eQUALITYtime

TIGHTROPE

Guide for Teachers

Table of Contents

Introduction

Welcome to the Tightrope Project, a comprehensive guide for teachers who want to safely guide their students to create social change.

In today's world, it is more important than ever to empower young people to take action and become the change they want to see in the world. However, it is equally important to ensure that they do so in a safe and responsible way. This guide is designed to equip you with the tools and resources you need to create a positive and inclusive classroom environment, foster critical thinking and dialogue, and support your students in developing effective strategies for creating social change. Whether you are a new teacher or a seasoned educator, the Tightrope Project has something for everyone.

Dutch students protesting about building conditions, 1973, Used under licence from https://www.flickr.com/photos/nationaalarchief/3922564838/

Motivation

Students are increasingly becoming involved in social change as they recognize the importance of making a positive impact on society. This can be seen in a growing interest in social activism, with movements such as the Black Lives Matter protests in the UK and the student-led movement for gun control in the United States. Students are motivated by a desire to create a more just and equitable world and to have their voices heard. They are also concerned about issues such as climate change, inequality, and discrimination, and are eager to make a difference. By being involved in social change, students are able to develop valuable skills, including leadership, teamwork, and problem-solving, and become active and engaged citizens who can make a positive impact on their communities.

It is important for students to understand how to keep themselves safe when taking action for social change for several reasons. Firstly, many students may be targeted by online trolls, hate groups or others who oppose their message and may be at risk of experiencing cyberbullying or harassment. Additionally, there is a risk of students falling victim to online scams or phishing attempts when using social media to promote their cause (Childnet International, 2021). Finally, students may be targeted by law enforcement or other authorities if their activities are deemed to be illegal or disruptive.

High school students protesting in favour of gun control, 2018, Used under licence from https://www.flickr.com/photos/fibonacciblue/40409777241/

To mitigate these risks, it is crucial that students understand how to keep themselves safe while taking action for social change. This includes understanding the legal implications of their activities and taking steps to ensure that they are not breaking any laws or engaging in activities that could result in harm to themselves or others.

Moreover, teaching students how to take action for social change in a safe and responsible way also helps to develop essential life skills such as critical thinking, problem-solving, and decision-making. It can help students to develop a sense of agency and empowerment, and foster a lifelong commitment to social justice and activism.

Background

The Tightrope Project is a unique and innovative initiative that has brought together two distinct areas of expertise - cybersecurity and social change. The project was developed by a team of experts in these fields who recognized the need for a comprehensive guide to help teachers empower students to create social change in a safe and responsible way. The collaboration between cybersecurity and social change experts has led to several advantages that make this guide invaluable for teachers.

Firstly, by combining the knowledge and experience of cybersecurity and social change experts, the Tightrope Project has been able to identify the potential risks and challenges that young people may face when attempting to create social change through online platforms. Cybersecurity experts have provided guidance on how to keep students safe while using technology, while social change experts have provided insights into how to promote positive change without inadvertently causing harm.

Secondly, the collaboration between these experts has resulted in a holistic approach to social change that takes into account both the online and offline worlds. The project acknowledges that the use of social media and other online platforms has become a powerful tool for social change, but it also recognizes the importance of taking action in the real world. By combining these two approaches, the Tightrope Project provides teachers with a comprehensive guide that addresses both aspects of social change.

Finally, the collaboration between cybersecurity and social change experts has led to the creation of a guide that is practical and easy to use. The Tightrope Project provides teachers with step-by-step instructions on how to guide students through the process of creating social change, while also providing them with the necessary resources and tools to do so in a safe and responsible way.

What this course is not

This course covers online safety - it does not cover topics like the following:

- Strong passwords
- VPNs
- Two factor authentication

- Anti-virus software.

Some of those practices are useful in everyday life and it is good to give that information to the students - but our course focuses on the more complex aspects of security, its relationship to power and access, and the trade-offs that people and organisations make every day and attempts to give the students the ability to accurately assess risk for themselves, but also their families and communities.

Lesson Plans

We provide teachers with six lesson plans that are designed to help students learn how to create social change in a safe and responsible way. The lessons cover a range of topics, from identifying social issues to developing strategies for creating change. Each lesson is structured to be flexible, allowing teachers to tailor the content to their students' needs and interests.

