

# ИНФОРМАЦИЯ О БЕЗОПАСНОСТИ, ЗАСТАВЛЯЮЩАЯ ДЕЙСТВОВАТЬ

*Превратите слабое звено в защитников компании*



«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



Обучение на основе игрофикации,  
с использованием ПК

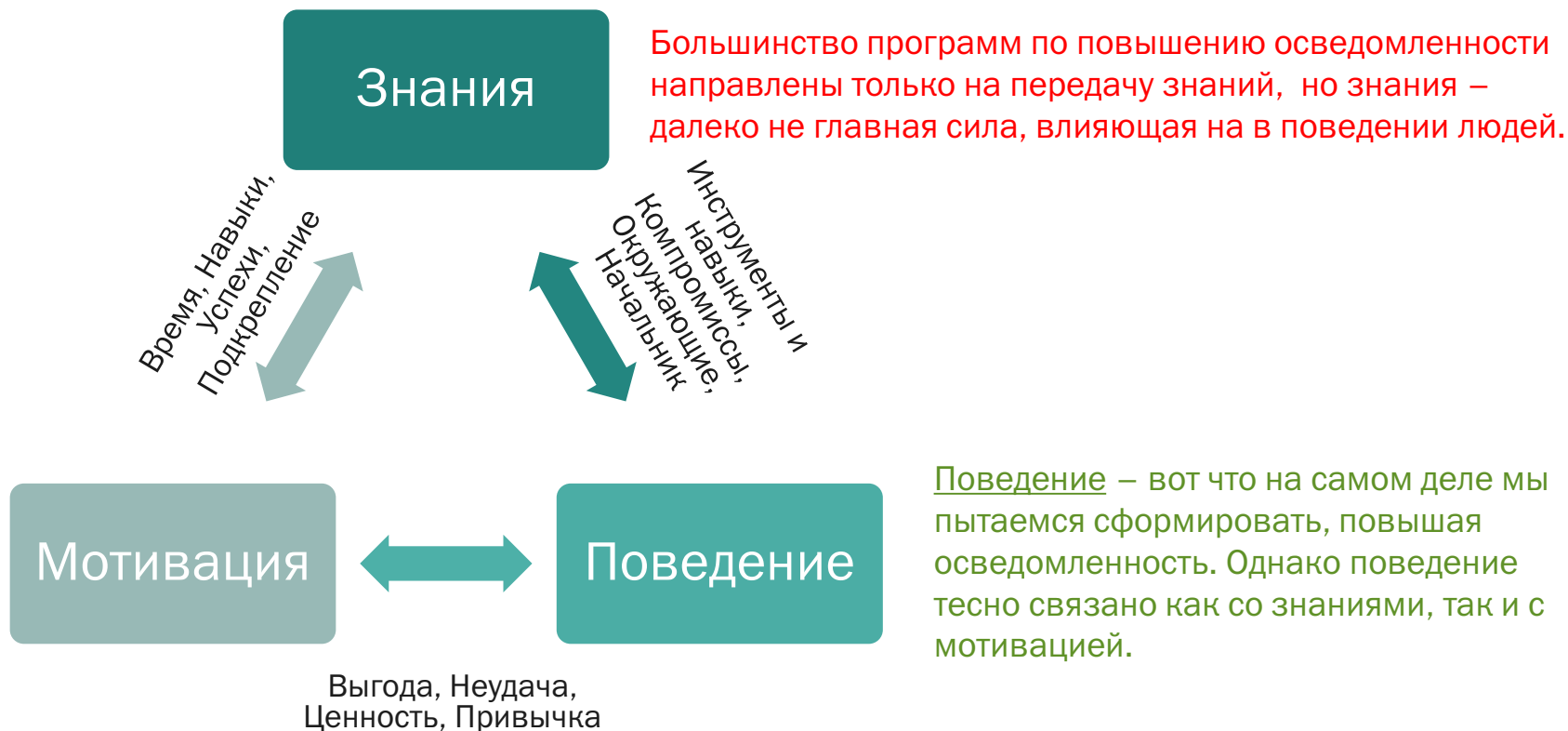
**Высокая эффективность**  
**Измеряемость**

- На 90% меньше инцидентов<sup>1)</sup>
- Снижение потерь денег<sup>2)</sup> на 50-60%.
- 37-кратный эффект от инвестиций<sup>3)</sup>

1) Истории успехов (Case Studies)

2) Aberdeen Group, 2014.

3) Ponemon Group Study, 2015



Подход, который мы предлагаем (CyberSafety Culture),

- эффективен
- измерим

на трех уровнях – знания, поведение, мотивация

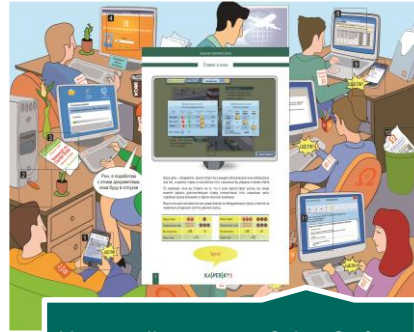
## Какого поведения мы ожидаем от людей после «программы повышения осведомленности»?

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

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.



