

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Психология цифровых атак

Ольга Лимонова psy@antiphish.ru



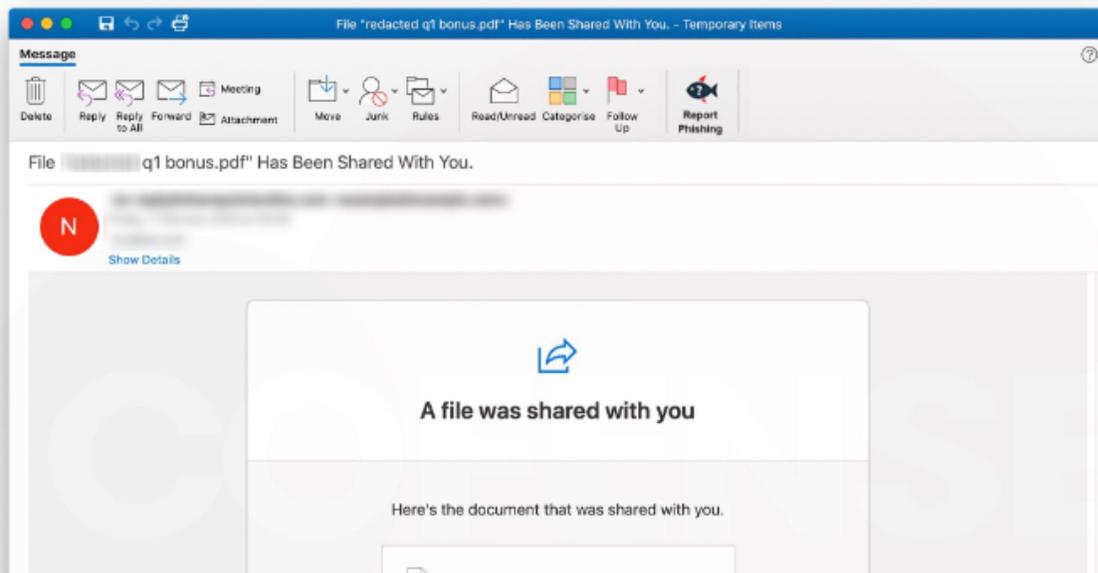
blog.antiphish.ru

Антифишинг-дайджест № 171 с 15 по 21 мая 2020 года

Представляем новости об актуальных технологиях фишинга и других атаках на человека с 15 по 21 мая 2020 года

Почта

Организаторы новой фишинговой кампании научились обходить многофакторную аутентификацию в Office 365, чтобы получить доступ к данным жертв в облаке.



[Андрей Жаркевич](#)
редактор



[Артеми́й Богданов](#)
технический директор



[Сергей Волдохин](#)
выпускающий редактор





1. Введение в проблему

Общая информация про обучение и тренировку навыков

(Знания + Навыки) + Измерение



Тренируйте
и измеряйте
ЭТИ НАВЫКИ

Модель Антифишинга



Модель Антифишинга



antiphish.ru/classification



Outline

- Антифишинг — сервис об...
- Классификация цифровы...
- Технологические векторы циф...
- Электронная почта
- Сайты
- Социальные сети
- Мессенджеры
- Офис, рабочие помещения
- Дополнительные технологиче...
- Работа через устаревшие в...
- Разнообразие версий опера...
- Использование нелицензио...