The six lesson plans are as follows:

1. Introduction - a discussion and exercise on the topic of security in the broad sense - including motivations and capabilities of attackers. The second half of the session is on recasting the social change into more immediate and personal goals like “Start a fencing club”, “advocate against animal testing”[1]. The key message of the session is “You secure things by making things hard to use and sometimes that is bad”.
2. Information - this session gives a four step framework for making changes and starts by asking the students to consider the difference between complaining and actually taking action to achieve change. The session focuses on ‘information’ and includes an introduction to Freedom of Information requests.
3. Privacy and Threat Modelling. This session examines a group of different activists and invites the students to understand why some conceal their identity and some don’t. It examines a case study of a very traumatic harassment campaign against an activist for trans-rights and discusses the production of risk assessments.
4. Cryptography. This session introduces Cryptography and discusses how it is used to secure communications in general.
5. Complex Systems. This session leads the students through a set of increasingly complex security systems - starting with the workplace, moving through friendships and relationships and ending with the family[2]. For each example we discuss the challenges inherent to each context and how to manage them.
6. Scams, magic,and future directions. This session has three roles. It’s a general overview of some common scam structures. It’s also a chance to catch up on the

[1] Or indeed “advocate in favour of animal testing” - we are deliberately neutral on what students want to achieve as long as they are safe doing it. The set change cards discussed below contain a lot of pairs of cards that are direct opposites.

[2] Ironically the workspace is inherently very easy to secure - there are clear sets of rules, clear hierarchies, established consequences, security breaches and lots of laws.

progress of any projects started during the course, and finally it's something of a reveal - showing how the majority of the content of the course is from a Cyber Security background and what students can do to find out more.

Taking on a single project

All Saints Primary school on a litter picking project, 2010, Used under licence from https://flickr.com/photos/35317151@N06/4763787826

While these lesson plans provide a comprehensive framework for teachers to follow, they are also designed to be flexible. If students have a specific social change they are passionate about, teachers can focus on that topic and adapt the lesson plans as needed. This allows students to take ownership of their learning and work collaboratively to create meaningful change.

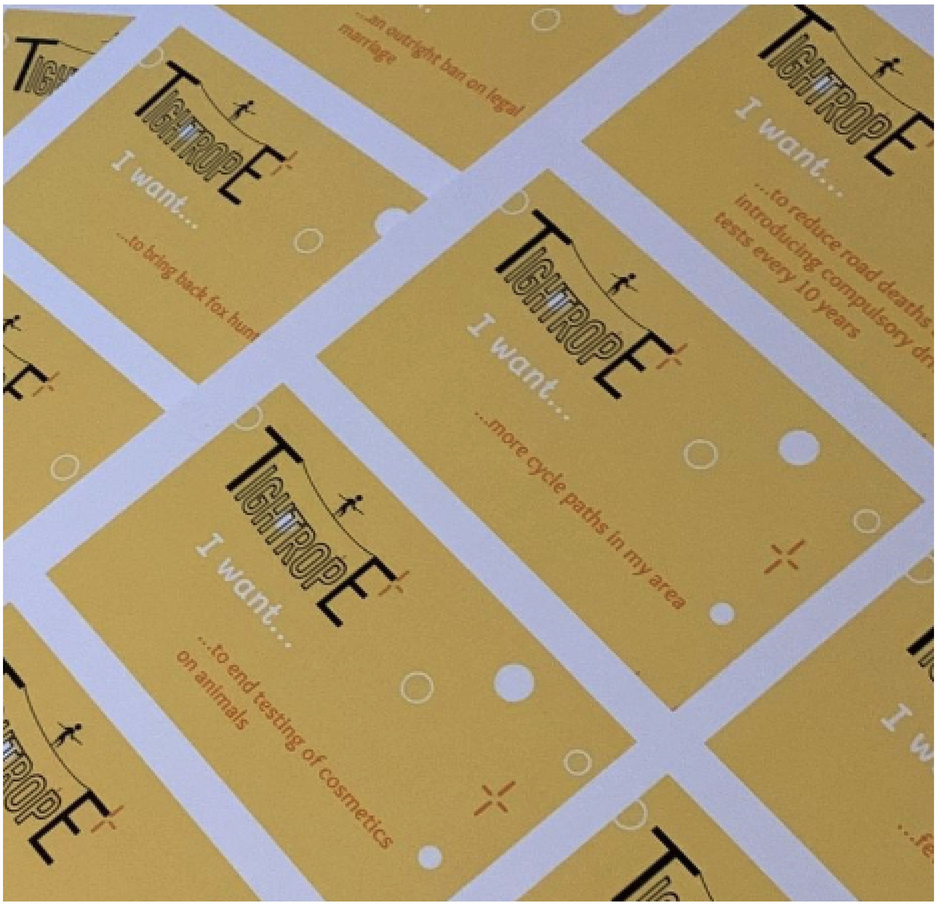
Examples of small scale social changes that students might be interested in:

1. Reducing food waste: Encouraging classmates and teachers to reduce the amount of food they waste in the school cafeteria, and promoting composting and recycling.
2. Promoting mental health awareness: Organising a school-wide campaign to promote mental health awareness, reduce stigma, and provide support for those struggling with mental health issues.

