Обучение, которое нельзя отменить

Киберграмотность не выходя из дома

Денис Баринов,
руководитель
Kaspersky Academy
academy.kaspersky.ru

kaspersky

Обсудим сегодня

- Сотрудники, удаленка и COVID-19: новые угрозы
- Что сделать прямо сейчас
- Как надежно научить сотрудников работать безопасно, а следовательно, эффективно

КАК COVID-19 ВЛИЯЕТ НА СТИЛЬ РАБОТЫ РОССИЯН

Исследование «Лаборатории Касперского»*

22% стали больше работать

59% используют личную почту для решения рабочих вопросов

56% могут чаще бывать с семьей и больше времени посвящать личным делам

55% общаются по работе в мессенджерах, не одобренных IT-отделами

58% стали больше читать новостей

71% читают новости онлайн на устройствах, которые используют для работы

*Исследование «Влияние COVID-19 на стиль работы» проведено «Лабораторией Касперского» апреле 2020 года. Опрошено 6016 сотрудников по всему миру.

51%

работников смотрят контент для взрослых и работают с одних и тех же устройств

К чему это приводит - ошибки сотрудников слишком дорого обходятся бизнесу – даже в «мирное» время

14,3 млн р.

для крупных предприятий

Средний ущерб от успешной атаки, в т.ч. вызванной неумышленными ошибками сотрудников *

4,3 млн р.

для сегмента СМБ

Средний ущерб от успешной атаки, в т.ч. вызванной неумышленными ошибками сотрудников *

33%

российских организаций

Хотя бы раз за год столкнулись с инцидентами, связанными с ненадлежащим использованием ИТ-ресурсов сотрудниками *

до $400

на сотрудника за год

Средние потери компаний от фишинга (без учета прочих векторов атак) **

* *Исследование «Информационная безопасность бизнеса», «Лаборатория Касперского», весна 2018.*
** *Calculations based on Ponemon Institute, "Cost of Phishing and Value of Employee Training", August 2015.*

Какие риски возникают при переходе на удаленку?

- Незащищенные wi-fi сети
- Использование личных устройств для работы
- Широкое использование видеоконференций
- Использование неодобренных IT-службой программ и сервисов
- Доступ семей к рабочим данным
- Интернет-мошенники, спекулирующая на ситуации

Когда надежный пароль становится фактором национальной безопасности

Используйте надежный пароль ко всем средствам деловой коммуникации – и не разглашайте даже части конфиденциальных данных

Good news for anyone who was hoping to join the meeting but had mislaid the Zoom meeting ID.

But bad news for any mischief makers hoping to take advantage – the Zoom meeting is password-protected. Thank heavens for that.

Let's hope it's a strong password, that's hard to guess.

Boris Johnson inadvertently reveals the UK Government's Cabinet Meeting Zoom I.D. on Twitter

Boris Johnson's Zoom meeting. Click for larger version

Вредонос-шпион AZORult эмулирует карту Университета Джона Хопкинса (через .exe-файл)

Троян собирает информацию, хранящуюся в браузерах: cookies, история посещений страниц, идентификаторы пользователей, пароли, ключи от криптовалютных кошельков

Защита: ставить антивирус и не ставить exe-файлы

Приложение COVID19 Tracker считывает пароль от телефона и блокирует вход, требуя выкуп

Бэкдор, вымогатель

Защита:
- бэкап
- не ставить неизвестные приложения
- отдельно защищать корпоративную информацию на устройствах

Письмо якобы от руководства предлагает ознакомиться с информацией – и ворует учетные записи Microsoft

Фишинг
Воровство аккаунтов

Защита:
- умение распознавать фишинг
- подозрительность при вводе логина и пароля

20 тысяч

студентов и сотрудников американских вузов получили фишинговое письмо якобы от руководства с просьбой ввести логин и пароль от учетной записи Microsoft