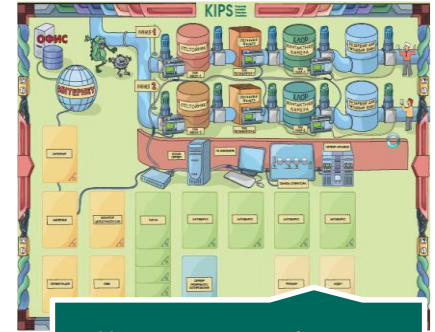
Платформа обучения навыкам



Игровой тренинг CyberSafety Games



Оценка культуры кибербезопасности



Интерактивная бизнес-симуляция KIPS

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



# 1. КОМПЬЮТЕРНАЯ ПЛАТФОРМА ОБУЧЕНИЯ НАВЫКАМ

## Модули интернет-обучения навыкам

+

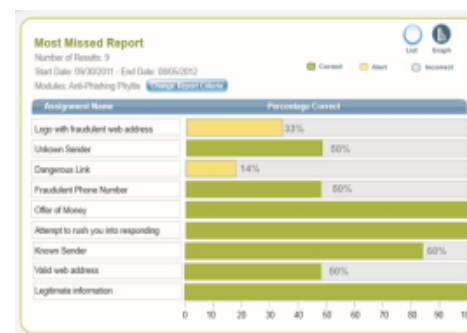
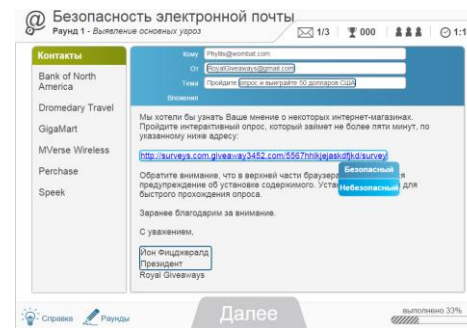
Имитация фишинговых атак

Оценка навыков

Анализ и отчеты

Каждому сотруднику в течение года назначаются различные краткие интерактивные модули интернет-обучения, имитационные 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

## Изменение убеждений, мотивация

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

## Бдительность

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

## Безопасность и эффективность – 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.

1. Преобразуйте заблуждения по поводу кибер-безопасности

2. В адекватное восприятие реальности

3. И покажите позитивные модели поведения

*«Вирус сломает мой компьютер»*

Опасаться нужно злоумышленников, а не сломанных компьютеров

Думайте, кто может воспользоваться вашими действиями

*«Я слишком мал для мишени»*

Жертвами становятся не только те, на кого направлена непосредственная атака

Станьте менее уязвимым, чем другие

*«Нет времени на заботу о безопасности»*

Безопасность необходима для эффективной работы

Сотрудничайте с отделом IT-безопасности



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.



Cyber Safety Mindset		
Employees in the organisation see Information Security Service as not open enough for collaboration and consultancy	Collaboration with IT	Employees see Information Security Service as a partner who is ready to support and assist with Cyber Security issues
Employees perceive Cyber Security rules as overly restrictive and creating unjustified obstacles in work	Policies Acceptance	Employees perceive Cyber Security rules as justified and necessary
In the organisation insufficient attention is paid to learning the rules of safe behavior for maintaining Cyber Security	Skills	In the organisation a lot of attention is paid to teaching employees the rules of maintaining Cyber Security
Risk Management		
Supervisors do not emphasize the importance of following Cyber Security rules, do not monitor employees' compliance with them	Management Support	Supervisors regularly remind how important it is to follow Cyber Security rules, monitor employees' compliance with them
Employees are not informed about the incidents threatening Cyber Security and how to act if such situations re-emerge	Lessons Learnt	Information Security Service informs employees how to act if an incident regarding Cyber Security violation re-emerges
Employees in the organisation are worried about possible consequences for themselves and thus do not tend to report incidents regarding Cyber Security	Reporting Culture	Employees willingly report situations threatening organisation's Cyber Security without worrying about possible consequences for themselves
Business Impact		
Employees in the organisation see Information Security Service's actions as inconsistent with business needs and not prompt enough	Implementation	Information Security Service's actions are seen as prompt and timely; changes in Cyber Security policies and procedures are perceived as justified for solving business tasks
In the organisation Cyber Security is not recognised as one of the processes that support Business Continuity and reaching key goals of the organisation	Trade-off	In the organisation Cyber Security is perceived as an important component of ensuring Business Continuity and business processes' implementation
The staff is facing difficulties in finding compromises with Information Security Service for solving business problems; the need to communicate with Information Security Service to find mutually acceptable ways for action in the interests of business is perceived as an obstacle	Security Recognition	Employees reach compromises with Information Security Service in solving business problems; find effective solutions in the interests of business in a joint discussion with Information Security Service
Commitment to Security		
The staff of the organisation shows low interest in supporting Cyber Security processes	Involvement	The staff of the organisation shows involvement and alertness to the issues of Cyber Security, going beyond the formal requirements
The prevailing notion in the organisation is that Cyber Security assurance depends solely on Information Security Service and the quality of software	Personal Responsibility	It is believed in the organisation that for maintaining Cyber Security the attention and responsibility of all employees are as important as the quality of software
An opinion prevails in the organisation that Cyber Security assurance has nothing to do with the staff	Impact - my actions matter	The prevailing opinion in the organisation is that every employee can affect Cyber Security

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.

