ЗНАНИЯ О КИБЕРБЕЗОПАСНОСТИ В ИГРОВОЙ ФОРМЕ

ИНФОРМАЦИЯ О БЕЗОПАСНОСТИ, ЗАСТАВЛЯЮЩАЯ ДЕЙСТВОВАТЬ

Превратите слабое звено в защитников компании

KASPERSKY lab

ОСВЕДОМЛЕННОСТЬ МОЖЕТ БЫТЬ ЭФФЕКТИВНОЙ

«Старые методы» - Инструкции, Ежегодные презентации, Постеры, Тренинги

Низкая эффективность
Неизмеряемо

Плакатов недостаточно

Отсутствие мотивации и ложные убеждения

Лишь 22% людей считают, что могут стать мишенью киберпреступников.

Тренинги проводятся скучно и вызывают лишь разочарование

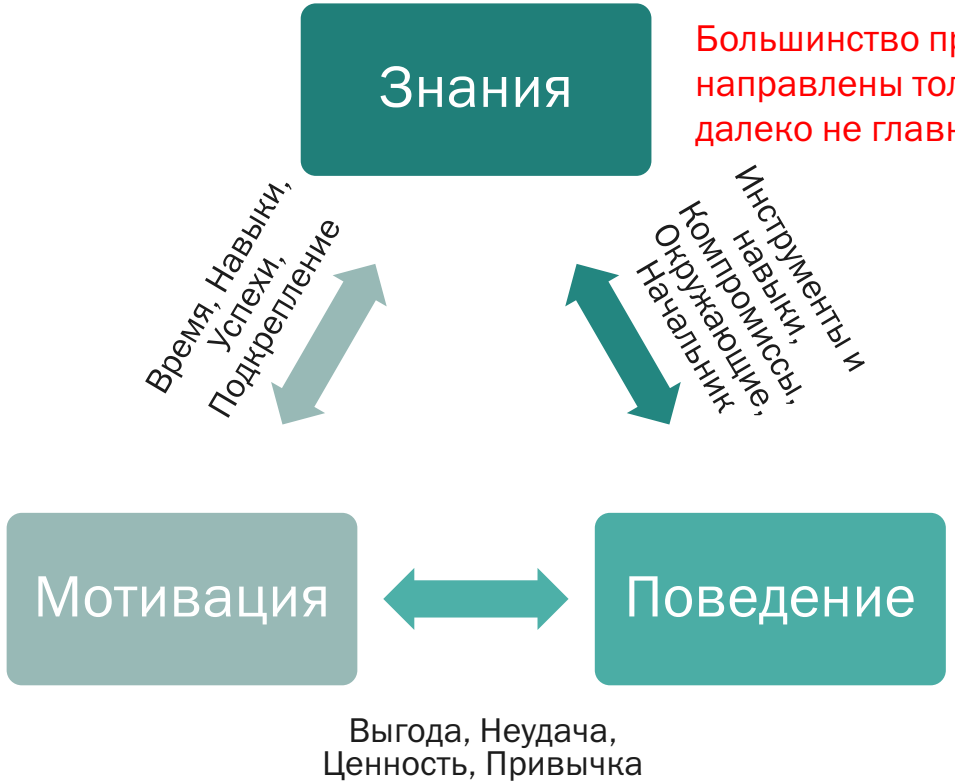
KASPERSKY lab

Обучение на основе игрофикации, с использованием ПК

Высокая эффективность
Измеряемость

- На 90% меньше инцидентов[1)]
- Снижение потерь денег[2)] на 50-60%.
- 37-кратный эффект от инвестиций[3)]

1) Истории успехов (Case Studies)
2) Aberdeen Group, 2014.
3) Ponemon Group Study, 2015



Большинство программ по повышению осведомленности направлены только на передачу знаний, но знания – далеко не главная сила, влияющая на в поведении людей.

Поведение – вот что на самом деле мы пытаемся сформировать, повышая осведомленность. Однако поведение тесно связано как со знаниями, так и с мотивацией.

Подход, который мы предлагаем (CyberSafety Culture),
- эффективен
- измерим

на трех уровнях – знания, поведение, мотивация

ОСВЕДОМЛЕННОСТЬ МЕНЯЕТ ПОВЕДЕНИЕ ЛЮДЕЙ

Какого поведения мы ожидаем от людей после «программы повышения осведомленности»?

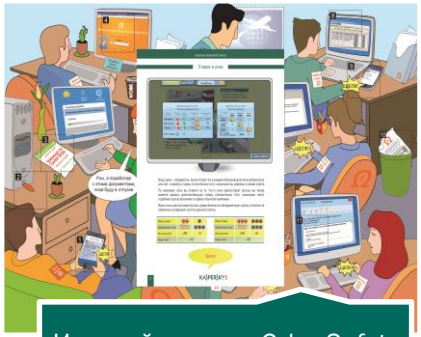
Руководство бизнес-подразделений	Сотрудничество с отделом IT-безопасности Принятие ответственности за кибербезопасность
Линейные руководители	Создание безопасной информационной среды Контроль за соблюдением правил кибербезопасности сотрудниками
Сотрудники	Принятие принципов кибербезопасности Соблюдение правил кибербезопасности Сообщение о потенциально опасных ситуациях Сотрудничество с отделом IT-безопасности

Методика повышения осведомленности в области кибербезопасности CyberSafety Culture, разработанная «Лабораторией Касперского», основана на программах промышленной безопасности, которыми пользуются DuPont, BP, Shell, Siemens и миллионы предприятий по всему миру.

KASPERSKY lab

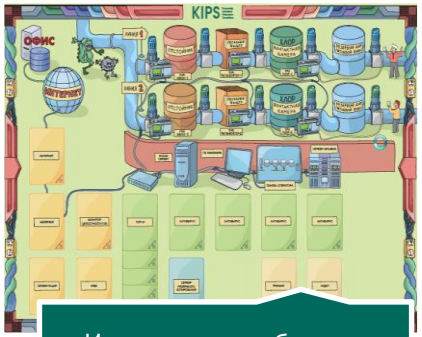
ПОРТФОЛИО CYBER SAFETY CULTURE

Платформа обучения навыкам



Игровой тренинг CyberSafety Games

Оценка культуры кибер-безопасности



Интерактивная бизнес-симуляция KIPS

	Знания	Поведение	Мотивация
На кого направлено	Все сотрудники	Линейные руководители	Руководители
Обучение	√ Платформа интернет-обучения (обучающие модули)	√ Игровой тренинг CyberSafety Games	√ Интерактивная бизнес-симуляция KIPS
Измерение результатов	√ Платформа интернет-обучения (программа оценки CyberStrength)	√ Платформа интернет-обучения (имитация атак PhishGuru)	√ Оценка культуры кибербезопасности

KASPERSKY lab

1. КОМПЬЮТЕРНАЯ ПЛАТФОРМА ОБУЧЕНИЯ НАВЫКАМ

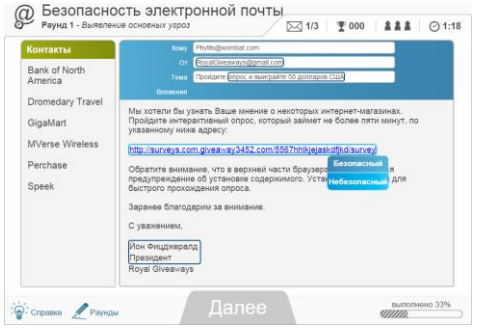
Модули интернет-обучения навыкам

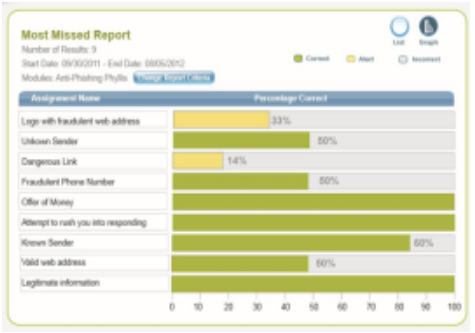
+

- Имитация фишинговых атак
- Оценка навыков
- Анализ и отчеты

Каждому сотруднику в течение года назначаются различные краткие интерактивныхе модули интернет-обучения, иимитационные атаки и опросы по оценке знаний. Программа обучения управляется отделом ИБ, на основе постоянного измерения эффективности.

16 интернет-тренингов по 15 минут.





Deutsch
Español
français
italiano
日本語
한국어
Nederlands
português
русский
简体中文
繁體中文

На русском, английском и других языках

Облачная платформа с несколькими административными ролями

KASPERSKY lab

2. ИГРОВОЙ ТРЕНИНГ CYBERSAFETY GAMES

Изменение убеждений, мотивация

- Почему нужно ответственно относиться к безопасности?
- Кого необходимо опасаться?