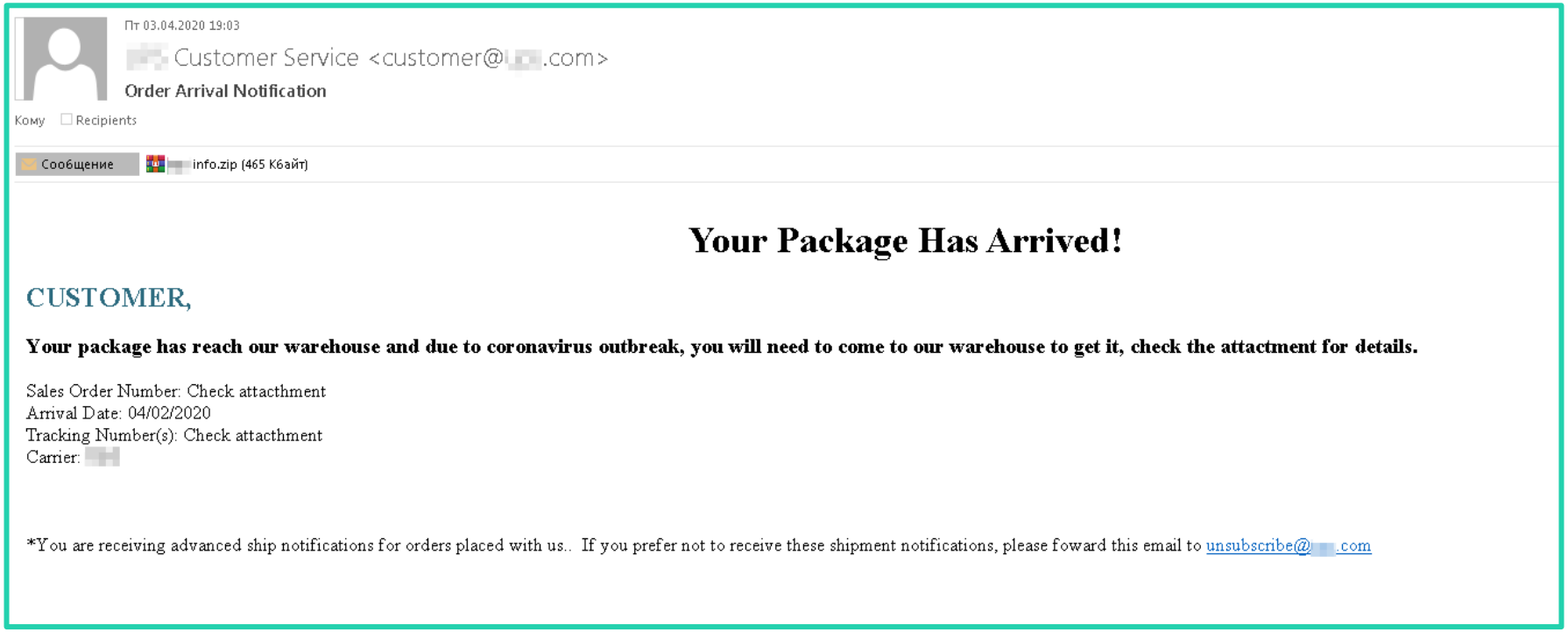
Hi [redacted],

Kindly check the Latest information about COVID-19 [Corona Virus]

https://www.[redacted].edu/content/covid-19-coronavirus-information.pdf

The Trustees of [redacted] University | Health Team

Кроме того – подделка писем от служб доставки….



Пт 03.04.2020 19:03

Customer Service <customer@[redacted].com>

Order Arrival Notification

Кому Recipients

Сообщение info.zip (465 Кбайт)

Your Package Has Arrived!

CUSTOMER,

Your package has reach our warehouse and due to coronavirus outbreak, you will need to come to our warehouse to get it, check the attactment for details.

Sales Order Number: Check attacthment
Arrival Date: 04/02/2020
Tracking Number(s): Check attacthment
Carrier: [redacted]

*You are receiving advanced ship notifications for orders placed with us.. If you prefer not to receive these shipment notifications, please foward this email to unsubscribe@[redacted].com

Кроме того – подделка писем от служб доставки….

Ср 01.04.2020 0:37

EXPRESS <shipping@.com>

Cargo Arrival Notice!!

Кому .com

Сообщение | Arrival Notice.jpg.ace (24 Кбайт)

Our Dear Customer ,

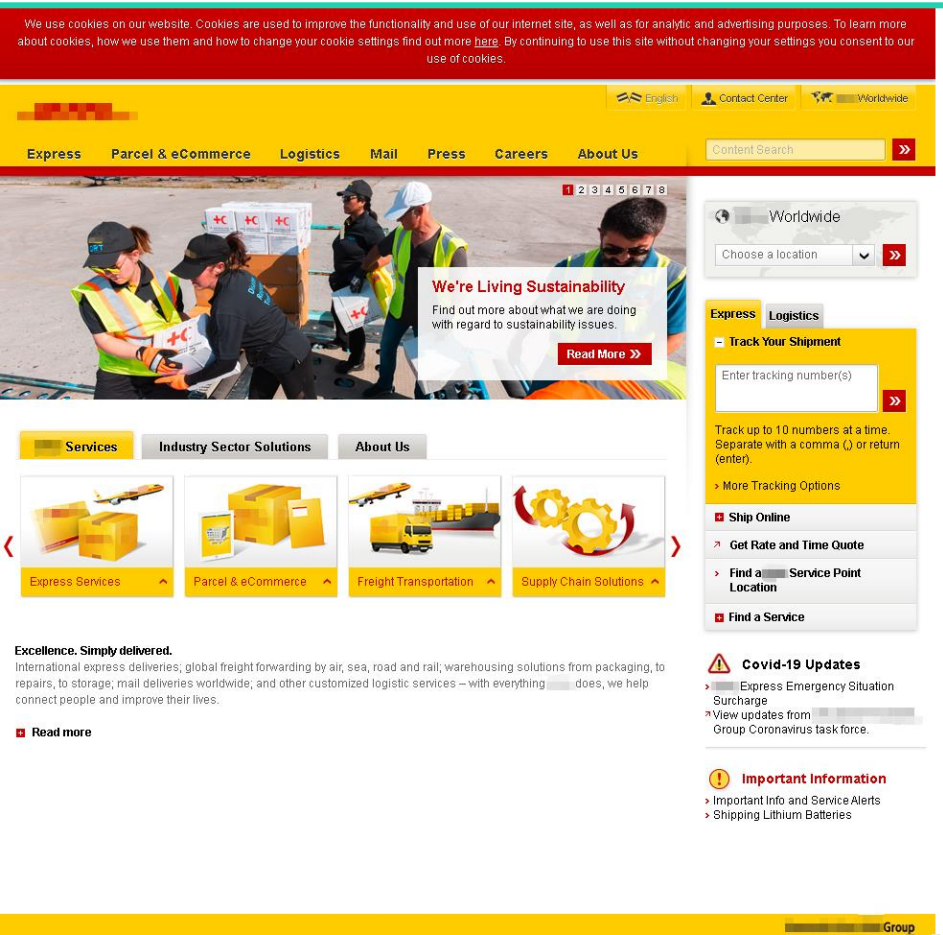
Urgent__ Your shipment arrived our regional Office on 30th, however the details provided for dispatch are incomplete pls check.