3. Tackling plastic pollution: Raising awareness of plastic pollution and encouraging classmates and teachers to reduce their use of plastic, by bringing reusable water bottles and lunch boxes to school, for example.
4. Improving accessibility: Identifying areas in the school that may be inaccessible to students with disabilities and working with the school to make necessary improvements.
5. Reducing energy consumption: Encouraging classmates and teachers to turn off lights and electronics when not in use, and promoting the use of energy-efficient appliances in the school.

By focusing on local and achievable goals, students can make a real impact on their school and community while also learning valuable skills for creating positive change.

Change cards


...an outright ban on legal marriage
TIGHTROPE
I want...
...to bring back fox hunt
...to reduce road deaths introducing compulsory dr tests every 10 years
...more cycle paths in my area
...to end testing of cosmetics on animals

Our change cards before cutting out, 2023, Released under Creative Commons by us.

One challenge that teachers may face is that some students may be too afraid or shy to express their ideas about social change. This can make it difficult to engage them in discussions and activities related to creating positive change. To address this issue, the Tightrope Project created 'change cards' that can help students overcome their fears and share their ideas in a safe and non-threatening way. These are available in our resource pack to print out and you should feel free to tailor them to the specific needs and interests of their students. This can be done by brainstorming with students or by using resources such as the United Nations' Sustainable Development Goals[3] to identify key areas of focus.

The change cards are a set of cards that contain a range of social issues, such as climate change, bullying, or poverty. These cards are randomly assigned to students during classroom activities, giving them a specific social issue to focus on during the exercise. By using the change cards, students can express their ideas and opinions about social issues without fear of judgement or criticism from their peers.

The change cards serve several purposes. Firstly, they can help students who are too shy or scared to talk about social issues to overcome their fears and express their ideas in a safe and supportive environment. Secondly, the cards can help students focus their ideas and develop a plan of action for addressing a specific social issue. Finally, the cards can help teachers identify which social issues are important to their students, and tailor their lessons and activities accordingly.

The use of change cards is a creative and innovative approach to helping students engage with social change in a safe and supportive way. By providing students with a specific social issue to focus on, teachers can help them develop the critical thinking and problem-solving skills they need to create positive change in their community.

Cyber Security Background

We used the UK's Cybersecurity Body of Knowledge (Cybok) framework as the basis for our lesson plans, ensuring that students are taught the skills and knowledge necessary to be responsible and secure digital citizens.

The use of the Cybok syllabus also ensures that the lessons are based on up-to-date, industry-standard cybersecurity practices. This can help students to gain a deeper understanding of cybersecurity issues and give them context for the real-world scenarios they will study in the lessons.

Content Warnings

The Tightrope Project's lesson plans cover a wide range of topics related to social change, including some that may be sensitive or triggering for some students. These topics may include domestic abuse, doxing, and gender-based violence. To ensure that all students feel safe and supported, the project includes content warnings for these topics, as well as guidance for teachers on how to manage discussions around these issues.

[3] United Nations' Sustainable Development Goals: https://www.un.org/sustainabledevelopment/sustainable-development-goals/

Content warnings are important because they allow students to prepare themselves emotionally and mentally for potentially sensitive material. They give students the opportunity to choose whether they want to engage with a particular topic or not, and allow them to seek out support if needed. Content warnings can also help to create a safe and inclusive learning environment where all students feel valued and supported.

It is important to note that while content warnings and guidance for teachers can be helpful, they are not a substitute for appropriate mental health support. Teachers and schools should also provide students with access to counselling or other support services if needed.

Real world examples

The Tightrope Project's lesson plans include exercises that give teachers and students the opportunity to make real Freedom of Information (FOI) requests or write directly to elected officials on behalf of the students. These exercises are designed to provide students with practical experience in engaging with government and to promote civic participation and democratic engagement.

The FOI exercises are particularly valuable because they teach students how to access information that is not currently readily available to the public. This can be an empowering experience for students, as they learn how to navigate complex bureaucratic systems and exercise their right to access information.