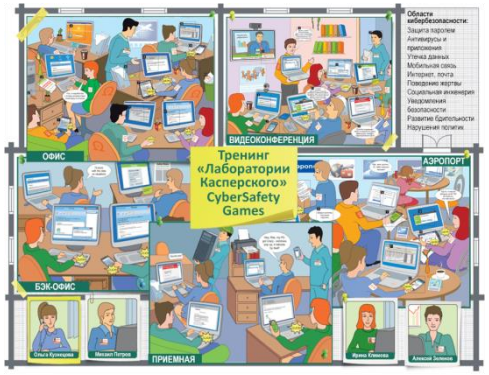
Бдитель-ность

- Различие между опасным и безопасным поведением (развитие бдительности и технических навыков)
- Положительные примеры: «как нужно», а не только «как нельзя»

Безопасность и эффектив-ность – выигрыш на обоих фронтах

- Поощрение сотрудников к обучению и сотрудничеству с отделом IT-безопасности (безопасность не мешает эффективности, концепция «добровольных дружин»).

10 областей безопасности – антивирусы и приложения, утечка данных, мобильная связь, интернет, почта, характерное поведение жертвы, социальная инженерия, уведомления безопасности, развитие бдительности, нарушения политик, социальные сети.
Типичные рабочие места – в офисе, в дороге, в конференц-зале



Руководители отделов и подразделений

Люди, влияющие на отношение подчиненных к кибербезопасности в повседневной работе

Игровая среда

Поощрение соревновательного духа и обучения на собственном опыте.

Однодневный тренинг у клиента, проводимый специалистом «Лаборатории Касперского», 20–50 человек.

KASPERSKY lab

МОТИВАЦИЯ = СМЕНА УБЕЖДЕНИЙ

1. Преобразуйте заблуждения по поводу кибер-безопасности

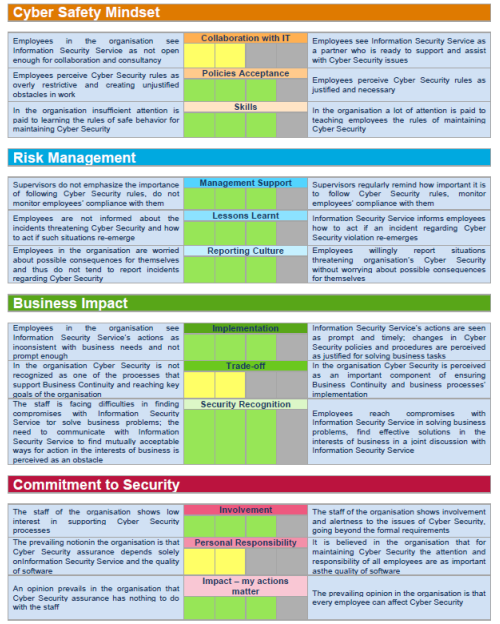
2. В адекватное восприятие реальности

3. И покажите позитивные модели поведения

«Вирус сломает мой компьютер»	*«Я слишком мал для мишени»*	*«Нет времени на заботу о безопасности»*
Опасаться нужно злоумышленников, а не сломанных компьютеров	Жертвами становятся не только те, на кого направлена непосредственная атака	Безопасность необходима для эффективной работы
Думайте, кто может воспользоваться вашими действиями	Станьте менее уязвимым, чем другие	Сотрудничайте с отделом IT-безопасности

3. ОЦЕНКА КУЛЬТУРЫ

Оценка культуры кибербезопасности анализирует реальное повседневное поведение и отношение к безопасности сотрудников предприятия на всех уровнях управления. Это позволяет директору по IT-безопасности обнаружить проблемные зоны и области, требующие внимания.



По результатам оценки можно предметно обсудить с руководством роль и место кибербезопасности в обеспечении эффективной работы организации.

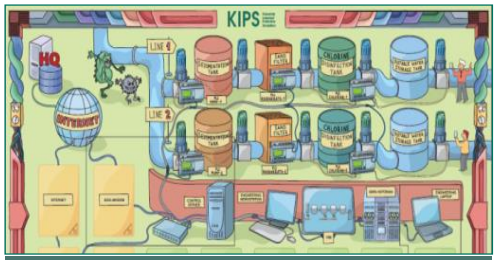
Интернет-опрос. Занимает у сотрудника около 15 минут. Консолидированный отчет.

KASPERSKY lab

4. ИНТЕРАКТИВНАЯ БИЗНЕС-СИТУЛЯЦИЯ

Стратегическая игра, посвященная кибербезопасности. Предназначена для руководителей IT-отдела, коммерческих отделов и службы ИБ.

- Командная работа способствует сотрудничеству специалистов из различных областей.
- Соревновательные элементы развивают инициативу и аналитические навыки.
- Игровая среда позволяет глубже понять меры и стратегию кибербезопасности.



Сценарий для завода по очистке воды.

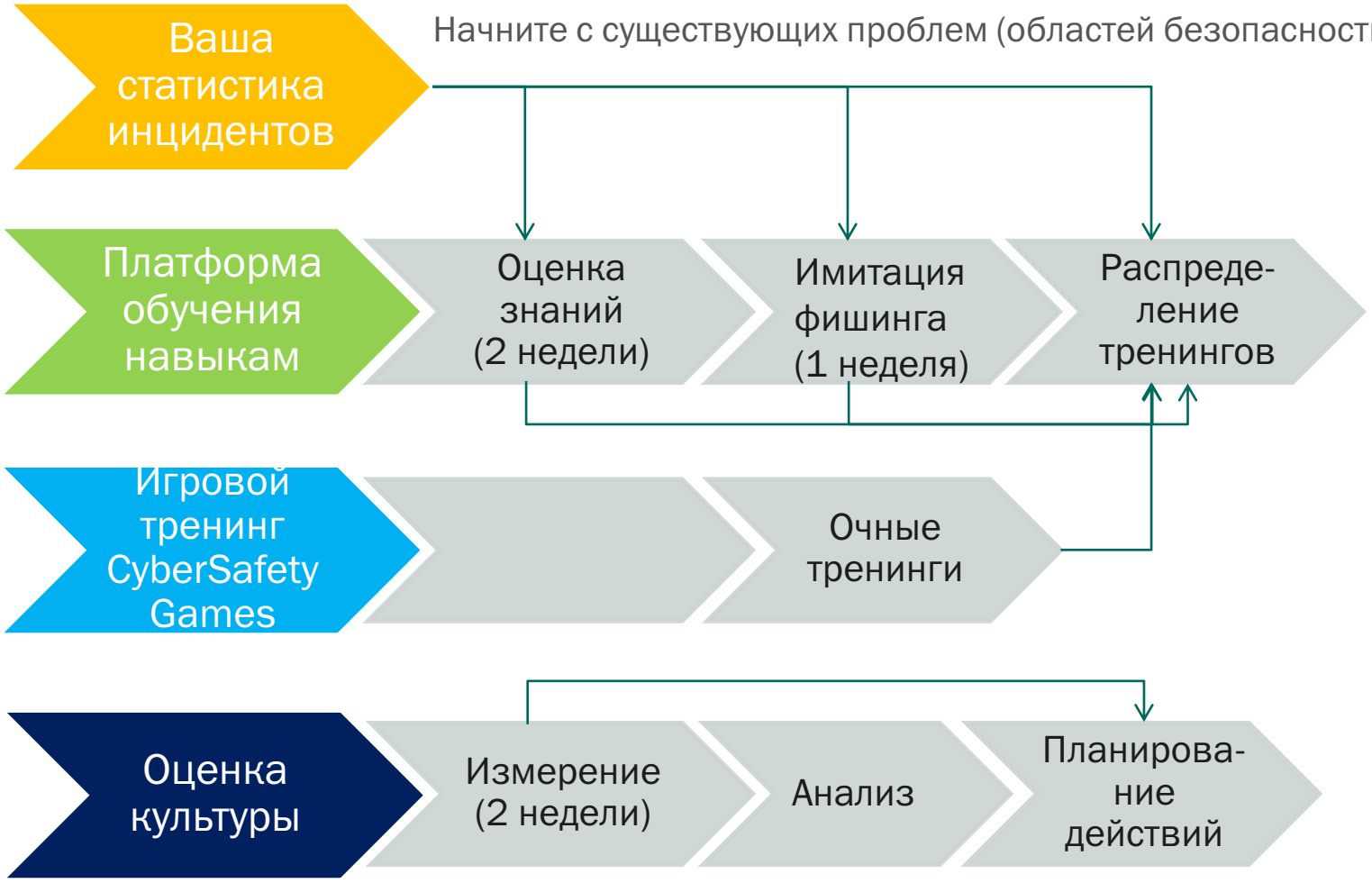
Команды соревнуются, управляя виртуальными компаниями и зарабатывая деньги.
Когда компания подвергается кибератаке, команда видит последствия: снижение производительности и доходов компании. Чтобы снизить негативное влияние и увеличить прибыль, приходится использовать различные бизнес- и IT-стратегии.

- Интересная, увлекательная и динамичная игра (2 часа).
- Не требует глубоких технических знаний.

