Приоритеты и последствия

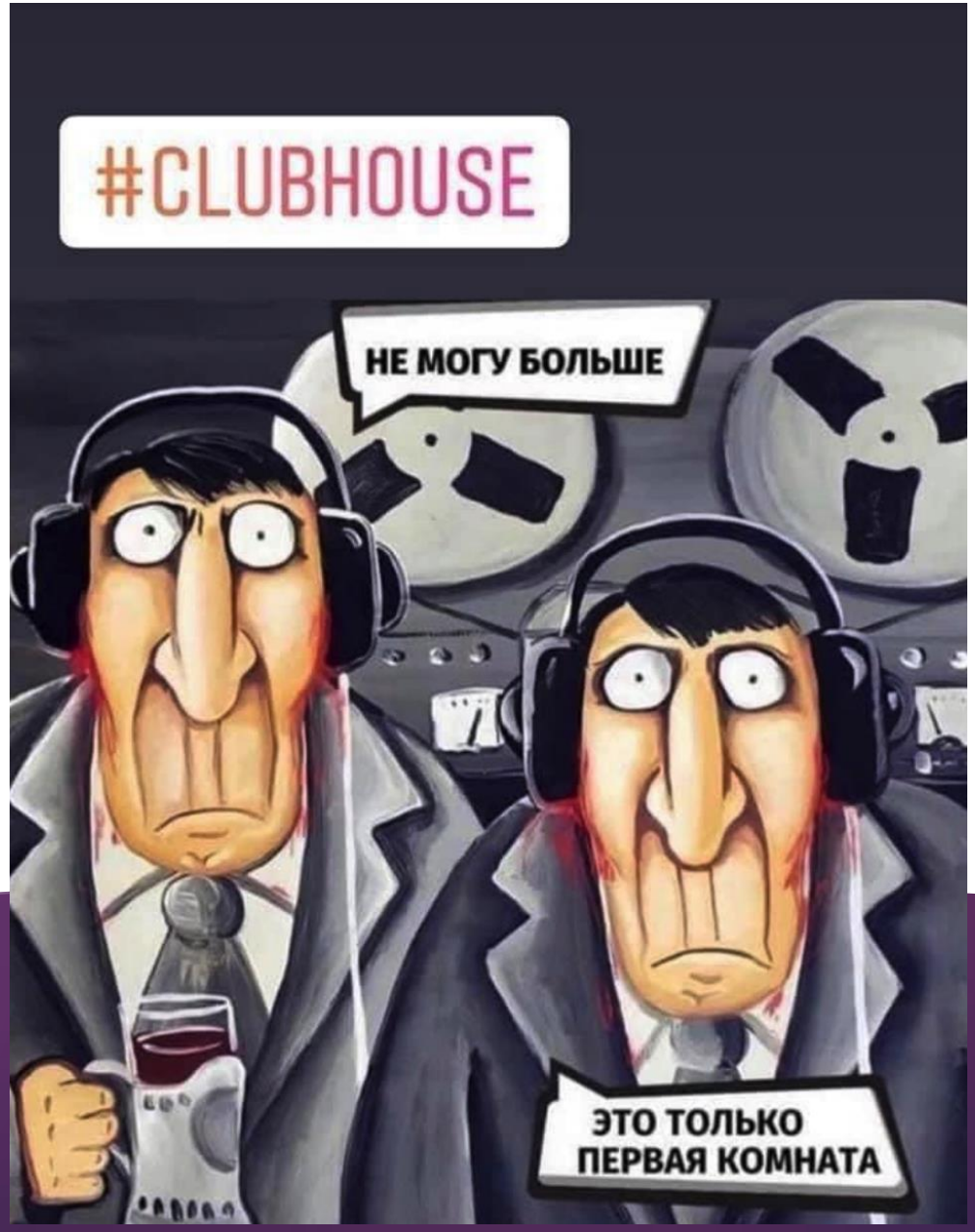
ПОЧЕМУ НЕ НАДО ВНЕДРЯТЬ SECURITY AWARENESS, И КАК БЫ ОТ ЭТОГО ЧЕГО НЕ ВЫШЛО…

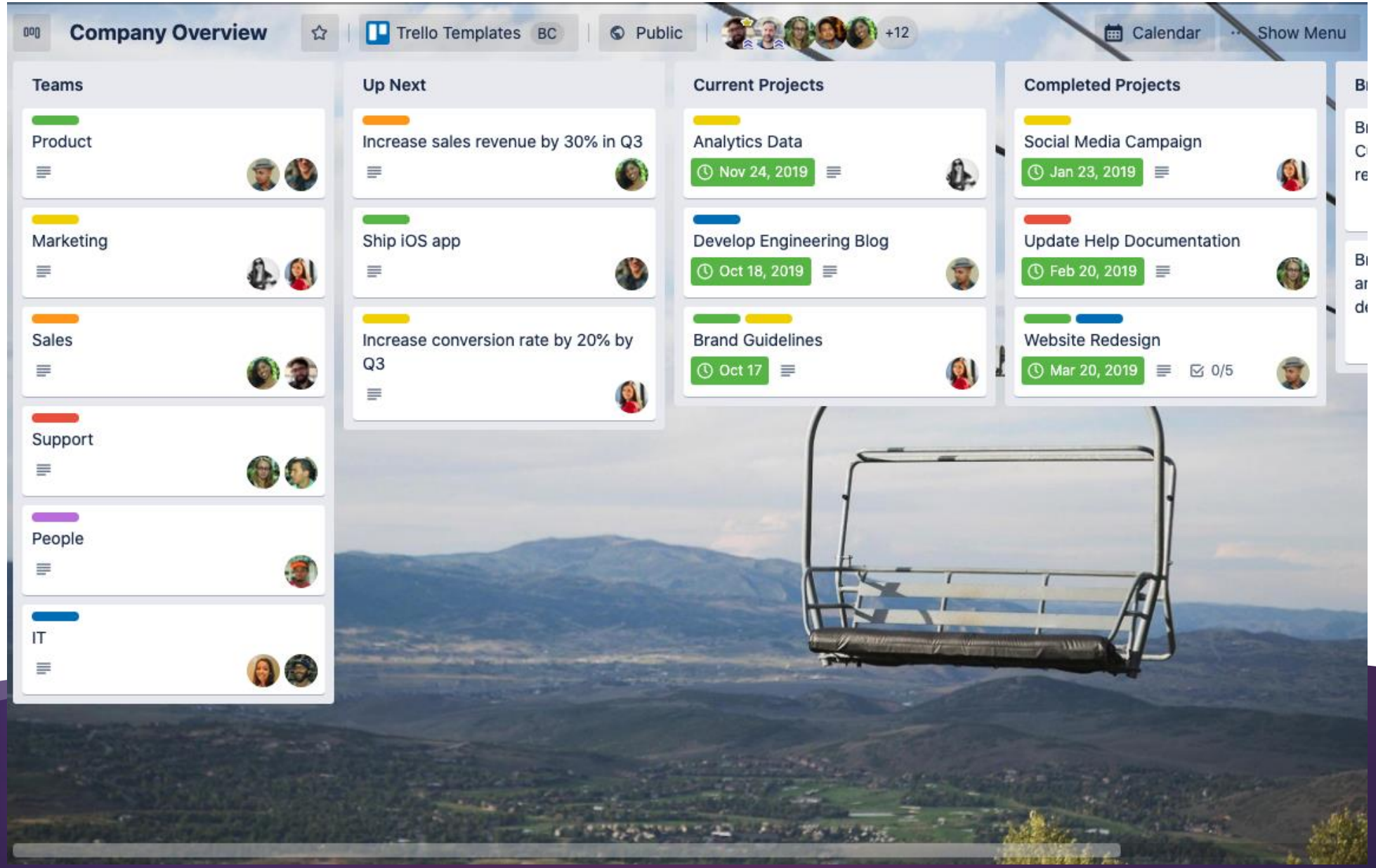
ЕВГЕНИЙ ПИТОЛИН

ЭКСПЕРТ ПО КИБЕРБЕЗОПАСНОСТИ

Эксперт?