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.

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.



# Развертывание и запуск в течение месяца



Мы предоставляем руководство по рекомендованным практикам и техническую поддержку

# Обучение продолжается в течение года, цикл за ЦИКЛОМ



Мы предоставляем руководство по рекомендованным практикам и техническую поддержку

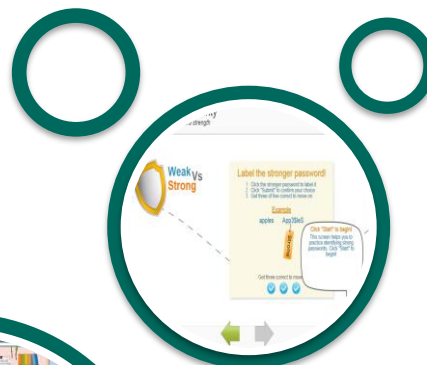


Постоянное измерение успехов

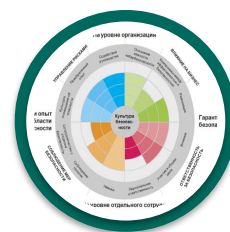
## Эффект

- Сокращение количества инцидентов – до 90%
- Уменьшение рисков на 50–60% в денежном выражении<sup>1)</sup>
- 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



# Подробное описание

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



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.

# Каждое рабочее место содержит 12 размеченных зон

## РАБОЧИЕ МЕСТА





## 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.

CyberSafety Games Москва / 2015-09-01 13:55:08 Round 01 Введение

Ваша ставка:  
▶ Степень уверенности:

**Правила расчета очков**  
**Степень уверенности**

Ставка команды	Является угрозой	Не является угрозой	Правильный ответ	Неправильный ответ
Не знаю			+10	-10
Возможно			+20	-20
Точно			+30	-60
Нет ставки				-10

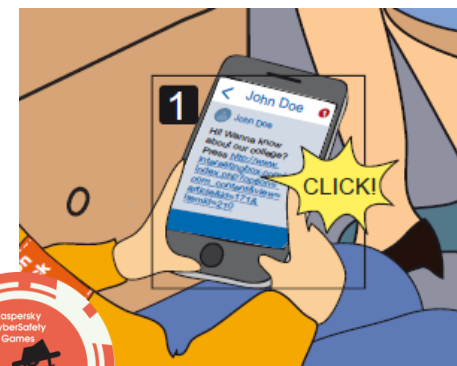
**Правила расчета очков**  
**Частота угрозы**

По факту \ Ставка	Редкая	Средняя	Частая
Редкая		0	-5
Средняя	0		0
Частая	-5	0	
Нет ставки на частоту угрозы			0

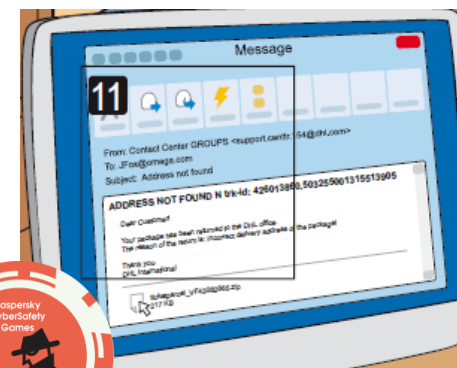
1. Перетащите 2 зеленых фишки на квадратное поле / в квадрат

Карта открыта

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



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







The screenshot displays the CyberSafetyGames interface during a video conference. At the top, it shows the event name "CyberSafetyGames", the location and date "Moscow / December 15, 2014 International Antivirus Conference", the current map "VideoConference", the current turn "01", and the leading team "05" with a score of "06".

The main content area lists proposals from three teams:

- Team 01** (Voted teams: 10):
  1. Prohibit flash-drives
  2. Fine the owner of the flashdrive
  3. Take the unattended flash and return to IT Security
- Team 05** (Voted teams: 4):
  1. Put a chain on flash-drive to stick to the belt
  2. Encrypt all flash-drives
- Team 03** (Voted teams: 3):
  - Take flash-drive with me

At the bottom, there is a section for "Other teams" with buttons for 01, 02, 05, 06, 07, 08, and 09. A "Best answers" button is located in the bottom right corner.

A circular inset on the right side of the interface shows a hand holding a flash drive, with a small black box containing the number "5" overlaid on the image.

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.

The screenshot displays the 'CyberSafety Games' interface. At the top, it shows 'Current Map: VideoConference', 'Turn 6', and 'Leader # 05 > 06'. The main area is divided into two panels:

- Situation by Team 04:** A text box describes a chief tax officer hiring staff. Below is a 3x3 grid of colored circles (green, yellow, red) representing different risk/need levels. The bottom-right circle (High security risk, Low business need) has a white 'X' over it. A 'Submit' button is at the bottom.
- Your situation rated by Team 06:** A text box describes Dina copying artwork. Below is a 3x3 grid of colored circles. The top-left circle (High business need, Low security risk) has a green 'X' over it. 'Agree' and 'Don't agree' buttons are at the bottom.

At the bottom of the interface, it shows 'Team #05' with 9000 coins and 20 stars, a 'Check opponent' button, and a timer at 00:24. A circular inset on the right shows a close-up of a computer screen displaying a progress bar for 'Copying 90 items (100%)'.