KASPERSKY lab

СЛАЖЕННАЯ РАБОТА ВСЕХ ЭЛЕМЕНТОВ

Развертывание и запуск в течение месяца



Мы предоставляем руководство по рекомендованным практикам и техническую поддержку

KASPERSKY lab

МЕТОДОЛОГИЯ НЕПРЕРЫВНОГО ОБУЧЕНИЯ

Обучение продолжается в течение года, цикл за циклом

Мы предоставляем руководство по рекомендованным практикам и техническую поддержку

KASPERSKY lab

ИЗМЕРЯЕМАЯ ОСВЕДОМЛЕННОСТЬ

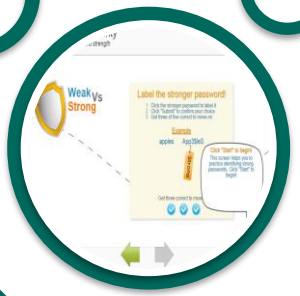
Постоянное измерение успехов

КОНКРЕТНЫЕ РЕЗУЛЬТАТЫ

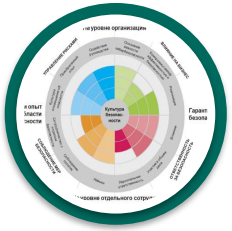
Эффект

- Сокращение количества инцидентов – до 90%
- Уменьшение рисков на 50–60% в денежном выражении[1)]
- Включение в процесс руководителей организации благодаря переводу требований кибербезопасности на понятный язык без IT-терминологии
- Измеримые результаты программы осведомленности

Тренинг CyberSafety Games
для руководства



Платформа интернет-обучения навыкам
для всех сотрудников



Оценка культуры кибербезопасности

Aberdeen Group. Исследование 2014 г.

KASPERSKY lab

Подробное описание

1. Игровой тренинг CyberSafety Games (стр.2)
2. Платформа обучения навыкам (стр. 13)

ПОДРОБНОЕ ОПИСАНИЕ CYBERSAFETY GAMES

Организация тренинга:
В большой аудитории собираются 50–100 человек, которые делятся на соперничающие друг с другом команды.
Им раздают обучающие материалы: игровые поля, фишки, планшеты iPad с приложением CyberSafety Games.

В процессе игры команды перемещаются по виртуальному предприятию, изучая каждую комнату в поисках всевозможных лазеек для киберугроз.

После обнаружения всех источников опасности участники учатся их обезвреживать.

KASPERSKY lab

РАБОЧИЕ МЕСТА

Каждое рабочее место содержит 12 размеченных зон

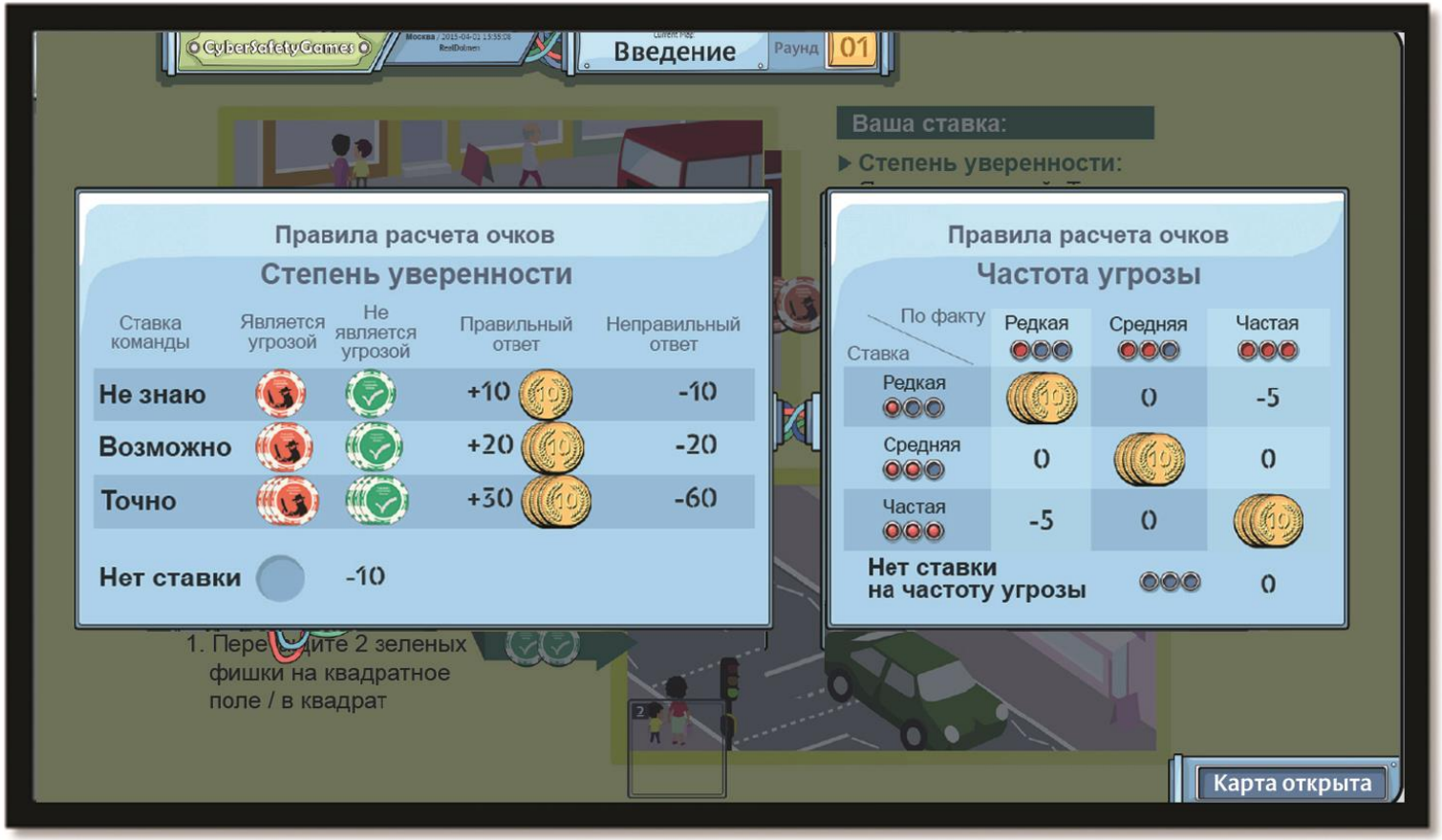
ПОТЕНЦИАЛЬНЫЕ УГРОЗЫ

Зоны на карте содержат потенциальные угрозы кибербезопасности

10 областей безопасности – антивирусы и приложения, утечка данных, мобильная связь, интернет, почта, характерное поведение жертвы, социальная инженерия, уведомления безопасности, развитие бдительности, нарушения политик, социальные сети.

KASPERSKY lab

ИГРОВАЯ СРЕДА

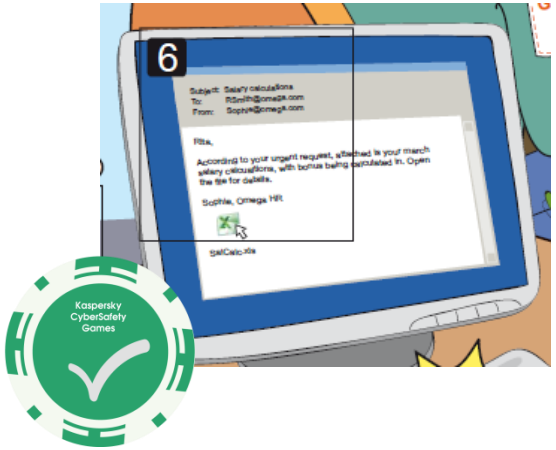


Полагаясь на свои знания, участники CyberSafety Games делают «ставки» на зоны потенциальных киберугроз и рискуют своей репутацией, чтобы добиться максимального результата в соревновании.

KASPERSKY lab

РАЗНООБРАЗИЕ

Некоторые зоны содержат угрозы, а некоторые – нет. Иногда «хорошие» и «плохие» зоны относятся к одной области безопасности