Как можно говорить о вещах, в которых ты не разбираешься?
Рот открываешь и говоришь
©Кир. Анастасин
komikaki.ru


#CLUBHOUSE
НЕ МОГУ БОЛЬШЕ
ЭТО ТОЛЬКО ПЕРВАЯ КОМНАТА


Company Overview
Trello Templates
BC
Public
+12
Calendar
Show Menu
Teams
Product
Marketing
Sales
Support
People
IT
Up Next
Increase sales revenue by 30% in Q3
Ship iOS app
Increase conversion rate by 20% by Q3
Current Projects
Analytics Data
Nov 24, 2019
Develop Engineering Blog
Oct 18, 2019
Brand Guidelines
Oct 17
Completed Projects
Social Media Campaign
Jan 23, 2019
Update Help Documentation
Feb 20, 2019
Website Redesign
Mar 20, 2019
0/5

How I used a simple Google query to mine passwords from dozens of public Trello boards

Kushagra Pathak Follow

May 9, 2018 · 5 min read

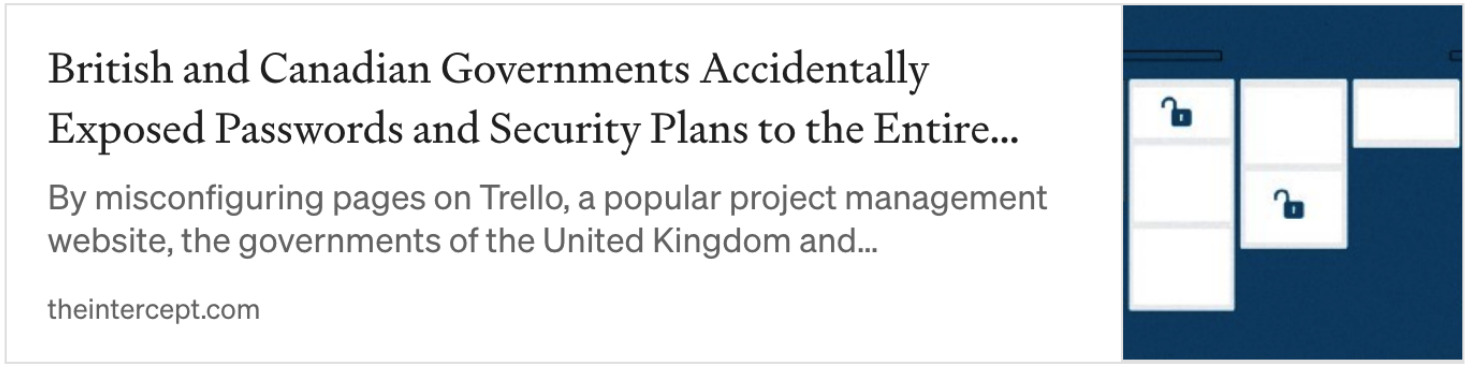
How I used a simple Google query to mine passwords from dozens of public Trello boards

Kushagra Pathak Follow

May 9, 2018 · 5 min read

Update —17 August 2018:

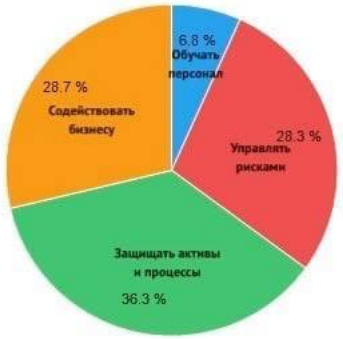
In the recent months I had discovered a total of **50 Trello Boards of the British and Canadian governments** containing internal confidential information and credentials. The Intercept wrote a detailed article about it here.