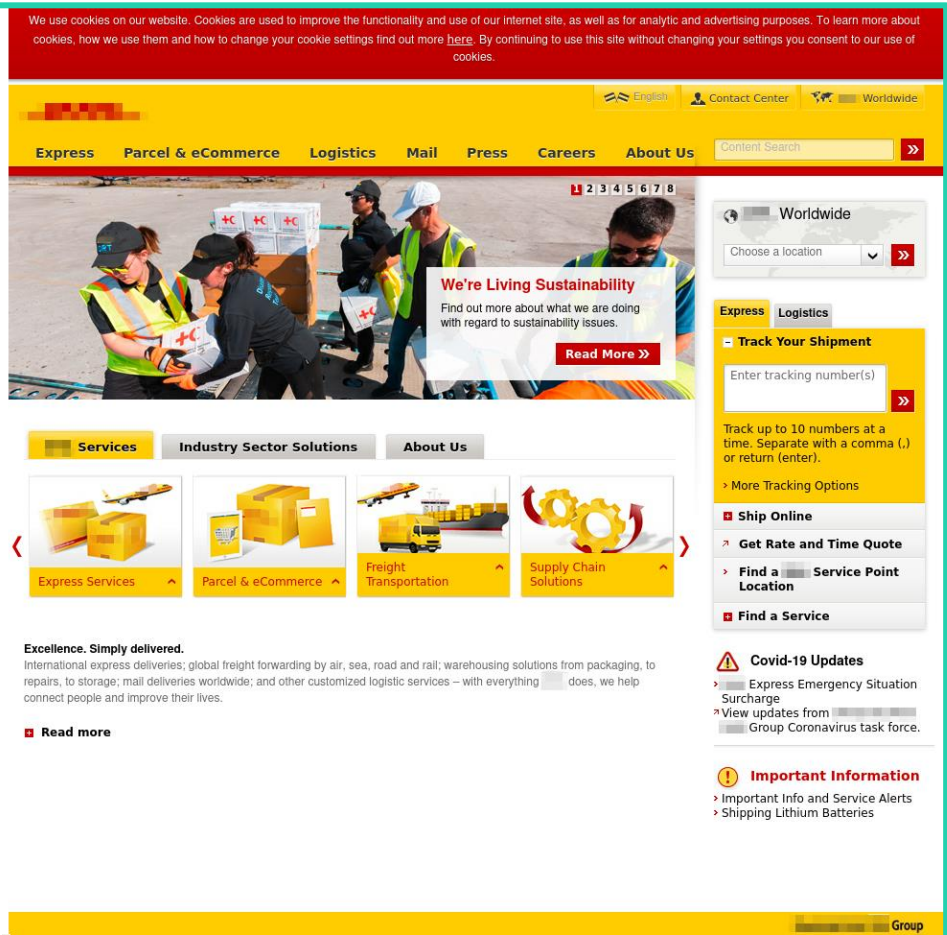
kindly see attach document and resend us corrected details for Tracking your address, to enable us proceed with Dispatch before goverment lock down, prior to the Coronavirus pandemic precautionary major.

Yours Sincerely,

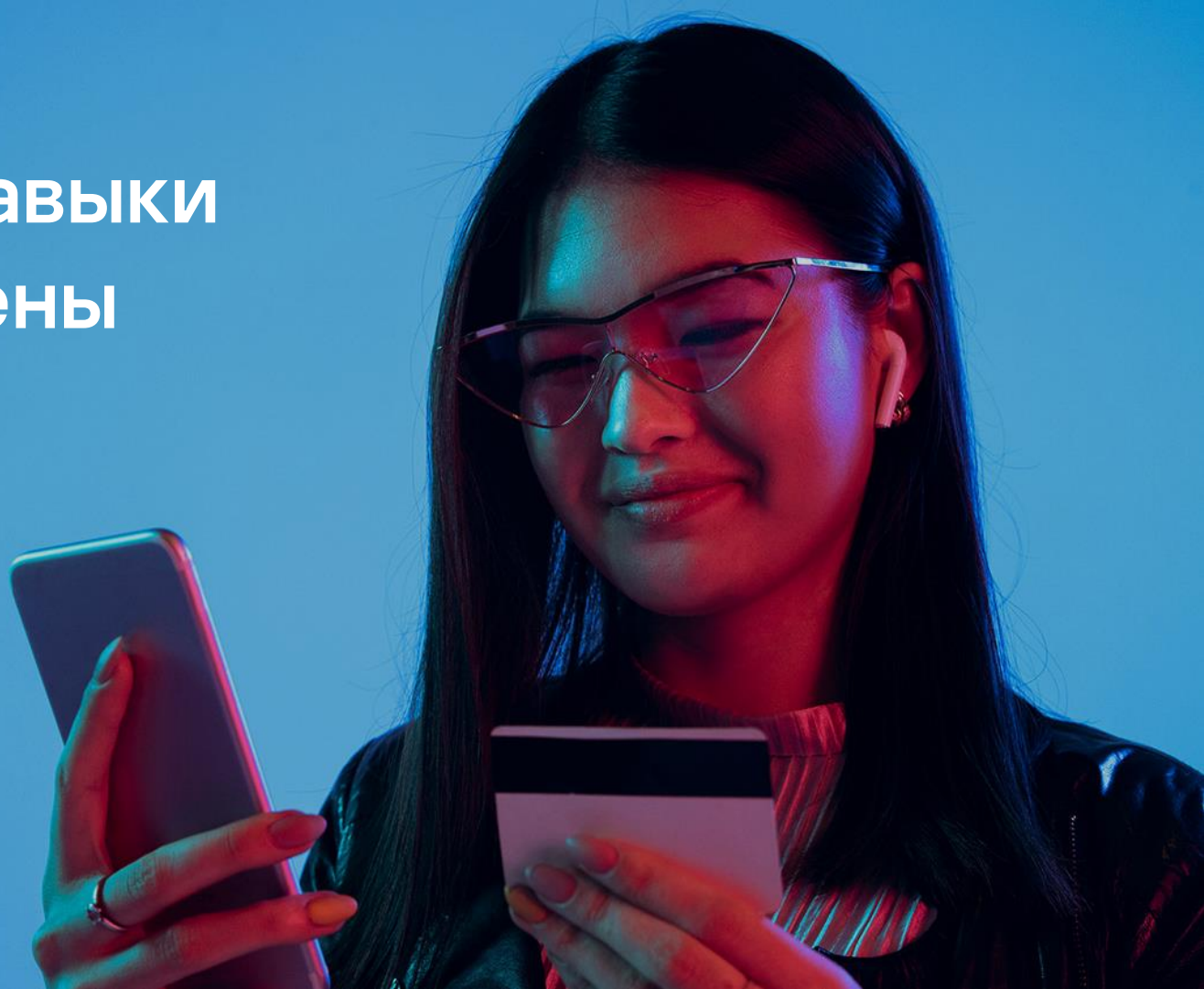
Customer Service Officer
EXPRESS
support@worldwide.inc