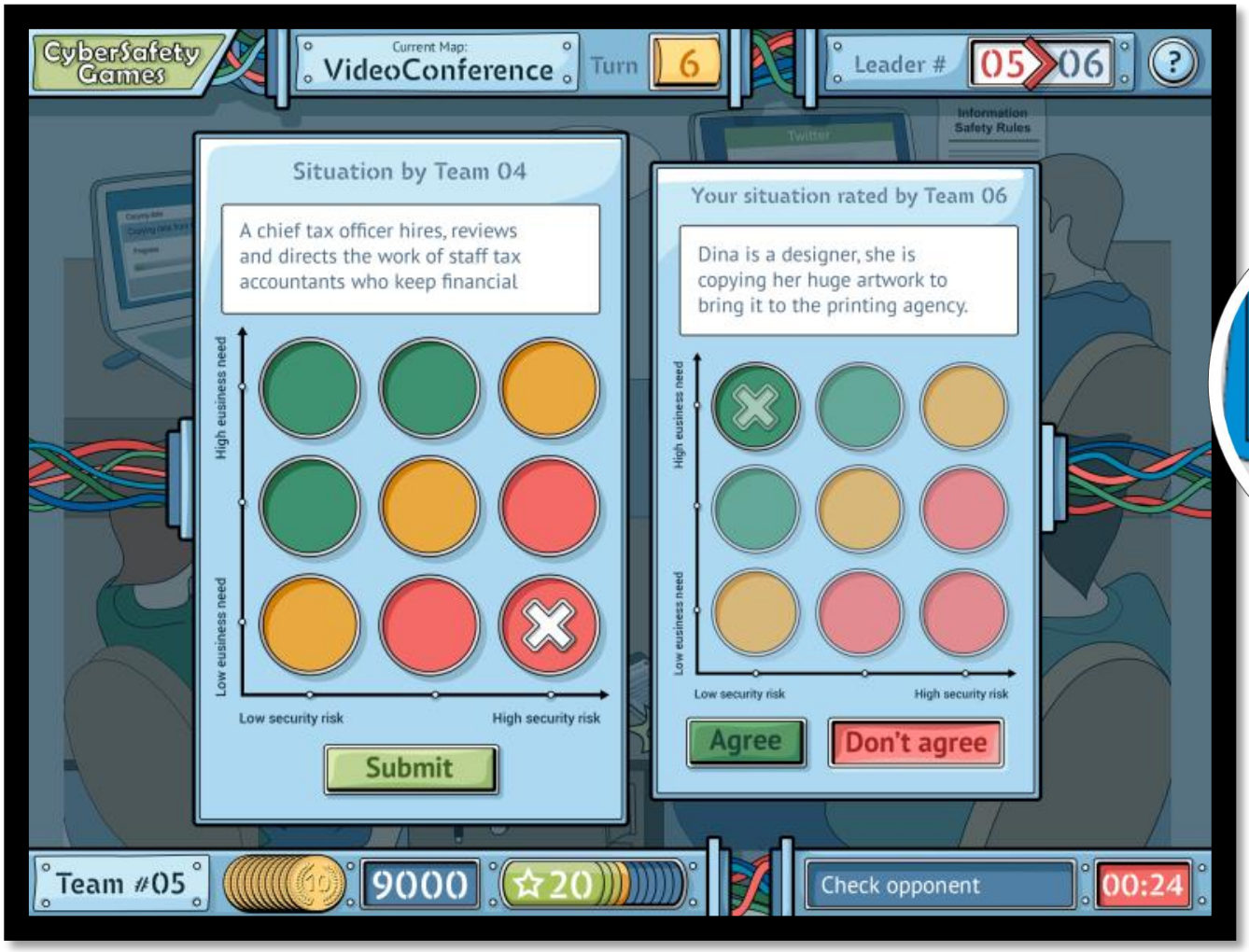
KASPERSKY lab

УПРАЖНЕНИЯ

Для каждой обнаруженной угрозы команды предлагают комплекс действий, которые можно выполнить на рабочем месте для снижения или исключения риска. За это участникам начисляют игровые очки.

Затем ведущий рассказывает, какой тактики рекомендуется придерживаться в данной ситуации за своим рабочим компьютером.

УПРАЖНЕНИЯ



Участники выполняют упражнения, которые учат принимать ответственные решения, оценивая различные ситуации из повседневной жизни предприятия с точки зрения безопасности и эффективности работы.

KASPERSKY lab

УПРАЖНЕНИЯ

Платформа интернет-обучения предлагает пошаговые упражнения для развития технических навыков (например, как заметить вредоносную почту, на что обращать внимание и как рассуждать), а также мультипликационные ролики, интерактивные элементы, тесты и теоретическое руководство в коротких 15-минутных модулях.

KASPERSKY lab

УПРАЖНЕНИЯ

Платформа интернет-обучения охватывает множество технических навыков и областей. На платформе описываются ситуации из реальной жизни, которые участники могут прокомментировать, а также услышать мнение профессионалов по реальному состоянию безопасности. Чтобы участники учились на собственном опыте, им предлагается предпринять те или иные шаги.

KASPERSKY lab

УПРАЖНЕНИЯ

Участники разыгрывают по ролям типичные беседы с сотрудниками IT-безопасности, которые запрещают многое из того, что сотрудникам хотелось бы делать, ссылаясь на уязвимости системы безопасности. Участники разыгрывают по ролям типичные беседы с сотрудниками IT-безопасности, которые, ссылаясь на уязвимости системы безопасности, запрещают многое из того, что сотрудникам хотелось бы делать.] В ходе этих переговоров участники тренинга понимают, что, правильно обсуждая вопросы со специалистами по IT-безопасности (то есть объясняя настоящие потребности и вместе работая над возможными решениями), обычно можно найти взаимовыгодный вариант: и эффективный, и безопасный.

KASPERSKY lab

ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ ТРЕНИНГА

«Лаборатория Касперского» предоставляет	Клиент обеспечивает
• Материалы для участников (игровые поля, фишки) и программное обеспечение CyberSafety Games • Квалифицированного тренера • Раздаточные материалы для участников	• Помещение, компьютеры, аудио- и видеооборудование, доступ к интернету • Еду и напитки • Приглашение и регистрацию участников

KASPERSKY lab

Подробное описание

Платформа обучения навыкам

KASPERSKY lab

ПЛАТФОРМА ОБУЧЕНИЯ НАВЫКАМ

Запись на модули

Сотрудников можно записывать на различные модули или программы обучения в зависимости от их профиля, отдела, результатов предыдущих оценок или времени, пройденного после предыдущих тренингов…

KASPERSKY lab

ПОДРОБНЕЕ О ПЛАТФОРМЕ ОБУЧЕНИЯ НАВЫКАМ

Интернет-платформа для каждого сотрудника

Навыки антифишинга

Обнаружение фишинговых атак по мошенническим URL-адресам.

Правила антифишинга

Обнаружение фишинговых писем по характерным «красным флажкам».

Защита и уничтожение данных

Безопасное пользование портативными носителями и надежное удаление конфиденциальных данных

Безопасность электронной почты

Обнаружение фишинговых писем, опасных вложений и других попыток мошенничества по электронной почте.

Безопасность мобильных устройств

Использование физических и технических средств для защиты устройств и данных.

Информация, позволяющая установить личность

Защита конфиденциальной информации о себе, работодателе и клиентах

Пароли

Создание и хранение надежных паролей.

Физическая безопасность

Защита персонала и имущества.

Информация о состоянии здоровья

Почему и как нужно защищать информацию о состоянии здоровья

Безопасность в социальных сетях

Ответственный подход к использованию социальных сетей.

Безопасный просмотр веб-сайтов


Безопасная работа в интернете: отказ от рискованных действий и избегание распространенных «ловушек».

Безопасность за пределами офиса

Предупреждение распространенных ошибок, нарушающих безопасность при работе из дома или в дороге

Основные правила безопасности

Учет вопросов безопасности в повседневных операциях.

Социальная инженерия

Обнаружение и избегание попыток мошенничества.