Психологические векторы атаки

Страх

«Ваш компьютер заражен и заблокирован. Кликните здесь»

Раздражение

«Чтобы отписаться, перейдите по ссылке»

Невнимательность

«www.sberbank.ru», «www.gmall.com»

Любопытство

«Смотри, как ты отжигашь на видео»

Жадность

«Скидка 50% при оплате прямо сейчас»

Желание помочь

«Кажется, ваш коллега потерял свои вещи. Дайте мне его номер»



antiphish.ru/template

Ид	Сценарий	Вектора атаки	Технологии
1	Руководитель HR-отдела обращается к сотруднику по имени и сообщает, что заключен договор с новой компанией ДМС. Обещают бесплатную стоматологию и полный чек-ап в известном медицинском центре. Полный список услуг во вложении. Полисы в этом месяце получают только те, кто перейдет по ссылке.	Корпоративная Персональная Жадность Любопытство Срочность	Эл. письмо Вложение MS Word Ссылка



2. Разбор атак

Применение модели Антифишинг

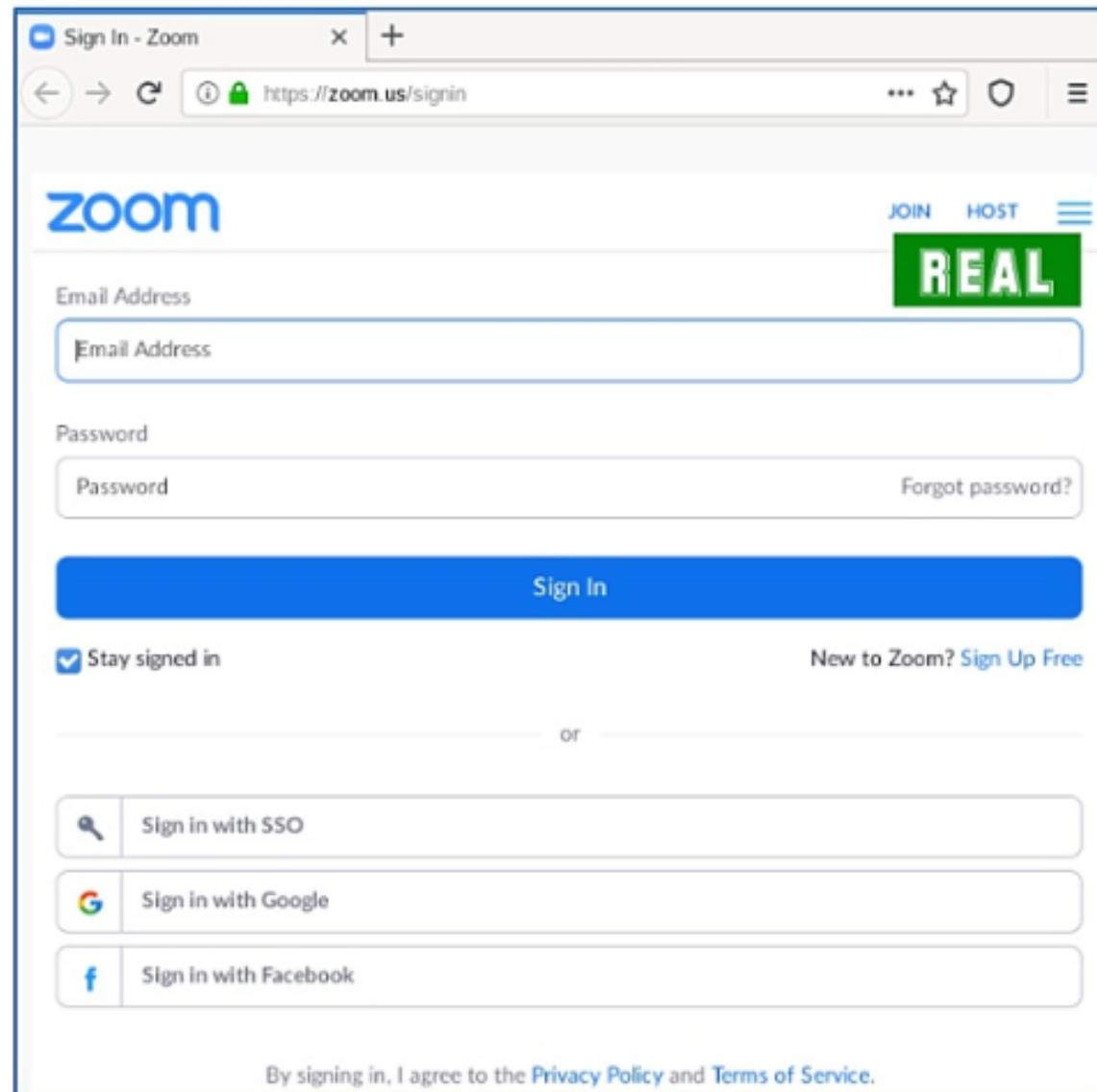
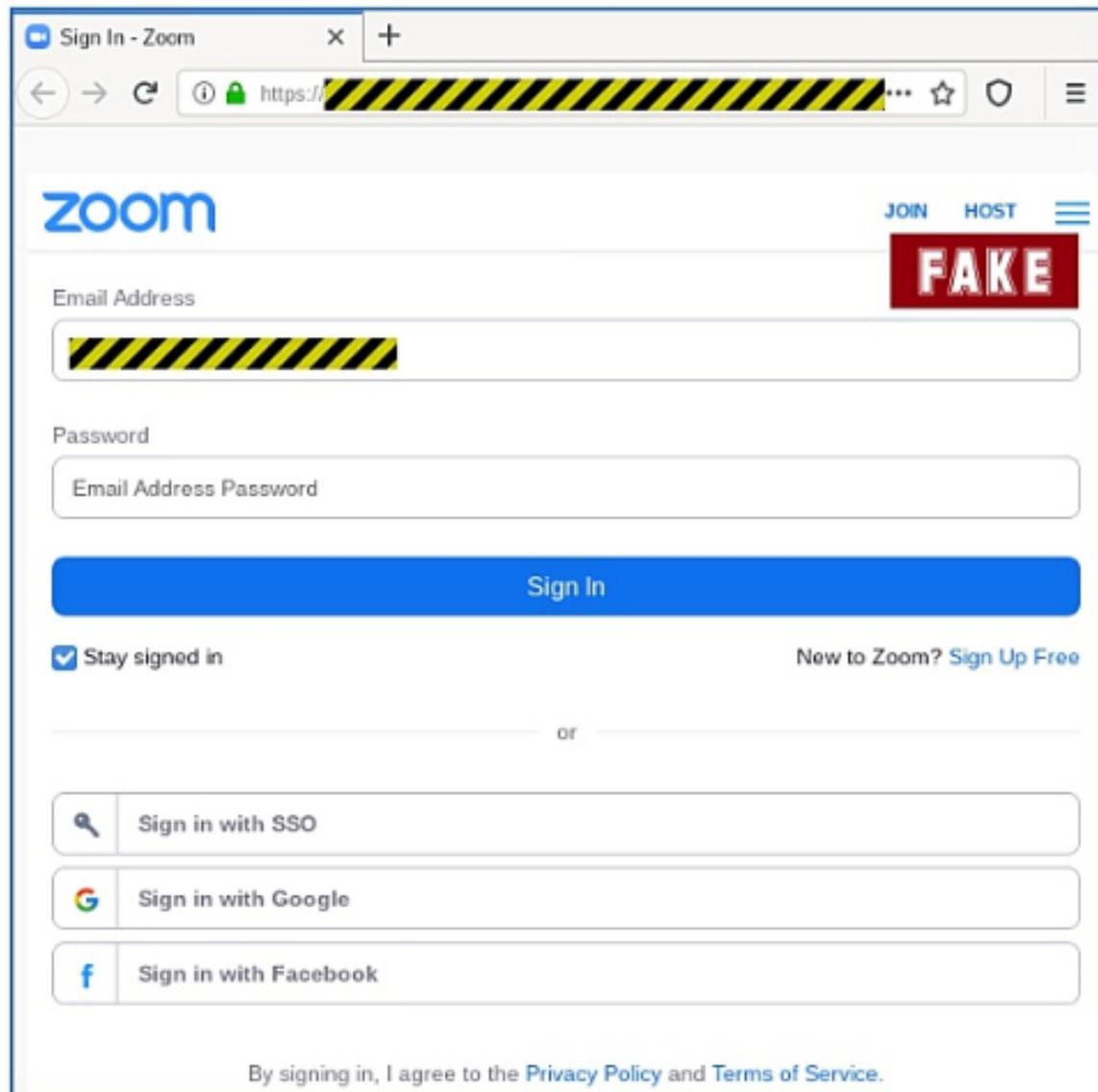
Join your bbbbb.example CEO and Management Board Meeting for all staffs on Zoom Meeting