....и даже целых сайтов





Простые навыки кибергигиены



Сделать:

- Используйте зашифрованное по стандарту **WPA2 соединение**
- Установите на доступ к роутеру сложный, **12-значный пароль**
- Используйте **двухфакторную аутентификацию** на важных ресурсах

Проверить:

- Ваши сотрудники знают, что это такое и как проверить, **какой стандарт использует сеть?**
- Сотрудники знают, где и как поменять **пароль** (и что такое **роутер**)?
- Важные **корпоративные ресурсы** имеют двухфакторную аутентификацию? Пользователи умеют ее устанавливать?

Сделать:

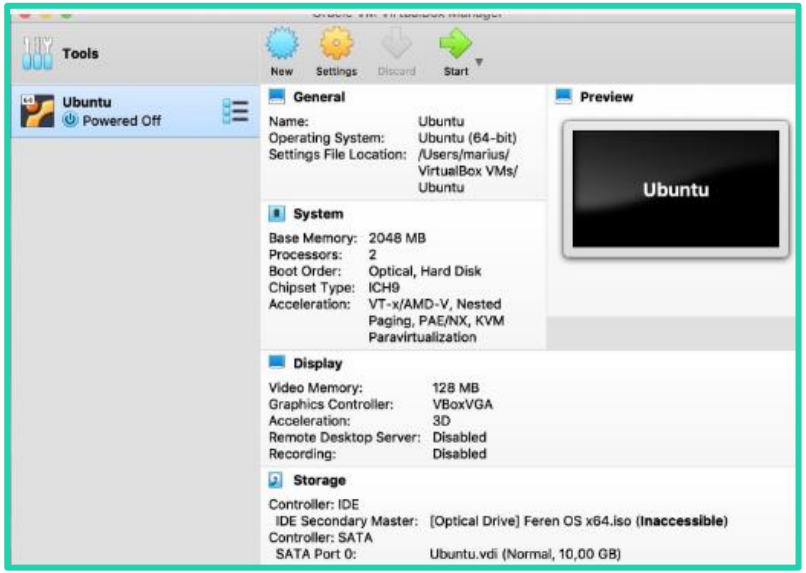
- Создайте для каждого пользователя (в т.ч. членов семьи и/или гостевую) **отдельную учетную запись**
- Защитите свою учетную запись **надежным паролем**

Проверить:

- Сотрудникам помогут создать **гостевые учетные записи** на рабочих компьютерах? А на личных?
- Сотрудники знают, что такое **надежный пароль**? Умеют их составлять? А запоминать? (или повесят бумажку с паролем на холодильник?)

Сделать:

- Создайте **список сотрудников**, для которых виртуальная машина обязательна
- Если сотрудник работает на личном компьютере – ставьте **виртуальную машину**!



Сделать:

- Проверьте на **адрес отправителя** и **текст** (грамотность, формат, контекст)
- Не открывайте **вложения** в письмах от служб доставки
- Осторожнее с письмами про **коронавирус**
- Не предоставляйте в ответ на письмо **никаких данных**
- Пользуйтесь **надежным защитным решением,** которое распознает вредоносное вложение и заблокирует фишинговый сайт

Проверить:

- Сотрудники умеют определять фишинговые письма? А **спирфишинг**?
- Вы когда-нибудь проводили **тестовую фишинговую рассылку,** чтобы это понять?
- Сотрудники могут распознавать и противостоять методам **социальной инженерии?**

Сделать:

- Проверяйте, не накопились ли неавтоматические обновления, и **своевременно** устанавливайте их!
- **Перезапускайте компьютер,** чтобы автоматические обновления начали действовать

Проверить:

- Расписание **автоматических обновлений** действует? А на личных компьютерах?
- Сотрудники понимают **важность обновлений?** Держат в голове необходимость проверки?
- Сотрудники понимают, что перезагрузка компьютера точно нужна **чаще раза в месяц?**

Другие важные принципы безопасности

1. Обеспечьте наличие и актуальность антивируса, в т.ч. на используемых для работы **личных ресурсах. Регулярно** сканируйте весь компьютер
2. Создавайте резервные копии
3. Используйте VPN и шифрование
4. Используйте разные браузеры для работы и личных надобностей. Не устанавливайте **плагины** в браузеры
5. Любую служебную информацию размещайте только **на корпоративных ресурсах**. В крайнем случае - на личных ресурсах (Google Drive и пр.) **с паролем**

Другие важные принципы безопасности

1 Обеспечьте наличие и актуальность антивируса, в т.ч. на используемых для работы личных ресурсах. Регулярно сканируйте весь компьютер

2 Создавайте сложные пароли

3 Используйте VPN и шифрование

4 Используйте разные браузеры для работы и личных надобностей. Не устанавливайте плагины в браузеры

5 Любую служебную информацию размещайте только на корпоративных ресурсах. В крайнем случае - на личных ресурсах (Google Drive и пр.) с паролем

Убедитесь, что:

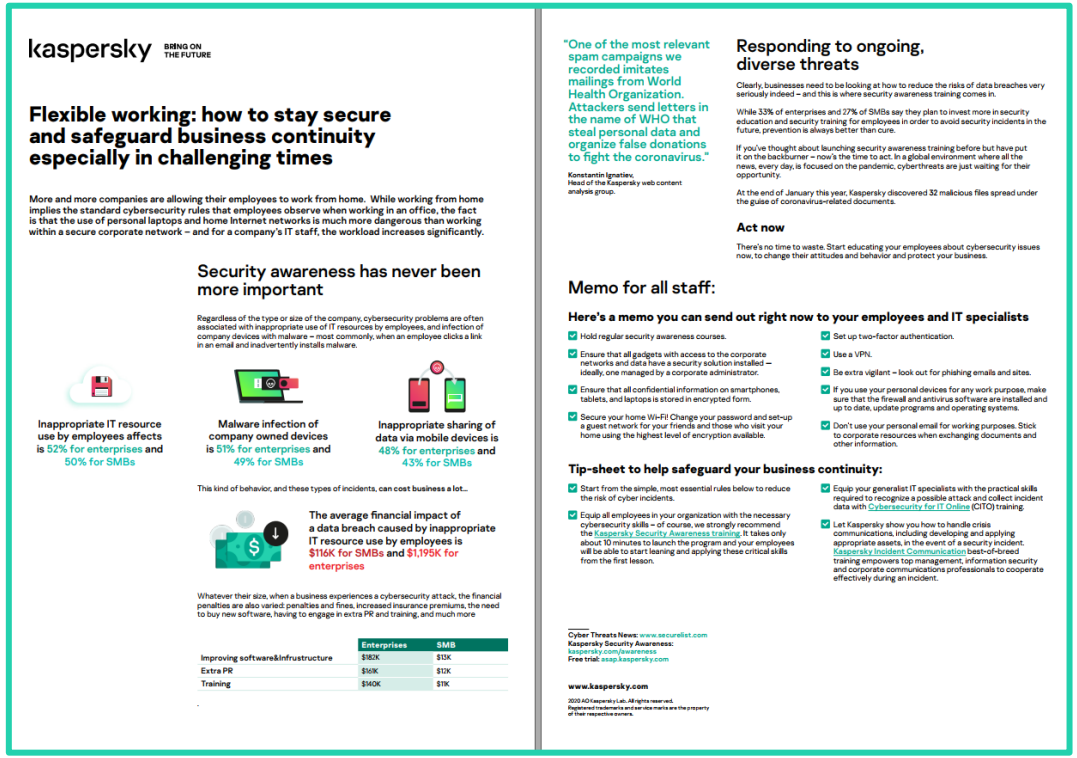
- ваш IT **готов** обеспечить эти меры
- сотрудники действительно **понимают**, зачем нужна каждая из них
- сотрудники умеют **пользоваться** этими советами
- сотрудники действительно ими **пользуются**

Срочные меры

Что сделать прямо сейчас:

— разошлите памятку
— проведите тренинги (в т.ч. используя бесплатные курсы от профессионалов)

Пример:
«Безопасность в жизни и бизнесе»
kas.pr/free-course



kaspersky BRING ON THE FUTURE

Flexible working: how to stay secure and safeguard business continuity especially in challenging times

More and more companies are allowing their employees to work from home. While working from home implies the standard cybersecurity rules that employees observe when working in an office, the fact is that the use of personal laptops and home Internet networks is much more dangerous than working within a secure corporate network – and for a company's IT staff, the workload increases significantly.

Security awareness has never been more important

Regardless of the type or size of the company, cybersecurity problems are often associated with inappropriate use of IT resources by employees, and infection of company devices with malware – most commonly, when an employee clicks a link in an email and inadvertently installs malware.

Inappropriate IT resource use by employees affects is 52% for enterprises and 50% for SMBs

Malware infection of company owned devices is 51% for enterprises and 49% for SMBs

Inappropriate sharing of data via mobile devices is 48% for enterprises and 43% for SMBs

This kind of behavior, and these types of incidents, can cost business a lot...

The average financial impact of a data breach caused by inappropriate IT resource use by employees is $116K for SMBs and $1,195K for enterprises

Whatever their size, when a business experiences a cybersecurity attack, the financial penalties are also varied: penalties and fines, increased insurance premiums, the need to buy new software, having to engage in extra PR and training, and much more

	Enterprises	SMB
Improving software&Infrustructure	$182K	$13K
Extra PR	$169K	$12K
Training	$140K	$11K

"One of the most relevant spam campaigns we recorded imitates mailings from World Health Organization. Attackers send letters in the name of WHO that steal personal data and organize false donations to fight the coronavirus."

Konstantin Ignatiev,
Head of the Kaspersky web content analysis group.

Responding to ongoing, diverse threats

Clearly, businesses need to be looking at how to reduce the risks of data breaches very seriously indeed – and this is where security awareness training comes in.

While 33% of enterprises and 27% of SMBs say they plan to invest more in security education and security training for employees in order to avoid security incidents in the future, prevention is always better than cure.

If you've thought about launching security awareness training before but have put it on the backburner – now's the time to act. In a global environment where all the news, every day, is focused on the pandemic, cyberthreats are just waiting for their opportunity.

At the end of January this year, Kaspersky discovered 32 malicious files spread under the guise of coronavirus-related documents.

Act now

There's no time to waste. Start educating your employees about cybersecurity issues now, to change their attitudes and behavior and protect your business.

Memo for all staff:

Here's a memo you can send out right now to your employees and IT specialists

- Hold regular security awareness courses.
- Ensure that all gadgets with access to the corporate networks and data have a security solution installed – ideally, one managed by a corporate administrator.
- Ensure that all confidential information on smartphones, tablets, and laptops is stored in encrypted form.
- Secure your home Wi-Fi! Change your password and set-up a guest network for your friends and those who visit your home using the highest level of encryption available.
- Set up two-factor authentication.
- Use a VPN.
- Be extra vigilant – look out for phishing emails and sites.
- If you use your personal devices for any work purpose, make sure that the firewall and antivirus software are installed and up to date, update programs and operating systems.
- Don't use your personal email for working purposes. Stick to corporate resources when exchanging documents and other information.