These exercises can help to foster a lifelong commitment to civic engagement and social change. By learning how to engage with the government and hold elected officials accountable, students can become active and engaged citizens who can make a positive impact on their communities and society as a whole. However, they also are not compulsory - and you should feel free to opt out. In particular - FOI requests can take up to six weeks to give a result, so they only really suit situations where you are delivering one session a week.

Sharing these resources

The Tightrope Project is committed to promoting a culture of open access and sharing of knowledge. To this end, all the materials developed by the project are licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. This licence allows anyone to use, share, and adapt the materials for non-commercial purposes, as long as they attribute the work to the Tightrope Project and share any derivative works under the same licence.

The use of an open access licence is essential to the mission of the Tightrope Project. By making our materials freely available, we hope to encourage more teachers to engage their students in discussions and activities related to social change. The open access model also helps to ensure that the materials are accessible to a wider audience, including educators in developing countries and under-resourced communities.

The use of the Creative Commons licence has several benefits. Firstly, it encourages collaboration and knowledge-sharing, as teachers are free to adapt and build upon the existing materials to suit their own needs and contexts. Secondly, it helps to promote transparency and accountability, as anyone can access and scrutinise the materials. Finally, it helps to foster a sense of community and shared ownership, as educators around the world can contribute to the development and improvement of the materials.

Session Guides

These session guides include example scripts - you are not obliged to follow them but it gives an overview of how other educators have delivered the course.

Session 1: Introduction

This is the introduction section - a discussion and exercise on the topic of security in the broad sense - including motivations and capabilities of attackers. The second half of the session is on recasting the social change into more immediate and personal goals like "Start a fencing club", "advocate against animal testing"[4]. The key message of the session is "You secure things by making things hard to use and sometimes that is bad".

Admin Section

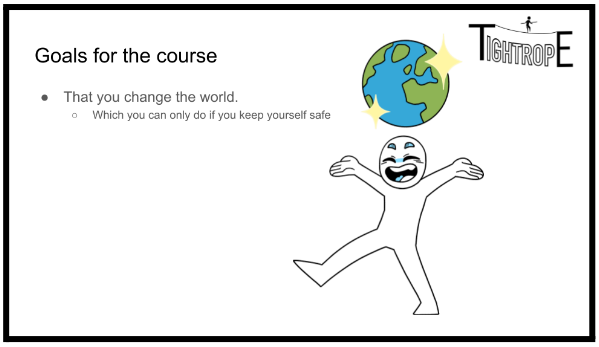
[4] Or indeed "advocate in favour of animal testing" - we are deliberately neutral on what students want to achieve as long as they are safe doing it. The set change cards discussed below contain a lot of pairs of cards that are direct opposites.

TIGHTROPE

Session 1

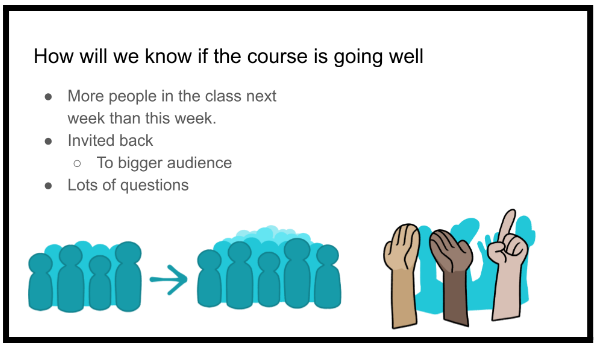
Introduction

equalitytime
ROYAL HOLLOWAY UNIVERSITY OF LONDON



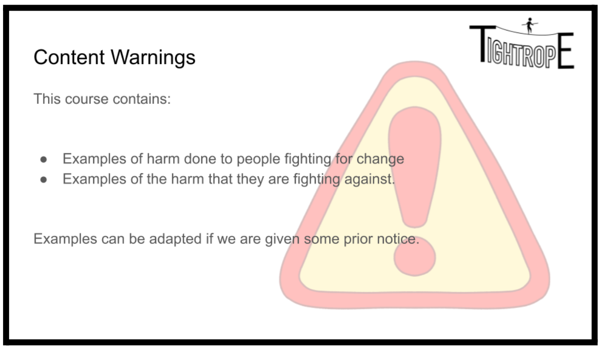
Goals for the course

- That you change the world.
  - Which you can only do if you keep yourself safe



How will we know if the course is going well

- More people in the class next week than this week.
- Invited back
  - To bigger audience
- Lots of questions

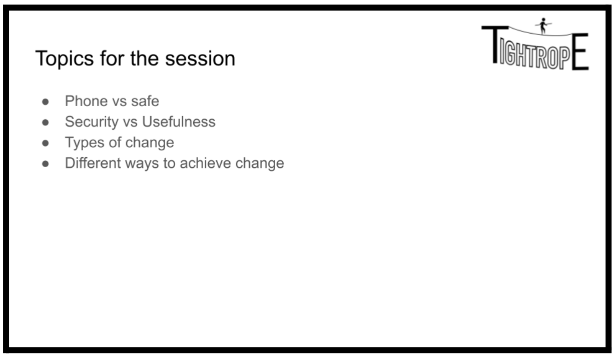


Content Warnings

This course contains:

- Examples of harm done to people fighting for change
- Examples of the harm that they are fighting against.

