме	-	Да	Да
CyberStrength (оценка полученных навыков)	-	-	Да
Сколько тренинговых модулей включено в пакет	3	Все*	Все*
Языковая поддержка **	Полная	Полная	Полная
Срок лицензии	1 год	1 год	1 год

* Все модули, доступные в системе на момент покупки, и добавленные в процессе использования лицензии. На момент подготовки описания – 18 обучающих модулей.

** На момент подготовки описания – 26 языков, включая русский.

Программа повышения осведомленности в области кибербезопасности

CyberSafety Management Games – это один из элементов разработанной “Лабораторией Касперского» Программы повышения осведомленности в области кибербезопасности.

«Лаборатория Касперского» помогает развивать культуру кибербезопасности с помощью набора интерактивных тренингов, основанных на использовании геймификации и других современных методов обучения. Тренинги направлены на каждый из уровней управления в организации и обычно внедряются совместно подразделениями ИБ и HR.

Структура тренингов «Лаборатории Касперского» по повышению осведомленности в области кибербезопасности

ВСЕОБЪЕМЛЮЩАЯ, НО ПРОСТАЯ И ДОХОДЧИВАЯ ПРОГРАММА

- Широкий спектр областей безопасности
- Привычные рабочие места и ситуации
- Увлекательный процесс обучения
- Практические упражнения и опыт
- Язык, понятный непрофессионалам

ЭФФЕКТ ОТ ПРОГРАММЫ

- Сокращение числа инцидентов до 90%
- Уменьшение рисков кибербезопасности на 50-60% в денежном выражении
- Включение в процесс руководителей организации благодаря переводу требований кибербезопасности на понятный язык без IT-терминологии
- Измеримые результаты программы осведомленности