Tip-sheet to help safeguard your business continuity:

- Start from the simple, most essential rules below to reduce the risk of cyber incidents.
- Equip all employees in your organization with the necessary cybersecurity skills – of course, we strongly recommend the Kaspersky Security Awareness training. It takes only about 10 minutes to launch the program and your employees will be able to start learning and applying these critical skills from the first lesson.
- Equip your generalist IT specialists with the practical skills required to recognize a possible attack and collect incident data with Cybersecurity for IT Online (CITO) training.
- Let Kaspersky show you how to handle crisis communications, including developing and applying appropriate assets, in the event of a security incident. Kaspersky Incident Communication best-of-breed training empowers top management, information security and corporate communications professionals to cooperate effectively during an incident.

Cyber Threats News: www.securelist.com
Kaspersky Security Awareness:
kaspersky.com/awareness
Free trial: asap.kaspersky.com

www.kaspersky.com

Как научить сотрудников вещам, которые им изначально неинтересны?

Как трансформировать знание в поведение?

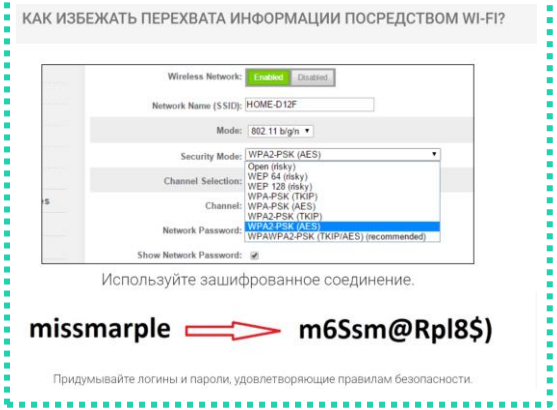
Один пример: как делают

1. Поняли, чему научить

Защита домашних wi-fi сетей

- Используйте зашифрованное по стандарту WPA2 соединение
- Установите на доступ к роутеру сложный, 12-значный пароль
- Используйте двухфакторную аутентификацию на важных ресурсах

2. Упаковали курс



3. Отчитались

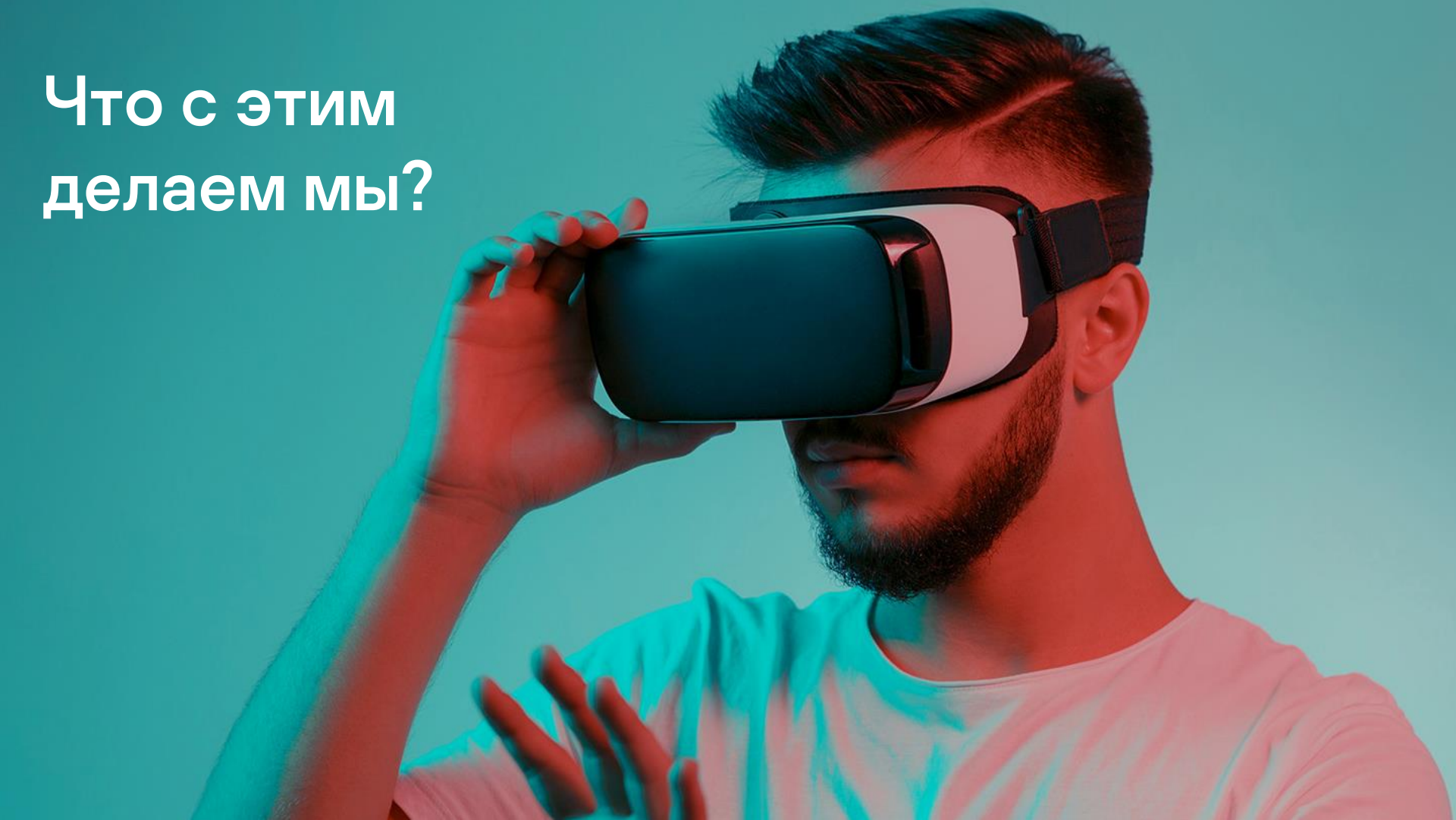
- Курс прошли 570 сотрудников
- Средний результат – 70%
- …

...И что получается

В реальной жизни по итогам обучения:

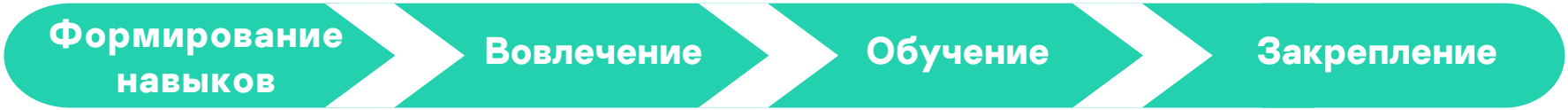
- Информация **теряется**
- Информация **забывается** (да и не запоминается)
- Знание **не трансформируется** в действие

Что с этим делаем мы?