This is a reminder that your zoom meeting appointment with **H.R and Audit Head** will start in few minutes.

Your presence is crucial to this meeting and equally required to commence this **Q1 perfomance review** meeting

[Join this Live Meeting](#)





Желание помочь

Страх

Срочность

Авторитет

Join your bbbbbb.example CEO and Management Board Meeting for all staffs on **Zoom Meeting**

This is a reminder that your zoom meeting appointment with **H.R and Audit Head** will **start in few minutes.**

Your presence is crucial to this meeting and equally required to commence this **Q1 performance review** meeting

[Join this Live Meeting](#)

От: Аптека Р+ <apteka_ru@inbox.ru> ☆

← Ответить

↶ Ответить всем

→ Переслать

Больше ▾

Тема: **Как не заболеть коронавирусом**

27.03.2020, 13:33

Кому: [REDACTED]

Дарим “вакцину” от коронавируса!

Вернее, просто разъясним некоторые моменты, которые непонятны многим, по всей видимости.

Не надо писать, что лечения от вируса нет. Нет вакцины! А лечение ЕСТЬ! Оно, как при пневмонии или острой форме гриппа. Потому что коронавирус и есть грипп.

Грипп — острое инфекционное заболевание дыхательных путей, вызываемое вирусом гриппа. А их существует более двух тысяч видов, включая коронавирус.

По вопросу смертей. Если у человека ослабленный иммунитет, хронические заболевания, плохой образ жизни, несбалансированное питание, вредные привычки и прочее, бонусом - он ещё и несвоевременно обратился за медицинской помощью - да, возможен летальный исход. Но! Внимание! Точно также, как и от другого гриппа. Отличие коронавируса – скорость поражения лёгких. Но тут вопрос времени: вашего и врачей. Никак не «смертельный вирус, от которого нет лечения и мы все умрём».

В итоге: и заражение, и лечение, и профилактика коронавируса такие же, как и от других вирусов из рода гриппа.

Хотим поделиться с вами лучшими на данный момент средствами профилактики, которые вы легко сможете приобрести по доступной цене в любой из аптек, а так же расскажем о способах их применений в краткой презентации по ссылке: <http://spectrplus.com>

[/Рекомендации по применению профессиональных стандартов от Аптекаг.zip](#)

Так же у нас на сайте вы можете приобрести противоинфекционные маски в любых количествах. Доставка бесплатна и производится в течении двух дней.

С наилучшими пожеланиями и будьте здоровы!

Аптека.ру

От: Аптека Р+ <apteka_ru@inbox.ru> ☆

← Ответить ← Ответить всем → Переслать

Личная

Тема: Как не заболеть коронавирусом

Кому:

Дарим "вакцину" от коронавируса!

Жадность

Вернее, просто разъясним некоторые моменты, которые непонятны многим, по всей видимости.

Не надо писать, что лечения от вируса нет. Нет вакцины! А лечение ЕСТЬ! Оно, как при пневмонии или острой форме гриппа. Потому что коронавирус и есть грипп.

Любопытство

Грипп — острое инфекционное заболевание дыхательных путей, вызываемое вирусом гриппа. А их существует более двух тысяч видов, включая коронавирус.