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

CyberSafety Games

Current Map: VideoConference Turn 6 Leader # 05 > 06

Information Safety Rules

@ Email Security Round 1 - Identifying Basic Threats 1/3 000 1:50

**Contacts**

- Bank of North America
- Dromedary Travel
- GigaMart
- MVerse Wireless
- Perchase
- Speak

To: Phyllis  
From: perchase4568@live.com  
Subject: Cash for your opinion

Attachments

We would like your opinion on our survey. The survey has only five short questions and will give you a \$10.00 credit on the purchase of any product. To fill out the survey, click the following link:

[http://perchasesurvey\\_survey4568.com/66556jdfisk/survey](http://perchasesurvey_survey4568.com/66556jdfisk/survey)

The survey link is only valid for two days, so please hurry!

Thank you,  
Perchase Survey Department

Next completed 33%

Team #05 9000 ☆20 Perform this exercise 02:08

From: Contact Center GROUPS - supportcenter\_s4@hivm.com  
To: J.Fine@surveys.com  
Subject: Address not found

ADDRESS NOT FOUND in text: 62861366\_602250e13

One Contact  
Your message has been returned to the CCL. Please check the address in your email and try again.

Thank you  
CCL Administrator

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.

CyberSafety Games

Current Map: VideoConference Turn 6 Leader # 05 > 06

Information Safety Rules

### Social Engineering

Lesson 1 - Social Engineering Basics

#### True or False

2/3

Good job! Filters and firewalls can protect you from some attacks, but they never catch everything.

Review Next

True False

completed 44%

Lessons

Team #05 9000 20 Perform this exercise 02:08

...s our French HR calling, asking for the email address of our accounting department to solve urgent problem with bonuses calculatuion, who knows this email?

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.





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.

**«Лаборатория Касперского»  
предоставляет**

- Материалы для участников (игровые поля, фишки) и программное обеспечение CyberSafety Games
- Квалифицированного тренера
- Раздаточные материалы для участников

**Клиент обеспечивает**

- Помещение, компьютеры, аудио- и видеооборудование, доступ к интернету
- Еду и напитки
- Приглашение и регистрацию участников



Подробное описание

Платформа обучения  
навыкам

## Create New Assignment

Step 2: Add Modules

<input type="checkbox"/>	Module Name
<input type="checkbox"/>	URL Training
<input type="checkbox"/>	Social Engineering
<input type="checkbox"/>	Smartphone Security
<input type="checkbox"/>	Security Beyond the Office
<input type="checkbox"/>	Safer Web Browsing
<input type="checkbox"/>	Safe Social Networks
<input type="checkbox"/>	Protected Health Information
<input type="checkbox"/>	Physical Security