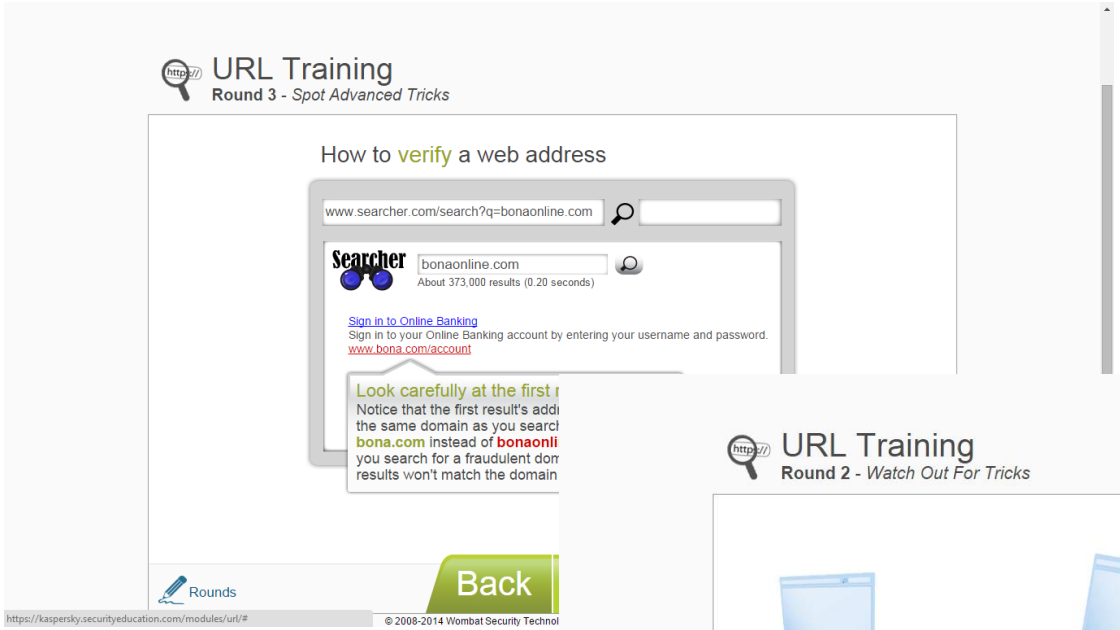
Распознавание URL-адресов

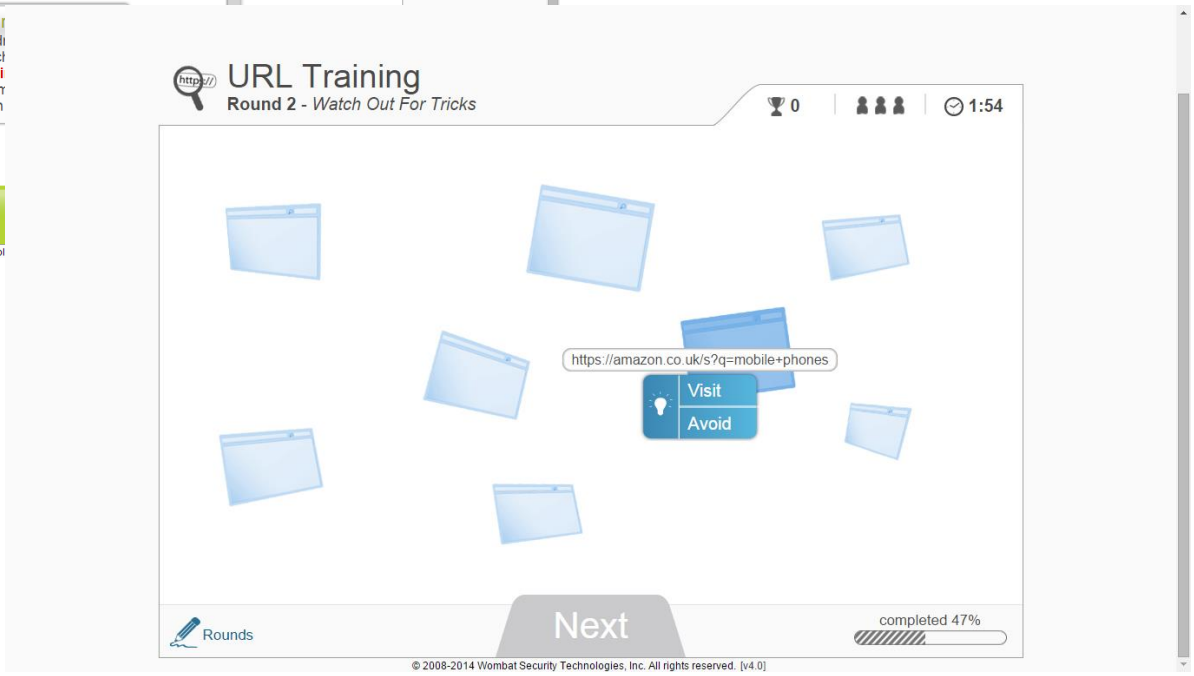
Обнаружение мошеннических URL-адресов

KASPERSKY lab

ПЛАТФОРМА ОБУЧЕНИЯ НАВЫКАМ

В каждый обучающий модуль входит теоретическая часть…





…и упражнения для обучения на собственном опыте

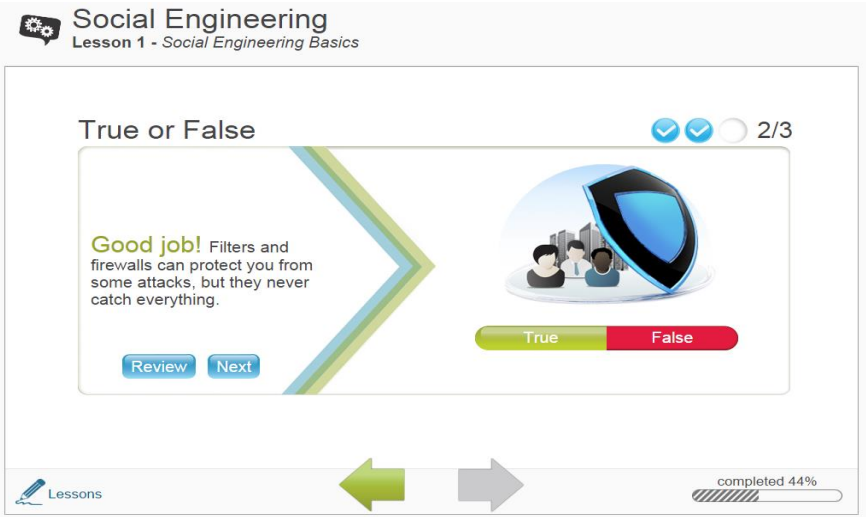
Короткие занятия около 15 минут

KASPERSKY lab

ПРИНЦИПЫ ОБУЧЕНИЯ

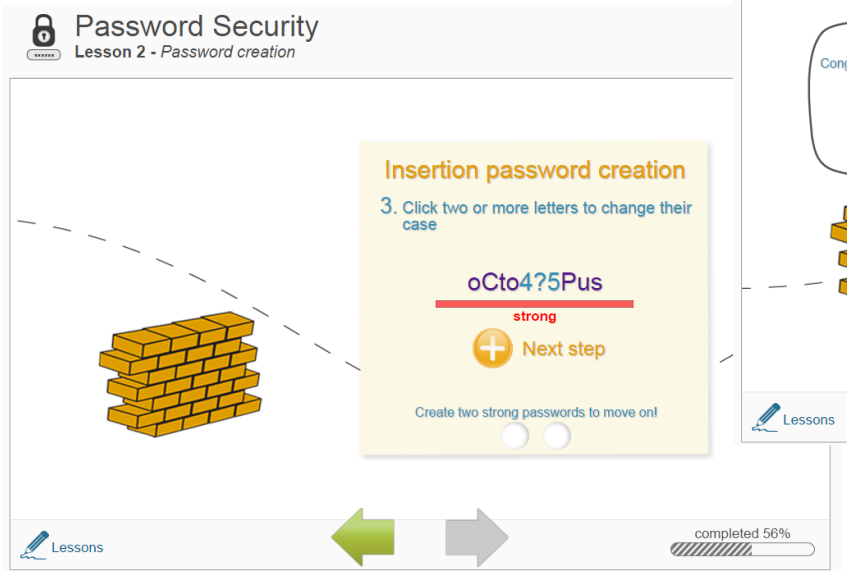
Сочетание теоретических разъяснений, тестов и самостоятельно выполняемых упражнений с подсказками и отзывами…

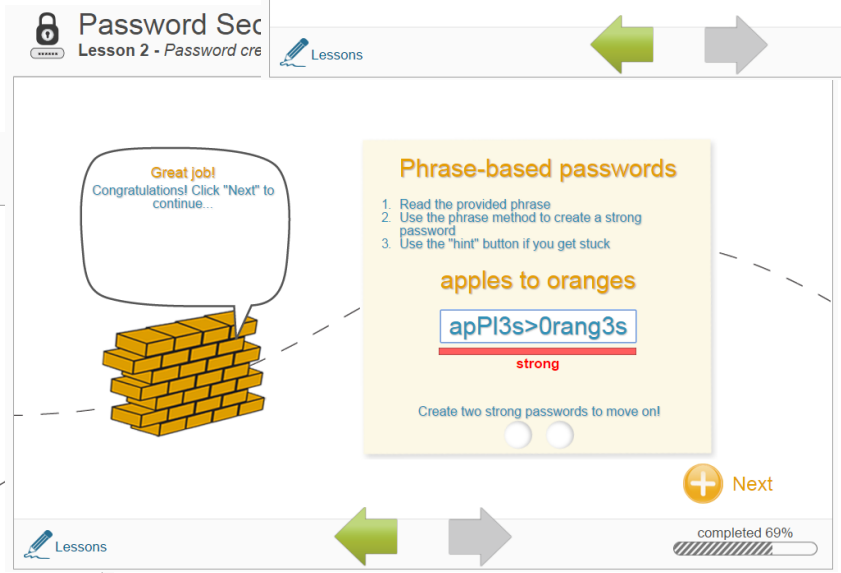
…гарантирует эффективность обучения



ШАГ ЗА ШАГОМ

Обучающий модуль по каждой теме строится по принципу «от простого к сложному»