Как мы формируем навыки

Наш подход заключается в работе с базовыми заблуждениями в области ИБ, изменением внутренней позиции и только затем – обеспечение знаний, выработка навыков и смена привычек



— это интересно — это важно — я точно в теме?	— микролернинг — непрерывность — автоматизация	— я точно понял? — я точно запомнил? — я точно делаю?
Геймификация, онлайн-интерактивы	Автоматизированная онлайн-платформа	

Вовлечение: онлайн-тренинг
Cybersafety Management Game

Совмещает «обучение и развлечение»

Формат зависит от целей:
- Онлайн и автоматизированно **(20-25 мин)**
- Оффлайн с тренером **(до 4 ч)**

Результат:
- Меняет отношение к кибербезопасности в повседневных рабочих процессах
- Повышает мотивацию учиться дальше
- В среднем 85% участников тренинга готовы рекомендовать его своим коллегам

Вовлечение: Kaspersky Interactive Protection Simulation (KIPS)

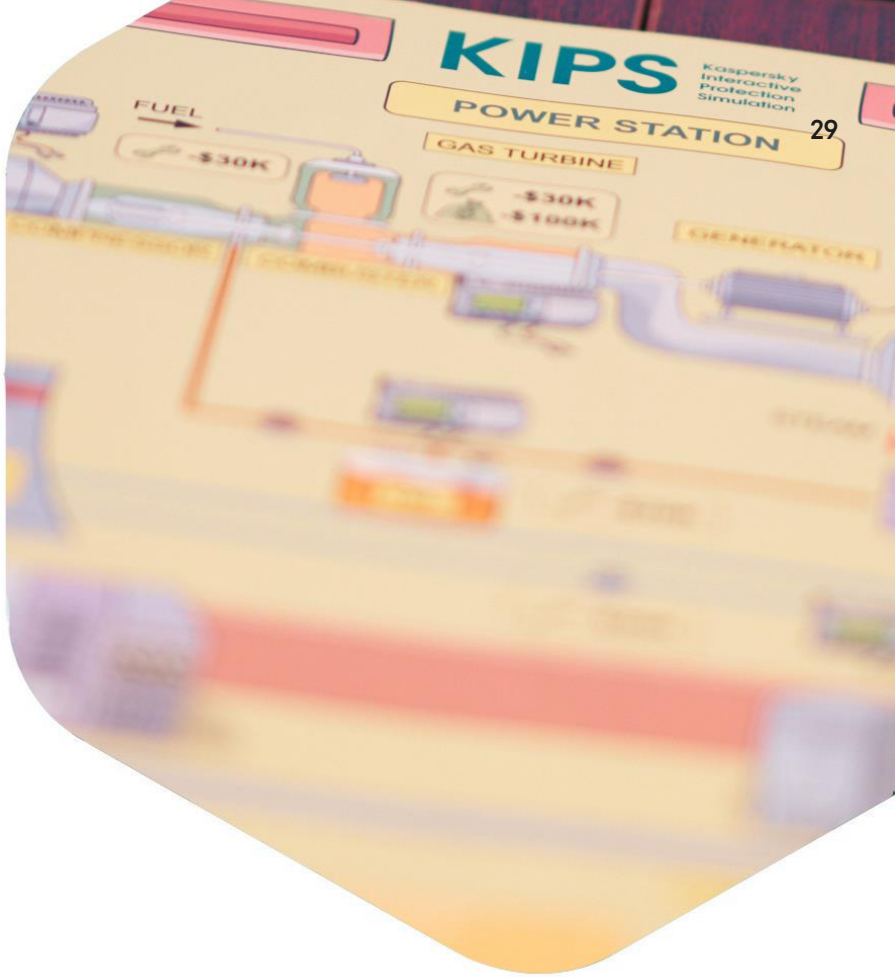
KIPS – командная игра, в которой нужно принимать решения, чтобы отразить атаки киберпреступников и сохранить доход вашей игровой компании.

до 1000
обучающихся за игру (до 300 консолей)

2 часа
длится игра от инструктажа до результатов

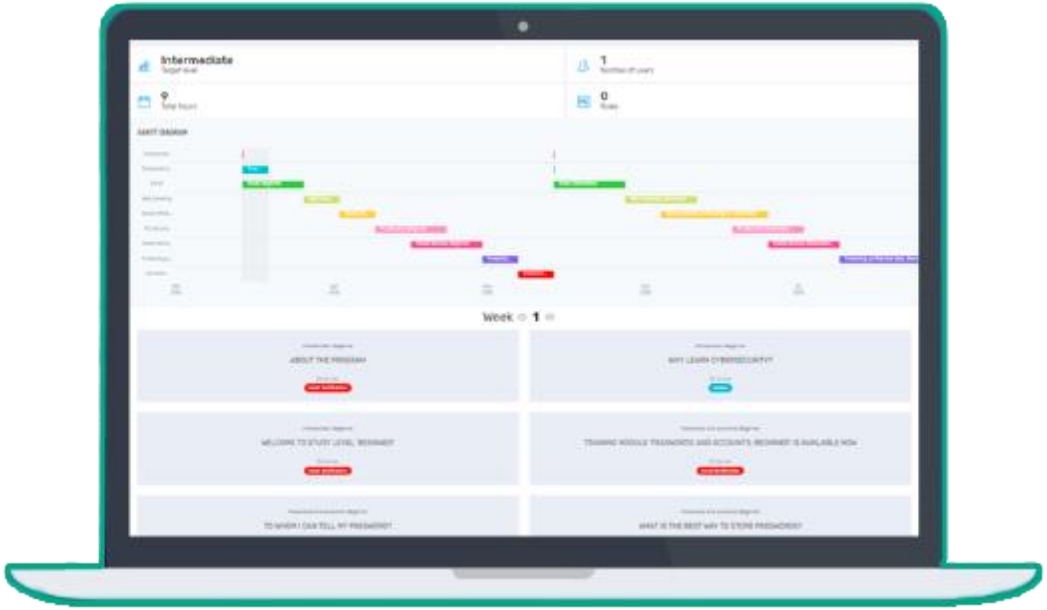
180k чел в 75 странах
уже прошли эту игру