Page 1 of 1

Cancel



1

2

3

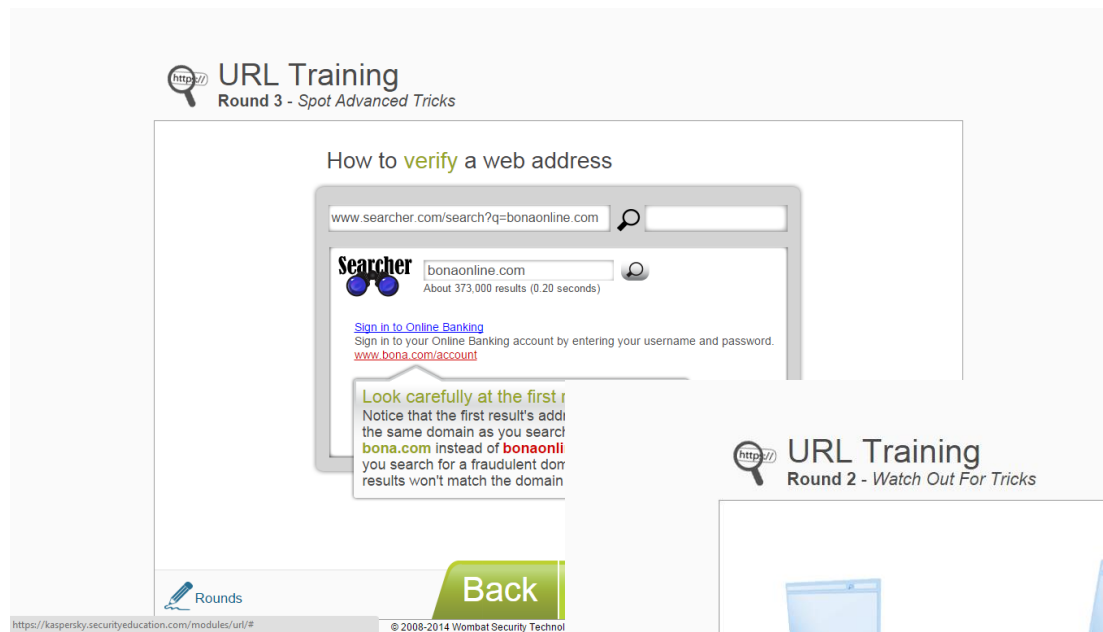
Запись на модули

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

# Интернет-платформа для каждого сотрудника

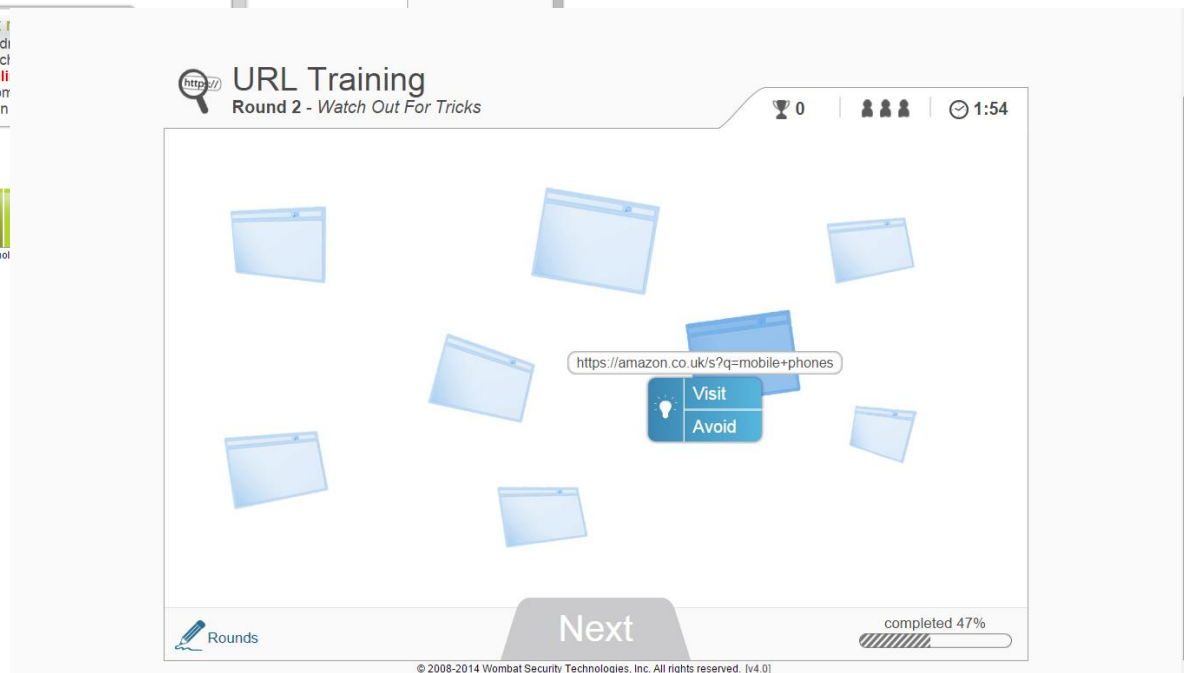
<p><b>Навыки антифишинга</b></p>  <p>Обнаружение фишинговых атак по мошенническим URL-адресам.</p>	<p><b>Правила антифишинга</b></p>  <p>Обнаружение фишинговых писем по характерным «красным флажкам».</p>	<p><b>Защита и уничтожение данных</b></p>  <p>Безопасное пользование портативными носителями и надежное удаление конфиденциальных данных</p>
<p><b>Безопасность электронной почты</b></p>  <p>Обнаружение фишинговых писем, опасных вложений и других попыток мошенничества по электронной почте.</p>	<p><b>Безопасность мобильных устройств</b></p>  <p>Использование физических и технических средств для защиты устройств и данных.</p>	<p><b>Информация, позволяющая установить личность</b></p>  <p>Защита конфиденциальной информации о себе, работодателе и клиентах</p>
<p><b>Пароли</b></p>  <p>Создание и хранение надежных паролей.</p>	<p><b>Физическая безопасность</b></p>  <p>Защита персонала и имущества.</p>	<p><b>Информация о состоянии здоровья</b></p>  <p>Почему и как нужно защищать информацию о состоянии здоровья</p>
<p><b>Безопасность в социальных сетях</b></p>  <p>Ответственный подход к использованию социальных сетей.</p>	<p><b>Безопасный просмотр веб-сайтов</b></p>  <p>Безопасная работа в интернете: отказ от рискованных действий и избегание распространенных «ловушек».</p>	<p><b>Безопасность за пределами офиса</b></p>  <p>Предупреждение распространенных ошибок, нарушающих безопасность при работе из дома или в дороге</p>
<p><b>Основные правила безопасности</b></p>  <p>Учет вопросов безопасности в повседневных операциях.</p>	<p><b>Социальная инженерия</b></p>  <p>Обнаружение и избегание попыток мошенничества.</p>	<p><b>Распознавание URL-адресов</b></p>  <p>Обнаружение мошеннических URL-адресов</p>

В каждый обучающий модуль входит теоретическая часть...