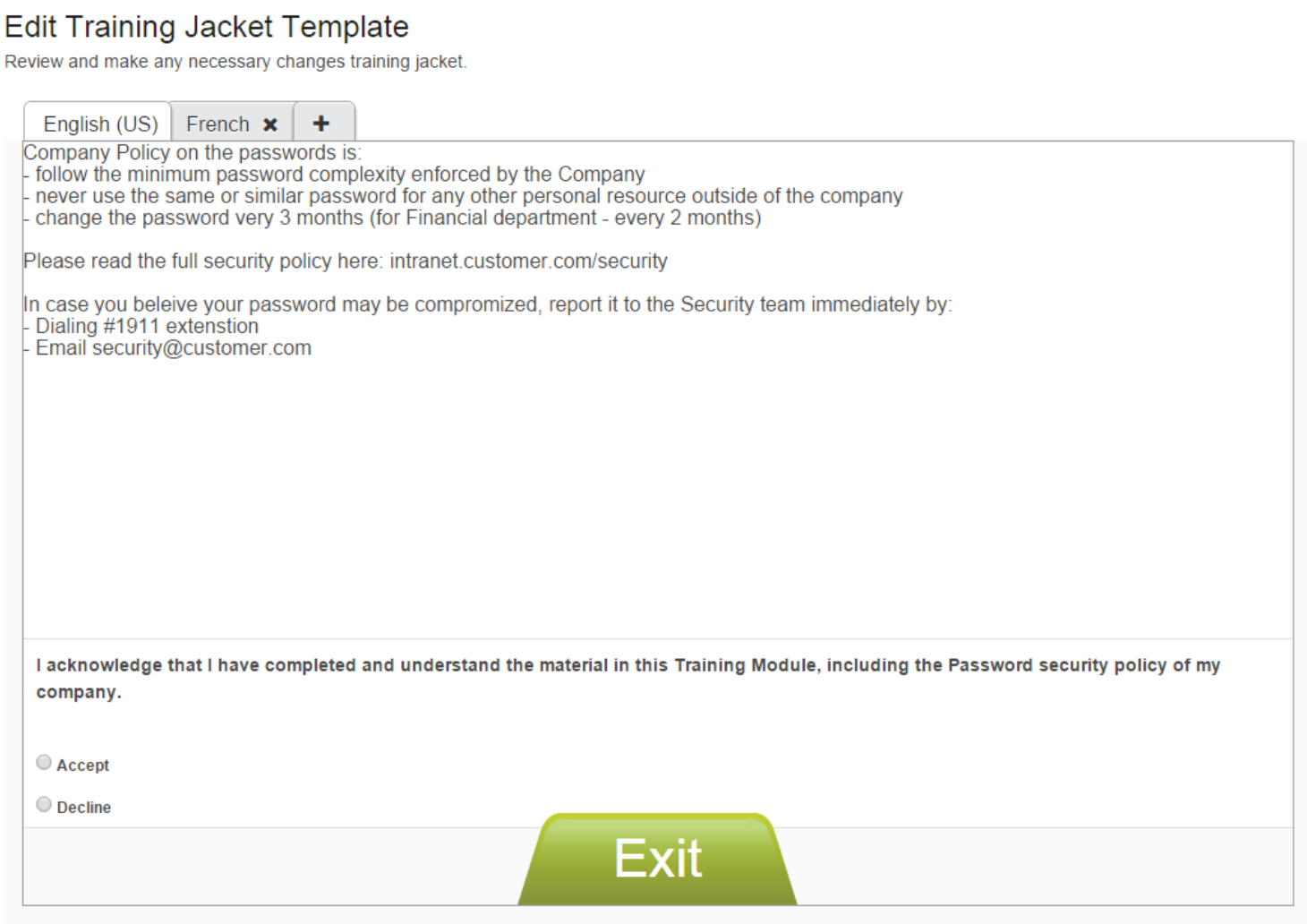




KASPERSKY lab

ПОДПИСАНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ

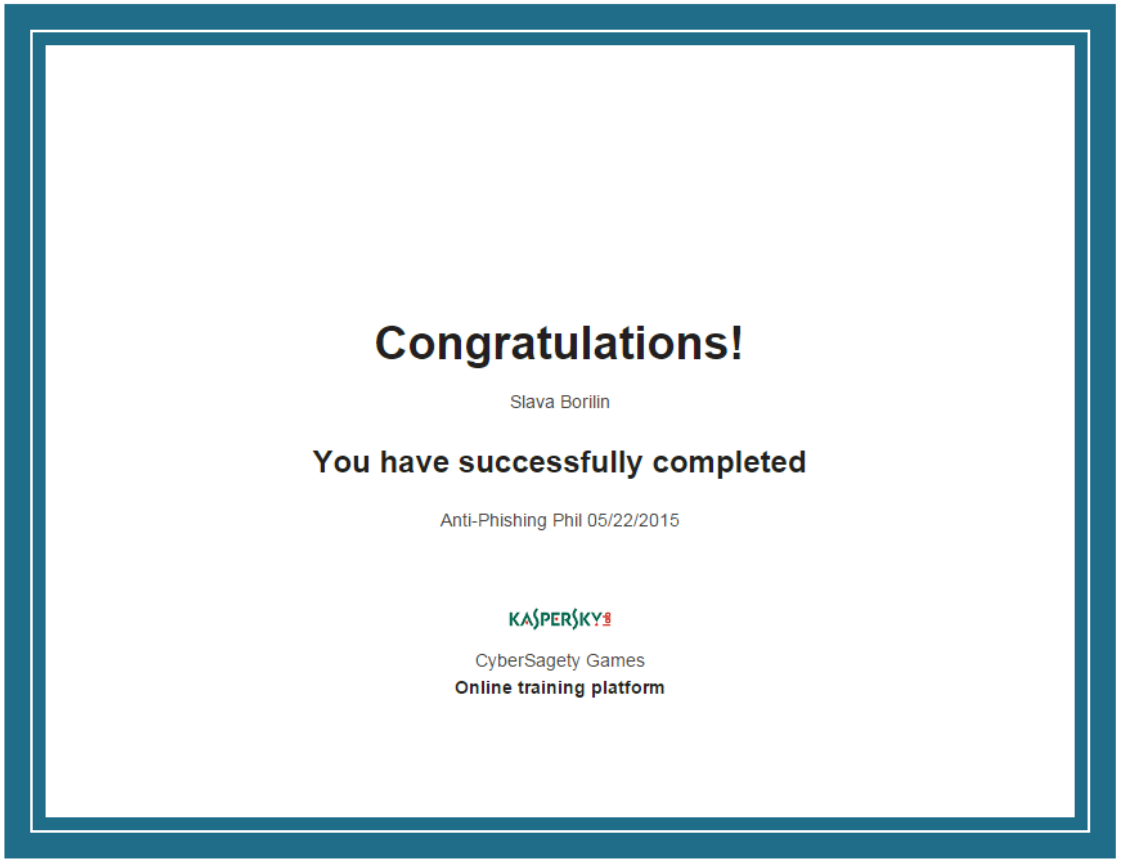
В конец обучающих модулей можно добавить информацию о политике безопасности, ссылки и контакты отдела IT-безопасности



KASPERSKY lab

СЕРТИФИКАТЫ

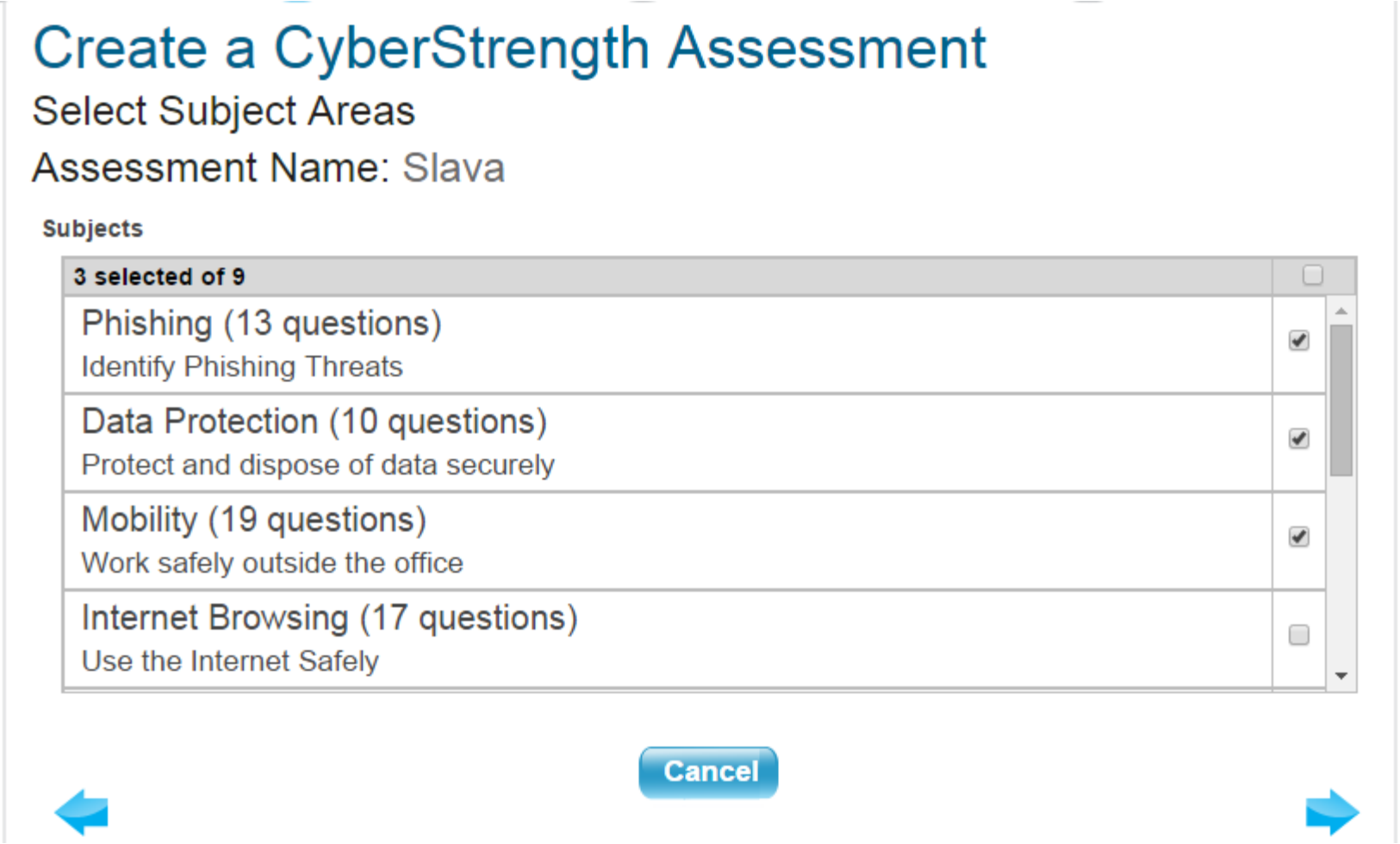
После обучения пользователь может получить фирменный сертификат