ПРИОРИТЕТЫ

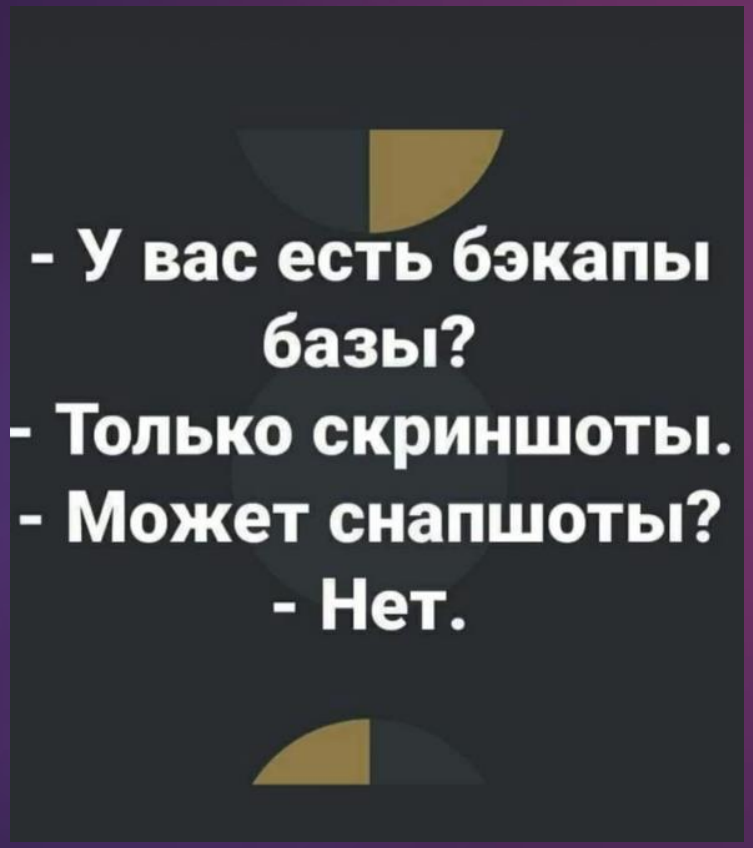
Чем занят ум CISO?

Миф



Реальность

Не назло, а вопреки



Развернуть новую систему защиты от целевых атак – дорого, да и зачем мы нужны злоумышленникам?

Купить новый LX 570 директору – ну нормально же, к уважаемым людям ездит.

Организовать своевременный пентест и определить слабые места заблаговременно – дорого, да и вдруг про нас сольют эту инфу?

Заплатить авторам шифровальщика $25k срочно чтобы 1С заработала – ну а что делать, не повезло..

Выделить денег на 2-3 вакансии в штат ИБ, чтобы сбалансировать нагрузку – ну нееет, мы не будем раздувать штат.

Заплатить 6М рублей за 2 недели срочного расследования инцидента – да легко!

5 шагов
по «продаже»
security awareness
изнутри

1. Начинать с самого верха.

ТОЛЬКО CEO,

только лично,
никаких технических
нюансов.