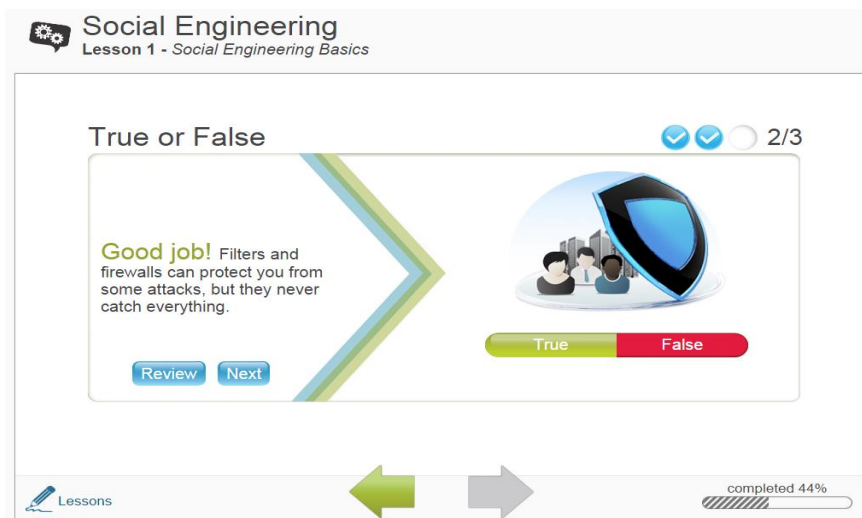
...и упражнения для обучения на собственном опыте

Короткие занятия около 15 минут



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

...гарантирует эффективность обучения



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

Password Security  
Lesson 2 - Password creation

Password Sec  
Lesson 2 - Password cre

Password Security  
Lesson 3 - Password families



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

### Edit Training Jacket Template

Review and make any necessary changes training jacket.

English (US) French ✕ +

Company Policy on the passwords is:

- follow the minimum password complexity enforced by the Company
- never use the same or similar password for any other personal resource outside of the company
- change the password very 3 months (for Financial department - every 2 months)

Please read the full security policy here: [intranet.customer.com/security](http://intranet.customer.com/security)

In case you beleive your password may be compromized, report it to the Security team immediately by:

- Dialing #1911 extenstion
- Email [security@customer.com](mailto:security@customer.com)

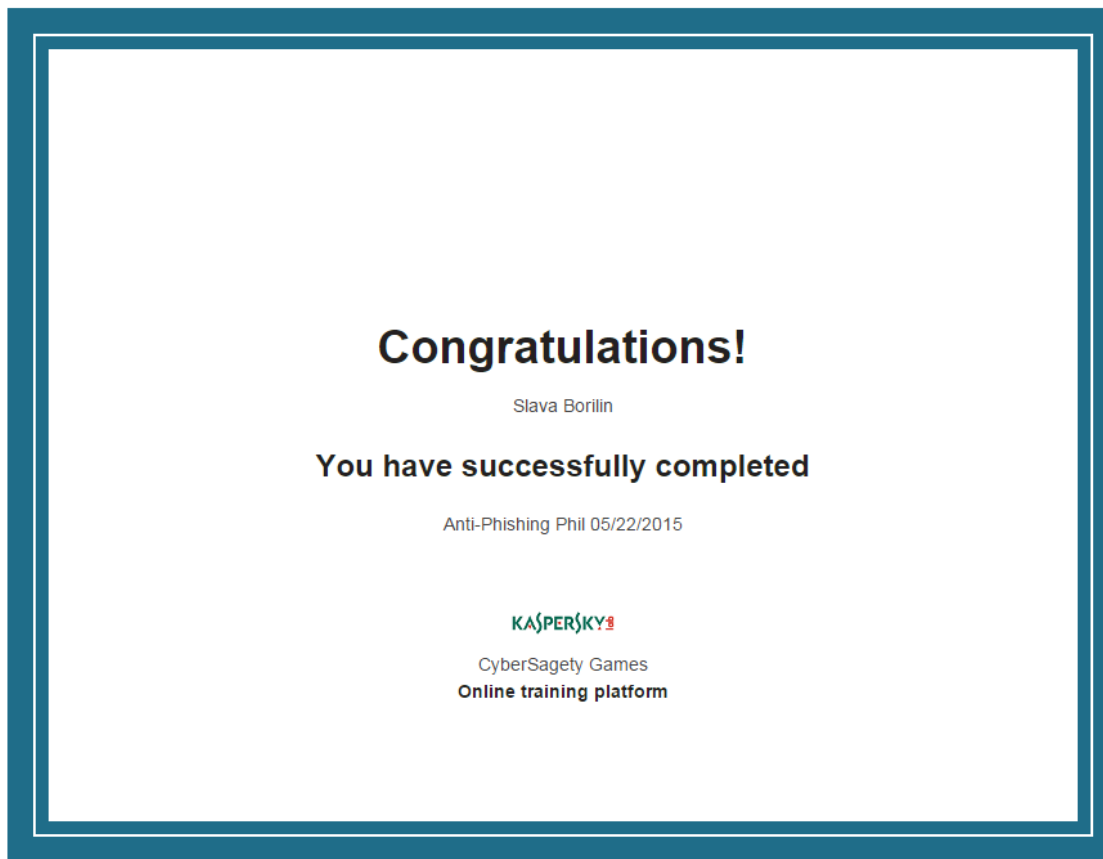
I acknowledge that I have completed and understand the material in this Training Module, including the Password security policy of my company.