По вопросу смертей. Если у человека ослабленный иммунитет, хронические заболевания, плохой образ жизни, несбалансированное питание, вредные привычки и прочее, бонусом - он ещё и несвоевременно обратился за медицинской помощью - да, возможен летальный исход. Но! Внимание! Точно также, как и от другого гриппа. Отличие коронавируса – скорость поражения лёгких. Но тут вопрос времени: вашего и врачей. Никак не «смертельный вирус, от которого нет лечения и мы все умрём».

В итоге: и заражение, и лечение, и профилактика коронавируса такие же, как и от других вирусов из рода гриппа.

Хотим поделиться с вами лучшими на данный момент **средствами профилактики, которые вы легко сможете приобрести по доступной цене в любой из аптек, а так же расскажем о способах их применений в краткой презентации по ссылке: <http://spectrplus.com>**
[/Рекомендации по применению профессиональных стандартов от Аптекаг.zip](#)

Так же у нас на сайте вы можете приобрести противоинфекционные маски в любых количествах. Доставка бесплатна и производится в течении двух дней.

С наилучшими пожеланиями и будьте здоровы!
Аптека.ру

Комплексный проект по созданию жилищно-строительных кооперативов для работников «об...

 **Д Д¾¼ÑÑ, DμÑ** <info@rostec.ru>
To fgup@ao-avtomatika.ru

↩ Reply ↩ Reply All → Forward ⋮

ⓘ Outlook blocked access to the following potentially unsafe attachments: Комплексный проект по созданию жилищно-строительных кооперативов для работников обороны.exe.

Добрый день, уважаемые коллеги!

К Дню первого мая направляю вам комплексный проект, направленный на улучшение жилищных условий работников «оборонки»

Вам от души поздравляю!

С уважением,



Полюшкина Елена Валерьевна
Департамент правового обеспечения
и корпоративного управления



Комплексный проект по созданию жилищно-строительных кооперативов для работников «...

 Д Д¾ÑÑ,ДµÑ.. <info@rostec.ru>
To fgup@ao-avtomatika.ru

Reply Reply All Forward

Outlook blocked access to the following potentially unsafe attachments: Комплексный проект по созданию жилищно-строительных кооперативов для работников оборонки.exe.

Добрый день, уважаемые коллеги!

К Дню первого мая направляю вам комплексный проект, направленный на улучшение жилищных условий работников «оборонки»

Вам от души поздравляю!

С уважением,

 **Ростех**
Партнер в развитии
Полюшкина Елена Валерьевна |
Департамент правового обеспечения
и корпоративного управления

Корпоративная

Жадность

Авторитет



От: Reg.ru <mail2@valeggini.it>

Дата: 29.04.2020, 11:37

Кому: salt-torg.ru <salt-torg.ru>

Тема: Служба приостановки - salt-torg.ru

Уважаемые клиенты, дорогие клиенты,

Это уведомление, чтобы сообщить вам, что ваша учетная запись была приостановлена.

Подробная информация об этой подвеске приведена ниже:

Доменное имя: salt-torg.ru

Причина приостановки: Наша платежная система обнаружила, что срок действия вашего доменного имени истек, а не продлен, несмотря на наше предыдущее повышение.

Для повторного его активации, вас просят вручную заполнить форму обновления для ваших услуг в соответствии с инструкциями и шагами по ссылке ниже:

<https://www.reg.ru/payment>

В случае неуплаты, ваш счет будет приостановлен в течение нескольких часов.