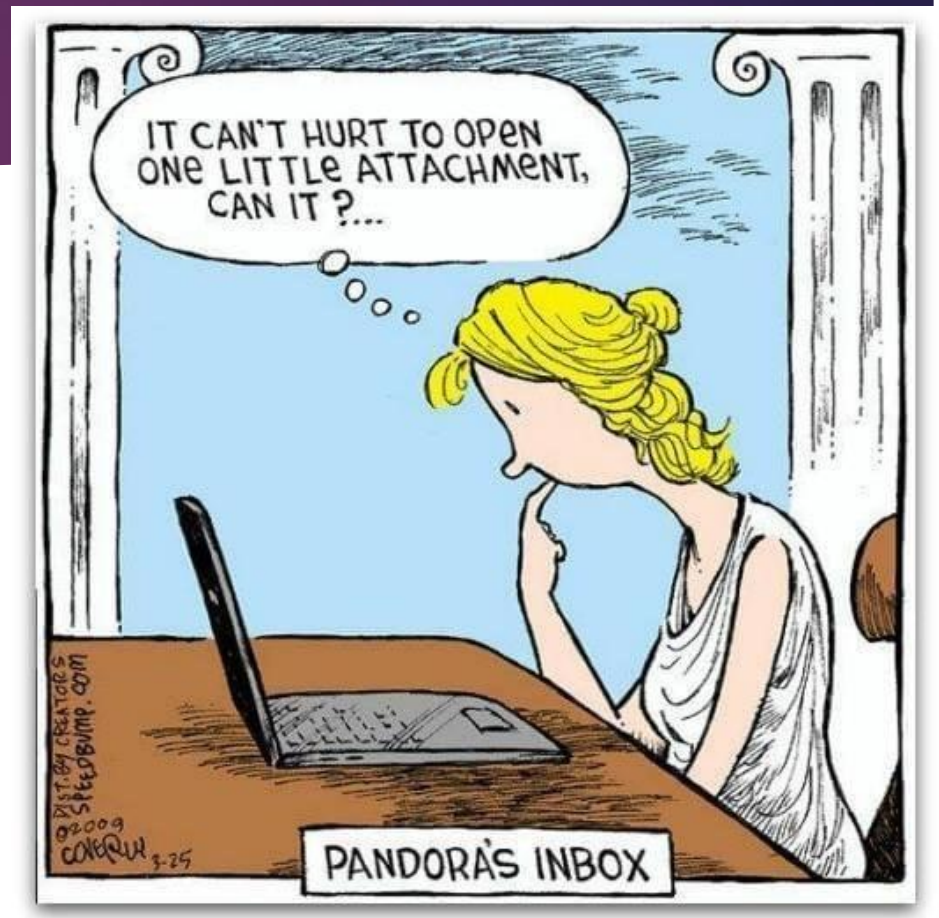
3-5 минутный доклад

в самое сердце

2. ФИШИНГОВАЯ РАССЫЛКА
(БЕЗОПАСНАЯ☺)

1) От имени CEO
2) В сторону CEO от любого другого значимого объекта

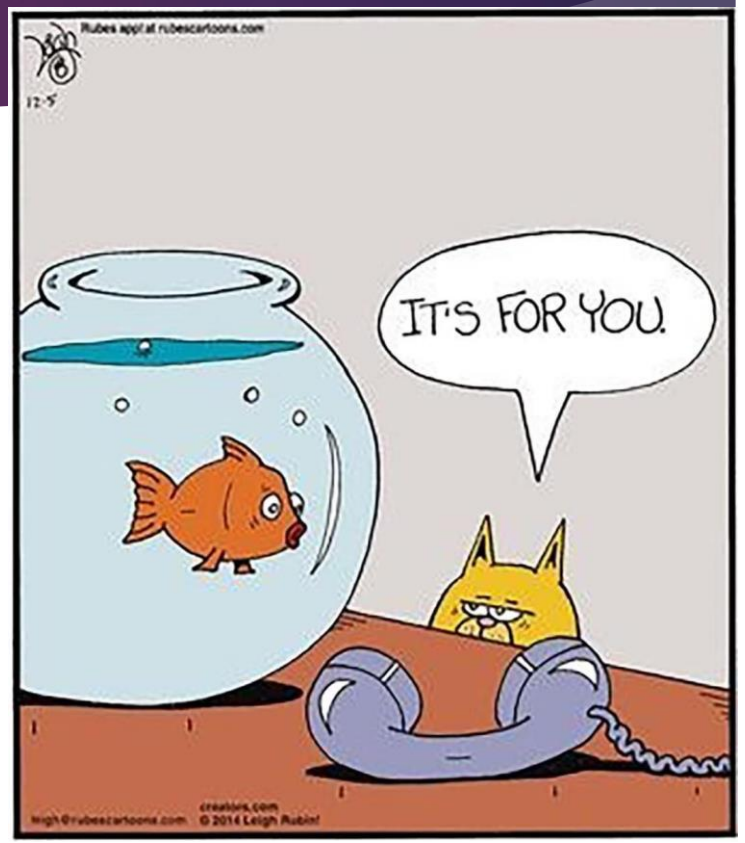
В ИТОГЕ – реальный срез кибергигиены, и сразу видны слабые звенья



3. СОЗДАТЬ ИБ-КУЛЬТУРУ, НАЧАТЬ ИСПОЛЬЗОВАТЬ ЭЛЕМЕНТЫ ГЕЙМИФИКАЦИИ, ДОСТИЖЕНИЯ, БОНУСЫ

4. ВНЕДРИТЬ НЕОБХОДИМЫЙ НАБОР ИНСТРУМЕНТОВ

1. Срез культуры ИБ (Ассесмент)
2. Онлайн-платформа
3. Персональные и групповые тренинги
4. Курсы для новичков
5. Раздаточные и информационные материалы
6. Обучение для тренеров / адоптеров (адвокатов дьявола)



5. ПРОВЕСТИ ГЛОБАЛЬНЫЕ КИБЕРУЧЕНИЯ ВНУТРИ КОМПАНИИ

И чо? / So what?

Все будет работать, если обучение:

- не абстрактно, привязано к конкретным рабочим ситуациям;
- не мешает выполнению основных задач;
- использует примеры из реальной жизни;
- дает исполнимые советы

И самое главное

Не усложнять.

Дать возможность действовать.

Демонстрировать результаты.

И самое главное - 2