Accept

Decline

Exit

После обучения пользователь может получить фирменный сертификат



Print Exit

# Программы оценки

# Определение продолжительности курса и областей безопасности

## Create a CyberStrength Assessment

Select Subject Areas

Assessment Name: Slava

Subjects

3 selected of 9		<input type="checkbox"/>
Phishing (13 questions) Identify Phishing Threats	<input checked="" type="checkbox"/>	
Data Protection (10 questions) Protect and dispose of data securely	<input checked="" type="checkbox"/>	
Mobility (19 questions) Work safely outside the office	<input checked="" type="checkbox"/>	
Internet Browsing (17 questions) Use the Internet Safely	<input type="checkbox"/>	

Cancel



# Интерактивные вопросы



CyberStrength

On the Road: Safe or Unsafe?

2/20

Is the displayed activity safe?



*Amy picks up her order at the counter.*



Safe

Unsafe



# Интерактивные вопросы

## Data Protection and Destruction

6/20

**Choose the best answer:**

**!** *Which of these is the best way to share sensitive data with colleagues?*

- A** Via a cloud-based file sharing app like Dropbox
- B** Via a CD that can be shredded
- C** Via a secure corporate server
- D** Via an encrypted company email

# Имитация фишинговых атак

# Готовые шаблоны



Security Education Platform

## Select Attack Category

Select the category below which most closely matches the type of

1 OF 1

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

# На основе реальных случаев фишинга

## Разный уровень сложности

### Select Attack : Work Related

Select a phishing attack from the list below:

Language:

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 %

# Удобная настройка

## Edit Email Template

Review and make any necessary changes to the phishing email for your campaign.

From Name: Customer Support

From Address: support.id429@us-3.track-my-package.net

Subject: Package denied at the parcel's delivery

Edit ▾ Insert ▾ Table ▾ Format ▾

↶ ↷ **B** *I* U [List Icons] A ▾ **A** ▾ Add Contact Property ▾

Font Family ▾ Font Sizes ▾ [Link Icon] [Unlink Icon] [List Icons] [List Icons] [Image Icon] [Code Icon]

Postal notification,

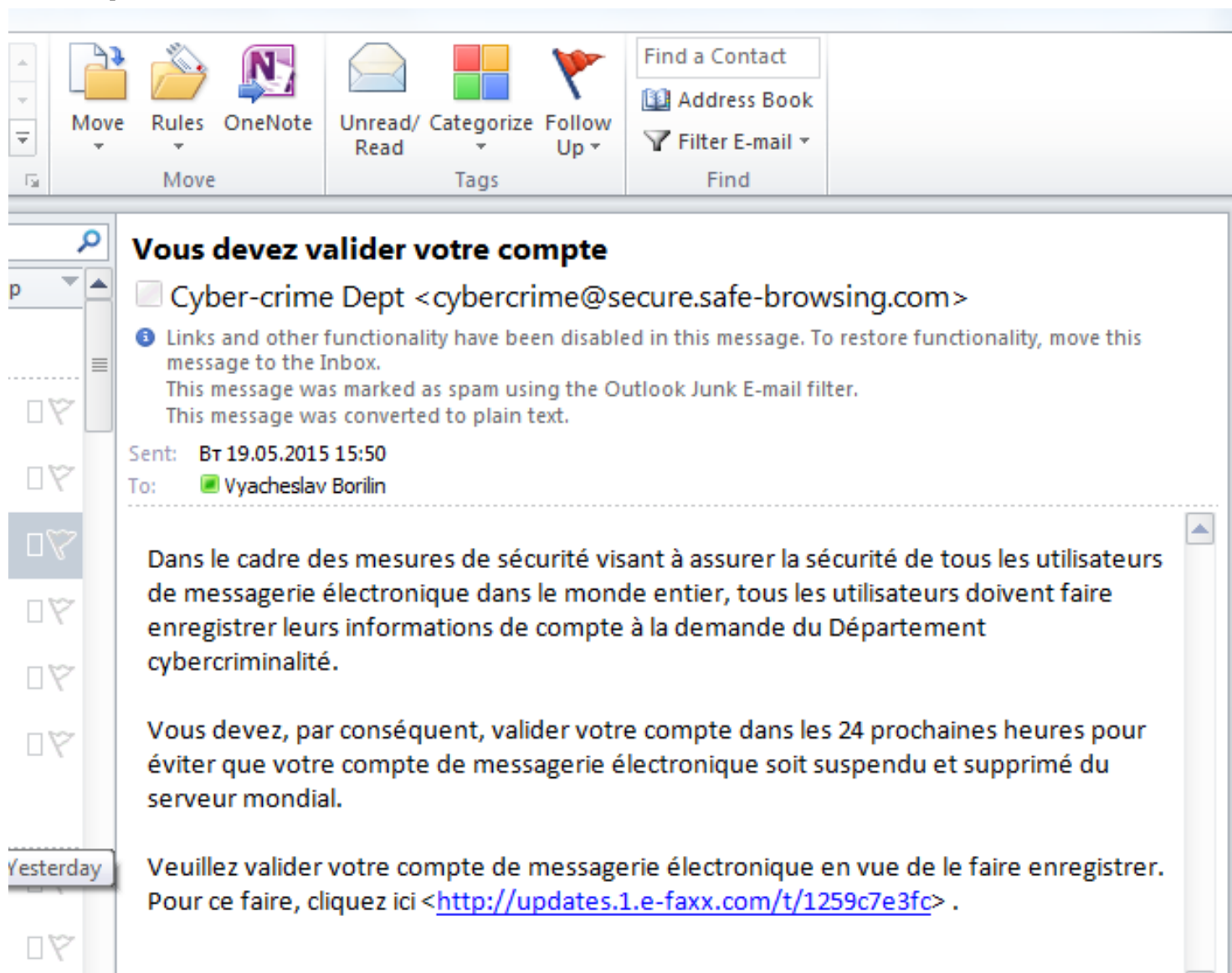
Courier service couldn't make the delivery of your parcel.  
Status:An error at the delivery address.