KASPERSKY lab

Программы оценки

Определение продолжительности курса и областей безопасности



Интерактивные вопросы

Интерактивные вопросы

Имитация фишинговых атак

Готовые шаблоны

KASPERSKY lab | Security Education Platform

Select Attack Category

Select the category below which most closely matches the type of

1 OF 1

Category	Description
Personal	Scams about your personal accounts
Social Network	Scams About Social Networks
Work Related	Scams involving work related accounts or information
Attachments	Scams asking a user to open an attachment
New Templates	Recently added phishing attacks
Logistics	Scams focusing on package delivery
Seasonal	Scams focusing on seasonal events
Financial	Scams About Your Bank
Custom	Create your own email from scratch

На основе реальных случаев фишинга
Разный уровень сложности

Select Attack : Work Related

Select a phishing attack from the list below:

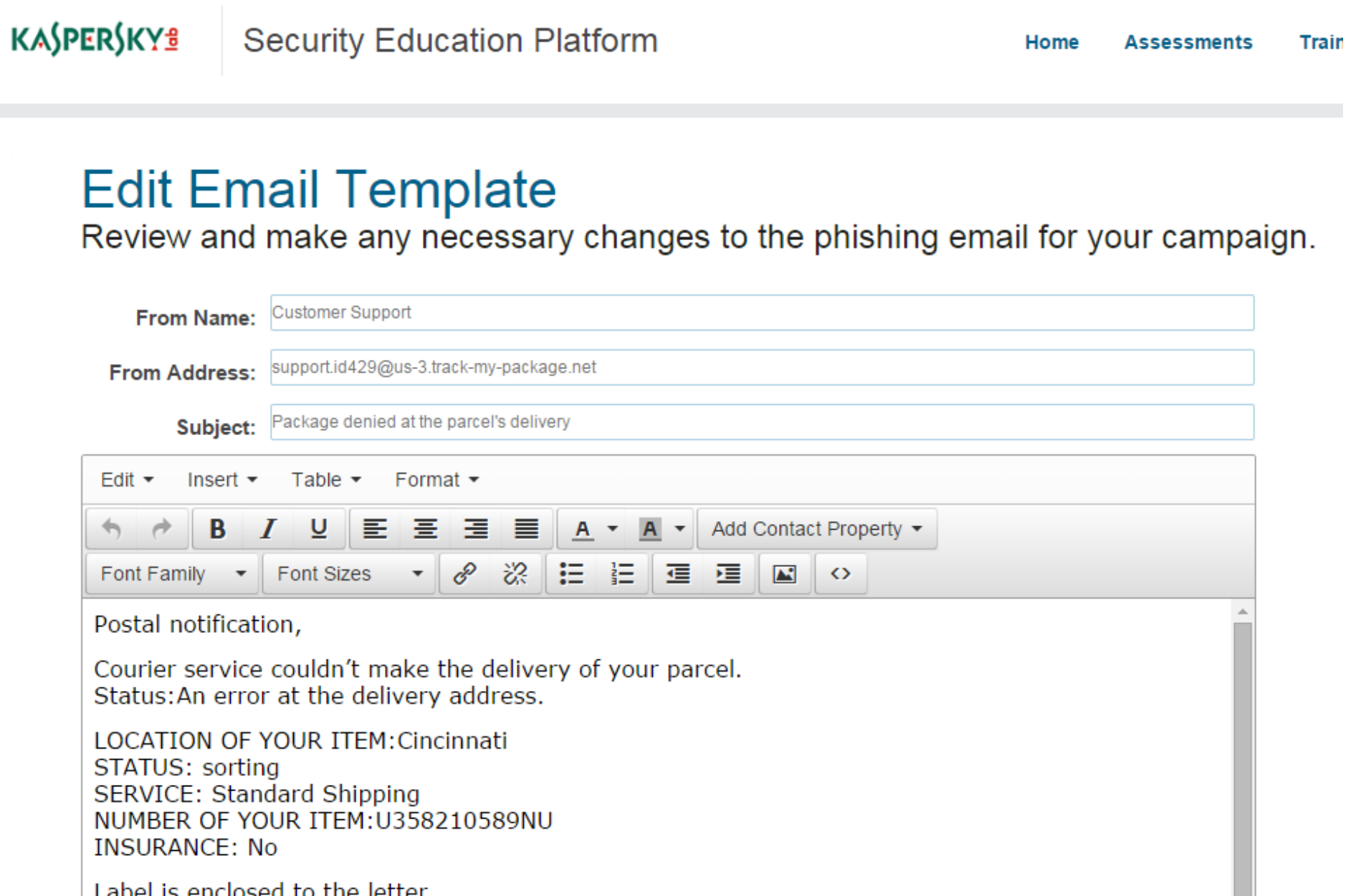
Language: French

1 OF 1

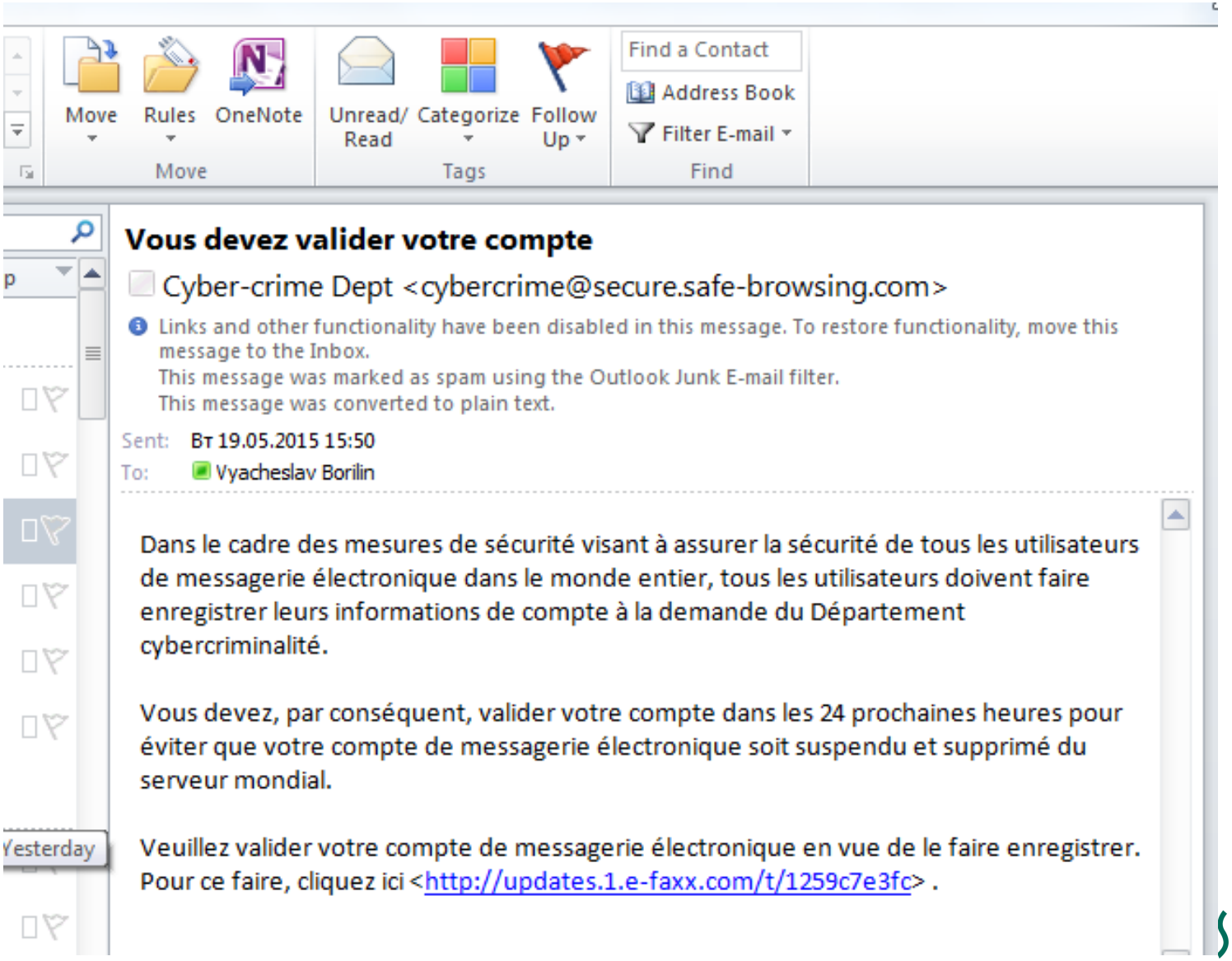
Name	Description	Failure Rate
Corporate e-Faxx message	The user receives a 5 page e-Faxx message containing a PDF link.	25.53 %
Email Improvements	Tells the user that there is a more secure email system and they must click to not lose access.	7.88 %
Email Password Change	Warns the user that their password is about to expire and if they don't change it they will lose access to email.	20.93 %
Email Quota Alert	Warns users their email has run out of space and they may not receive email unless they click a link.	19.24 %
NetworkMeet account suspended	Claims that the user's NetworkMeet account is disabled, they must click to reactivate.	8.94 %
Voicemail Alert	Tries to get the user to click on a link by looking like an automated voicemail alert.	30.03 %