98%
оценивают игру как «интересную и практико-ориентированную»



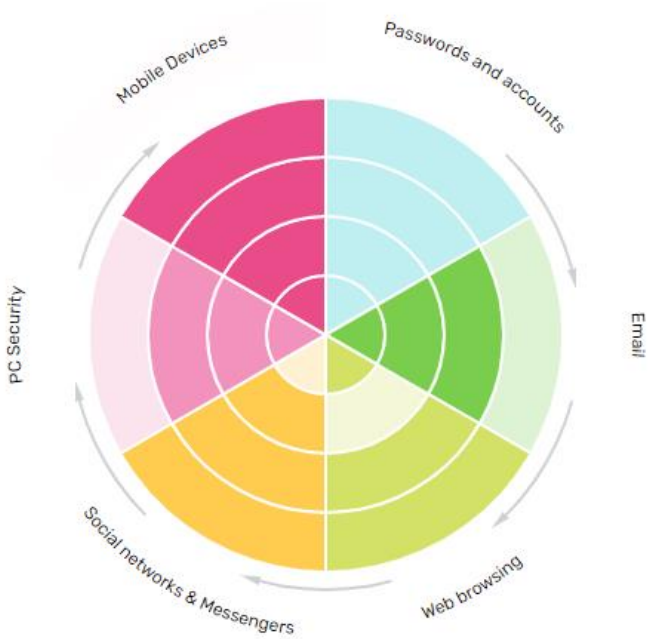
Автоматизированная онлайн-платформа по обучению кибербезопасности

k-asap.com/ru/



1. Четко определить безопасное поведение

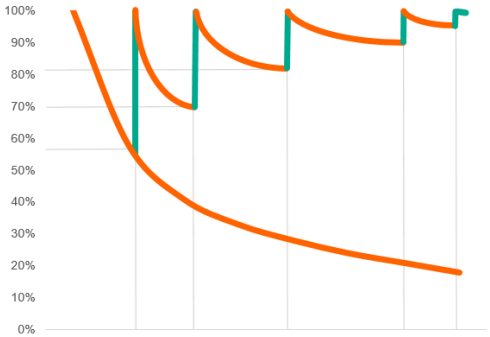
Единая программа обучения



300 практических микро-навыков

- Что может угрожать моей электронной почте?
- Кому можно сообщать свой пароль от почты?
- Что делать, если вашу электронную почту взломали?
- Какие пароли следует использовать для своих почтовых сервисов?
- Почему для корпоративной и личной электронной почты нужно использовать разные пароли?
- Какие данные не стоит отправлять по электронной почте?
- На что обращать внимание, если вас просят ввести пароль от почтового аккаунта?
- Опасны ли ссылки, состоящие только из цифр?
- Все ли вложения в электронные письма стоит открывать?
- Что стоит сделать в отношении своих почтовых аккаунтов уже сегодня?

2. Выстроить последовательный путь обучения



Кривая забывания Эббингауза

Многократное повторение прочно закрепляет навыки

- Obliteration
- Remembering after reinforcement

NEW LEVEL

NEXT TOPIC

Interactive lessons

Reinforcement email/ case study

Test

Simulated phishing attack

4 days later

3 days later

3 days later

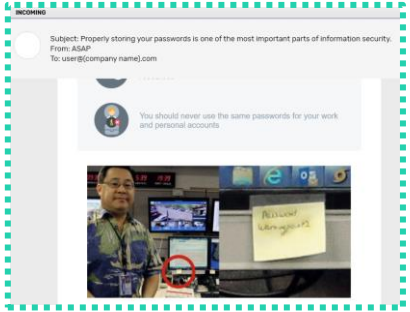
Level 1 topics are studied

3. Использовать мультимодальный контент, чтобы закрепить навык

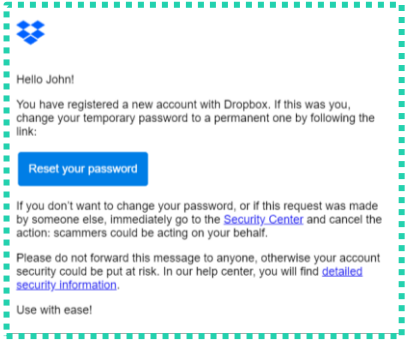
Интерактивные уроки

Тесты

Закрепление



Симулятор фишинга



Выводы

1. Обновляйте все ПО регулярно
2. Используйте сложные и разные пароли. Обновляйте регулярно
3. Убедитесь, что домашная wi-fi сеть безопасна. Работайте под VPN.
4. Установите антивирусное ПО и настройте защитный экран
5. Используйте виртуальные машины
6. Разделите учетные записи
7. Помните о фишинге
8. Проведите обучение сотрудников, ориентированное на изменение поведения

Берегите себя

Kaspersky Academy

kaspersky.com/awareness academy@kaspersky.com awareness@kaspersky.com

kaspersky