LOCATION OF YOUR ITEM:Cincinnati  
STATUS: sorting  
SERVICE: Standard Shipping  
NUMBER OF YOUR ITEM:U358210589NU  
INSURANCE: No

Label is enclosed to the letter



# Сотрудник получает фишинговое письмо и переходит по ссылке...



# Открытие фишинговой страницы – важный этап обучения

## Автоматическая запись на тренинги

### Статистика

Oups ! Le courriel auquel vous venez de répondre était un courriel d'hameçonnage factice. Pas la peine de s'inquiéter ! Il vous a été envoyé pour vous aider à apprendre à éviter les attaques réelles. Veuillez ne pas partager votre expérience avec vos collègues, pour qu'ils puissent également apprendre.

<p><b>John reçoit un courriel urgent...</b></p> <p>Ce courriel paraît important. Je ferais mieux d'agir au plus vite.</p> <p><b>ARRÊTEZ-VOUS !</b> Vous auriez pu vous faire avoir par cet hameçonnage par courriel. Les pirates utilisent les courriels pour voler des informations confidentielles.</p>	<p><b>Voici comment les escrocs essaient de vous tromper...</b></p> <p>Dans le cadre des mesures de sécurité visant à assurer la sécurité de tous les utilisateurs de messagerie électronique dans le monde entier, tous les utilisateurs doivent faire enregistrer leurs informations de compte à la demande du Département cybercriminalité.</p> <p>Vous devez, par conséquent, valider votre compte dans les 24 prochaines heures pour éviter que votre compte de messagerie électronique soit suspendu et supprimé du serveur mondial.</p> <p>Je vous envoie ce qui paraît être un message important ou intéressant pour vous persuader de répondre immédiatement.</p> <p>Le courriel paraîtra légitime, mais c'est une ruse. Dès que vous répondez avec des informations ou que vous cliquez sur des liens, j'ai facilement accès à vos données ou à vos comptes en ligne !</p>
<p><b>Comment vous protéger...</b></p> <ol style="list-style-type: none"> <li>1 Ne révélez jamais des informations personnelles, commerciales ou financières en réponse à un courriel non sollicité.</li> <li>2 Ne cliquez pas, ne répondez pas ou ne remplissez pas les formulaires envoyés dans des courriels suspects. Nom : <input type="text" value="John Smith"/> Numéro de sécurité sociale : <input type="text" value="111-11-111"/></li> <li>3 Pointez sur les liens pour afficher leurs véritables sources. <input type="text" value="http://updates.1.e-faxx.com/t/1259c7e3fc"/></li> </ol> <p>Ne soyez pas dupe de logos et de marques familières. Plutôt</p>	<p>Hmmm... je ne suis plus si sûr de ce courriel maintenant. Je vais y regarder de plus près avant de répondre.</p> <p>J'aurais pu avoir accès à de précieuses informations ! Il aurait suffi d'un clic !</p>

# Анализ и 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

# Контроль прохождения тренингов и результатов программ оценки

## Dashboard





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%**

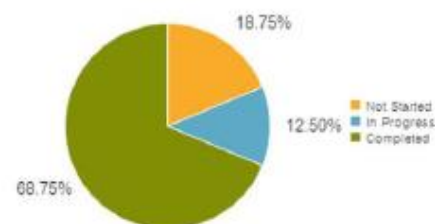
Number of Users: 16

Total Number of Questions: 10

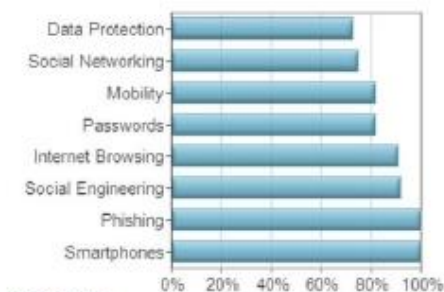
Question Generation Type: Administrator Defined

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

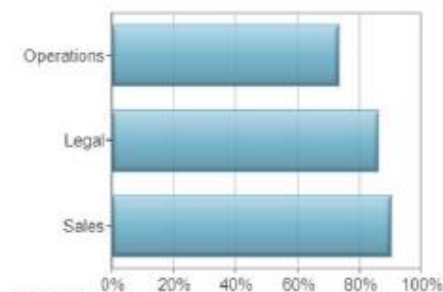


[Click for Details](#)



Export to Excel

#### Score By Group



[Click for Details](#)



Export to Word

**«Лаборатория Касперского»  
предоставляет**

- Учетную запись для интернет-платформы
- Обучение администраторов
- Техническую поддержку

**Клиент обеспечивает**

- Загрузку почтовых ящиков сотрудников в платформу
- Создание программ:
  - имитации атак
  - оценки
  - обучения
- Запись групп на обучающие модули
- Анализ результатов

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<sup>1)</sup>
- 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