Пожалуйста, свяжитесь с нашей службой поддержки клиентов в случае каких-либо проблем или любых других вопросов: support@reg.ru

С наилучшими пожеланиями

Команды REG.ru



От: Reg.ru <mail2@valeggini.it>

Дата: 29.04.2020, 11:37

Кому: salt-torg.ru <salt-torg.ru>

Тема: Служба приостановки - salt-torg.ru

Уважаемые клиенты, дорогие клиенты,

Это уведомление, чтобы сообщить вам, что **ваша учетная запись была приостановлена.**

Подробная информация об этой подвеске приведена ниже:

Доменное имя: salt-torg.ru

Причина приостановки: Наша платежная система обнаружила, что срок действия вашего доменного имени истек, а не продлен, несмотря на наше предыдущее повышение.

Для повторного его активации, **вас просят вручную заполнить форму обновления для ваших услуг** в соответствии с инструкциями и шагами по ссылке ниже:

<https://www.reg.ru/payment>

В случае неуплаты, ваш счет будет приостановлен в течение нескольких часов.

Пожалуйста, свяжитесь с нашей службой поддержки клиентов в случае каких-либо проблем или любых других вопросов: support@reg.ru

С наилучшими пожеланиями

Команды REG.ru

 Внешняя

Страх

Срочность

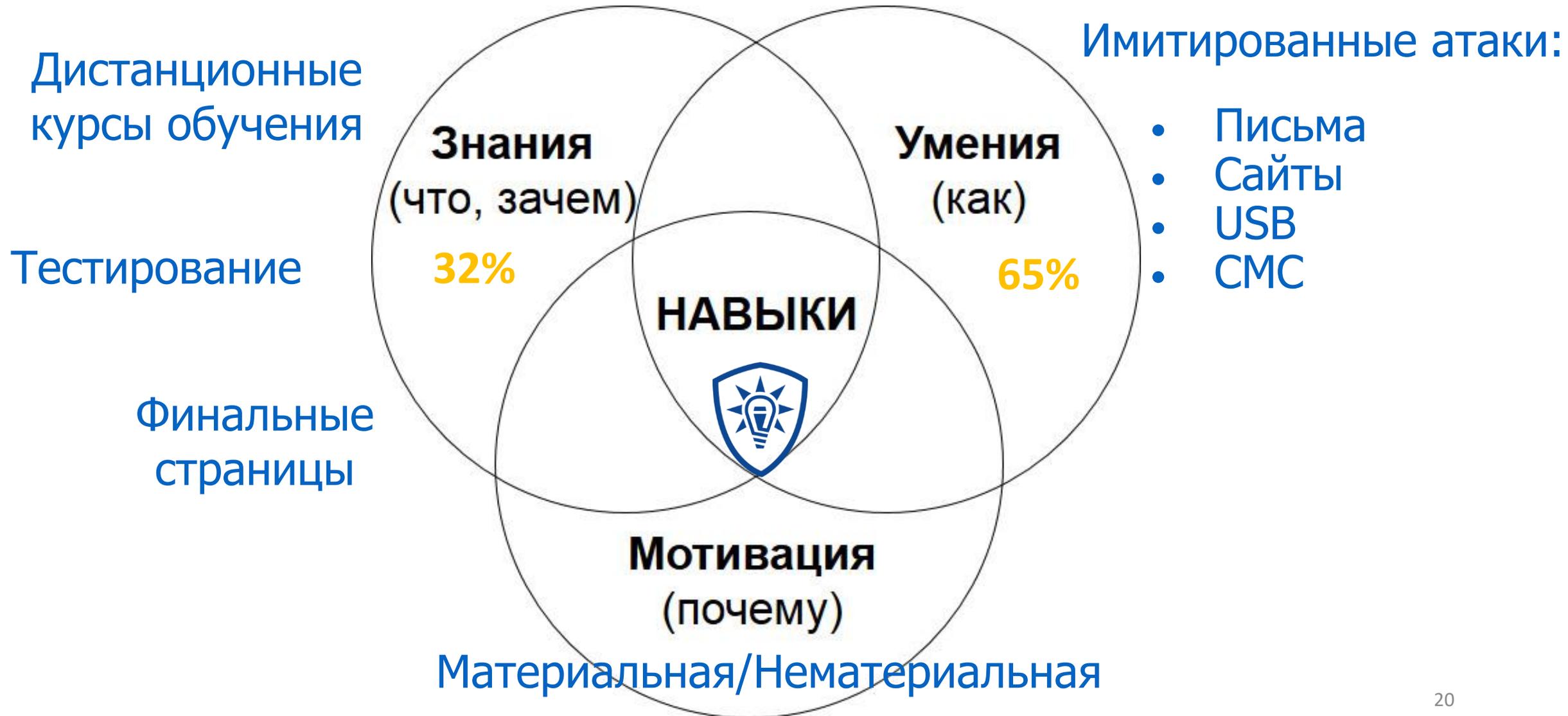




3. Мотивация

Как формируются навыки и почему важна мотивация

Как формируются навыки?



Используйте элементы мотивации:

- в процессах ИБ
- в интерфейсе платформ обучения



Эпический смысл

- 89% компаний заявили, что улучшение безопасности повышает лояльность и доверие клиентов
- 90% сообщили, что безопасность усилила их репутацию
- 89% указали, что безопасность стала конкурентным отличием которое помогло завоевать клиентов

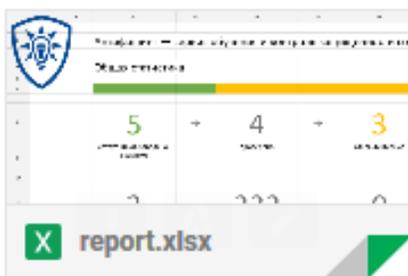


Обратная связь

Основной отчёт



Антифишинг <noreply@antiphish.ru>
кому: limonova



ОБРАТНАЯ СВЯЗЬ