KASPERSKY lab

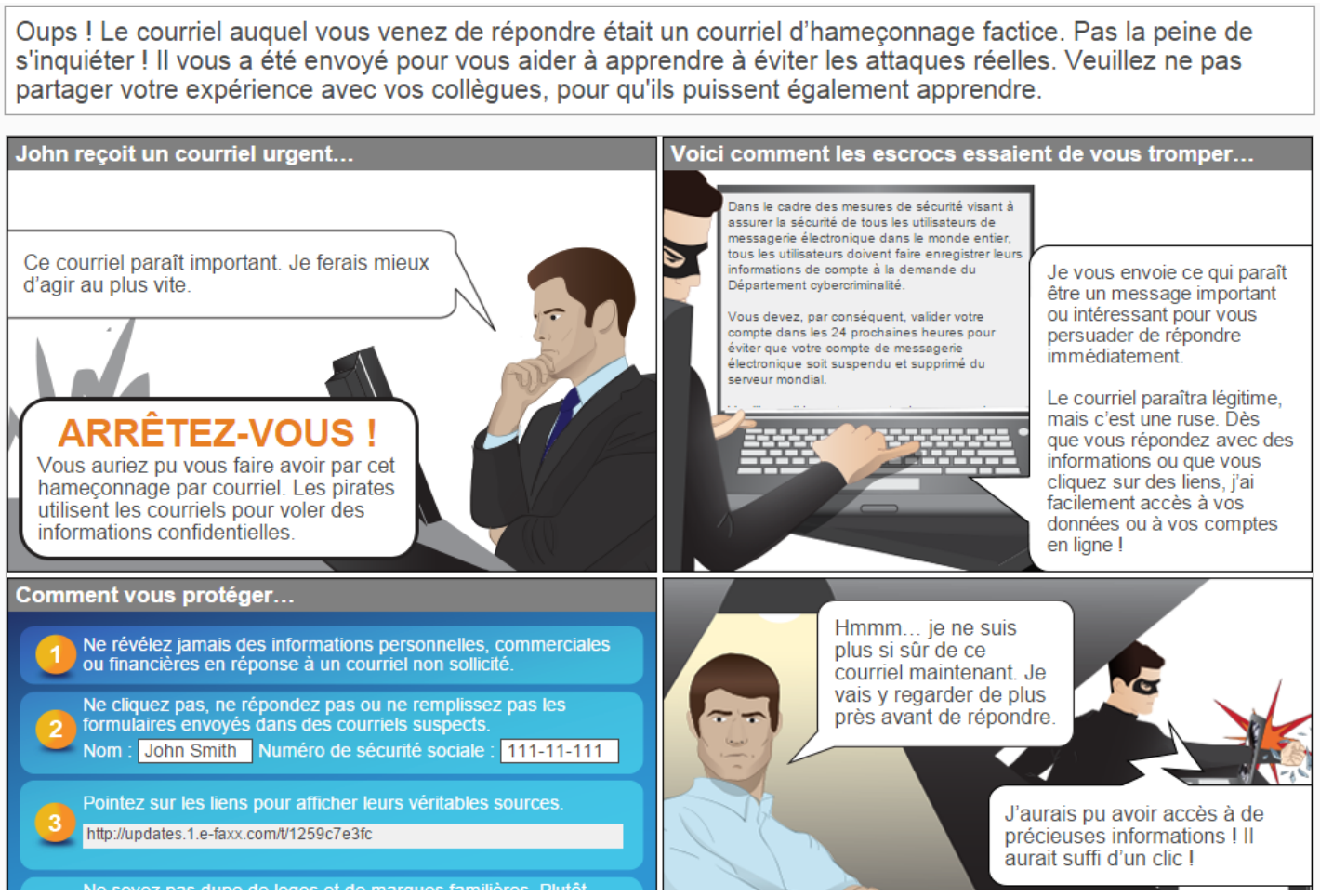
Удобная настройка



Сотрудник получает фишинговое письмо и переходит по ссылке…



Открытие фишинговой страницы – важный этап обучения
Автоматическая запись на тренинги
Статистика



Анализ и отчеты

ОТЧЕТЫ

- Assignment Details
- Most Missed Report
- Module Performance
- Module Completion Summary
- Policy Acknowledgement
- User Report Cards
- User Record Export

- CyberStrength Assessment
- CyberStrength Risk

PhishGuru

- Archived Campaigns
- Campaigns Report
- Contact Groups
- Device Type
- Repeat Offenders
- Twelve Month Trend

ПЛАТФОРМА ОБУЧЕНИЯ НАВЫКАМ

Контроль прохождения тренингов и результатов программ оценки

KASPERSKY lab

ПЛАТФОРМА ОБУЧЕНИЯ НАВЫКАМ

Данные о развитии навыков в различных областях безопасности, как в целом по организации, так и на индивидуальном уровне

CyberStrength Assessment Report

XYZ Company (DC)

CyberStrength Assessment Report

Assignment: Baseline Knowledge Assessment - CYB

Change Report Criteria

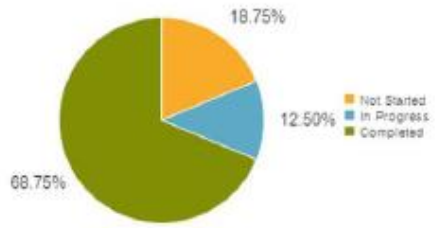
General Information

Overall Score: 85%

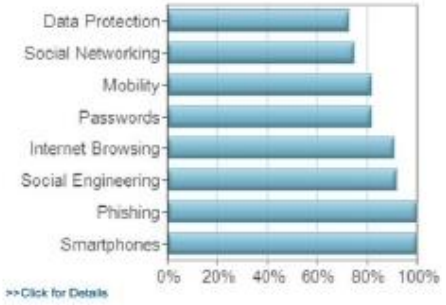
Number of Users: 16
Total Number of Questions: 10
Question Generation Type: Administrator Defined

Subject	Number of Times Asked
Data Protection	22
Internet Browsing	11
Mobility	11
Passwords	22
Phishing	12
Smartphones	12
Social Engineering	12
Social Networking	12

Assessment Status



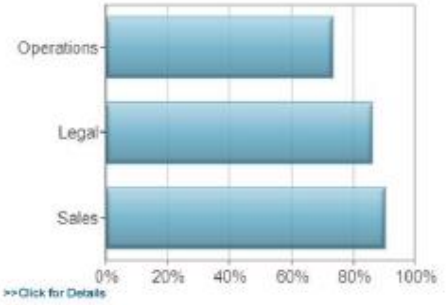
Score By Category



>>Click for Details

Export to Excel

Score By Group



>>Click for Details

Export to Word

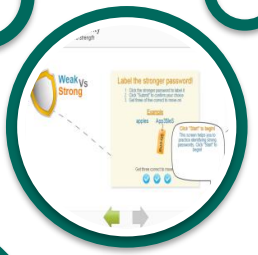
KASPERSKY lab

«Лаборатория Касперского» предоставляет	Клиент обеспечивает

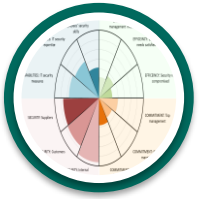
• Учетную запись для интернет-платформы
• Обучение администраторов
• Техническую поддержку
	• Загрузку почтовых ящиков сотрудников в платформу
	• Создание программ:
	  • имитации атак
	  • оценки
	  • обучения
	• Запись групп на обучающие модули
	• Анализ результатов

ЗАКЛЮЧЕНИЕ

Игровой тренинг
CyberSafety Games



Платформа
обучения навыкам



Cyber Safety
Culture Assessment

Эффект

- Сокращение количества инцидентов до 90%
- Уменьшение рисков кибербезопасности на 50–60% в денежном выражении[1)]
- Включение в процесс руководителей организации благодаря переводу требований кибербезопасности на понятный язык без IT-терминологии
- Измеримые результаты программы осведомленности

THINK ABOUT IT. WE DO.

THE KASPERSKY LAB TEAM

Aberdeen Group. Исследование 2014 г.

KASPERSKY lab