Какие действия выполнялись?

Какие были отклонения?

Что можно было сделать по-другому для достижения цели?

Естественная среда

Входящие - info@compbegin.ru - Outlook

ОАЙЛ ГЛАВНАЯ ОТПРАВКА И ПОЛУЧЕНИЕ ПАПКА ВИД Bluetooth

Создать сообщение Создать элемент
Отметить как спам Отметить как не спам Удалить
Ответить Ответить всем Переслать
Переместить в: ? Переместить
Руководителю
Сообщение гр...
Правила
OneNote
Поиск людей
Адресная книга
Фильтр почты
Отправить и получить почту — все папки
Отправка и получение

Избранное
Входящие 1
Отправленные
Удаленные

info@compbegin.ru
Входящие 1
Черновики
Отправленные
Удаленные
RSS-каналы
Исходящие
Нежелательная почта
Папки поиска

Поиск в папке "из текущего почтов... из текущего почтового ящика

Все Непрочитанные По Дата Новые

Сегодня

Валерий Чугунков
Тестовое сообщение 16:26
Привет! Это тестовое сообщение. <конец>

Пятница

robocommentit@www.compbegin.ru
Новый комментарий на Вашем сайте. Пт 24.01
Новый комментарий на странице

robocommentit@www.compbegin.ru
Новый комментарий на Вашем сайте. Пт 24.01
Новый комментарий на странице

Вторник

robocommentit@www.compbegin.ru
Новый комментарий на Вашем сайте. Вт 21.01
Новый комментарий на странице

Понедельник

Вс 26.01.2014 16:26
Валерий Чугунков
Тестовое сообщение
Кому info@compbegin.ru

Привет! Это тестовое сообщение.

Подробнее о Валерий Чугунков.

Система личных достижений

Мой рейтинг —



Новичок 🤔

ДОСТИЖЕНИЯ

Вы получили 67 из 149 (44%)



Вечеринка Окончена

В публичных матчах 100 раз повредите Генератор, пока хотя бы один Вьживший висит на крюке.



+59

Неполученные достижения



+75

Мои достижения

Обучайте и тренируйте своих людей!



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

www.antiphish.ru

psy@antiphish.ru