Examples can be adapted if we are given some prior notice.



Topics for the session

- Phone vs safe
- Security vs Usefulness
- Types of change
- Different ways to achieve change

This is the admin section of the course and the session. We cover the goals for the course, encourage people to ask questions, and give a general and specific content warning for the students before introducing the content. A general script for this section might be:

Hello, I'm X and welcome to our course on cyber security for changemakers. By the end of this course you'll have a better idea of how to talk about security and change than 90% of people who actually have security focused jobs.

There are six sessions. Some of them will focus more on security, some more on change. This is the introduction so it has a little bit of everything.

We have to start with some admin I'm afraid. Who we are, our goals for the course, a little bit of motivation. That sort of thing. We're then going to look at a very simple security question which will rapidly get more complicated. Then we're going to complain for a while. I hope that sounds good.

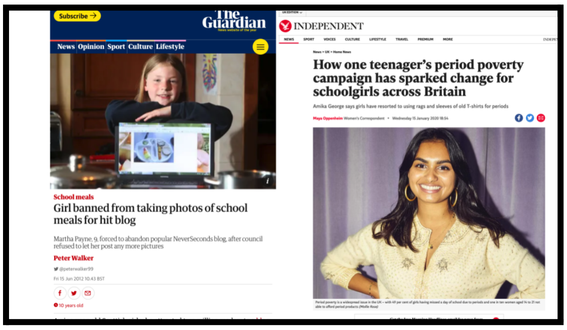
Our goal for the course is very simple. We want you to change the world. Safely. That means we need to show you how to both manage change and manage risk. And it's very hard to do both of those at the same time.   The balance is always hard, that's way we call *the project tightrope.*

The way I'll know if this course is going well is if there are more people here next week than this week. If I deliver these sessions well enough then you'll start bringing people with you. And it will be obvious to everybody how well it's going. The other good way to find out if it's going well is questions. I'm a firm believer that a lecture with less than 16 questions has failed, but for this course there's a lot of content that is potentially emotionally triggering so that might be a bit of an ambitious goal.

The last way I'll know this course is going well is if at the end of the session someone comes up to me and says "The thing I really want to change is this" That could be animal testing, it could be better support for cycling, it could be about awareness of a particular social issue. If you bring something like that to me, I can rewrite the course to support that.

The last bit of admin is the content warning. This course contains lots of examples of harm. Examples of harm done to activists and examples of harm done to them. Some of it keeps me up at night. If something you see in this course concerns you the right thing to do it go to a staff member here and say "Look, I've felt horrible since this happened" I can also alter some examples if I've got a bit of notice.

Inspiration and Fear



School meals

Girl banned from taking photos of school meals for hit blog

Martha Payne, 9, forced to abandon popular NeverSeconds blog, after council refused to let her post any more pictures

Peter Walker

@peterwalker99

Fri 15 Jun 2012 10.43 BST

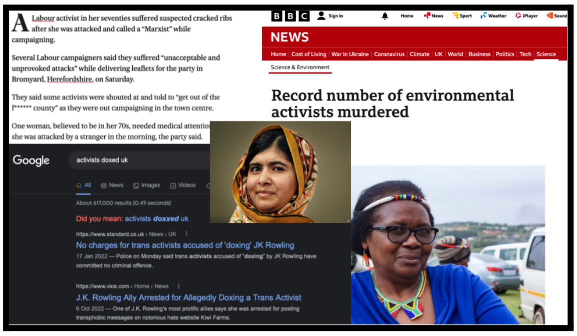
10 years old

How one teenager's period poverty campaign has sparked change for schoolgirls across Britain

Amika George says girls have resorted to using rags and sleeves of old T-shirts for periods

Maya Oppenheim Women's Correspondent • Wednesday 15 January 2020 18:54

Period poverty is a widespread issue in the UK – with 49 per cent of girls having missed a day of school due to periods and one in ten women aged 14 to 21 not able to afford period products *(Mollie Rose)*



A Labour activist in her seventies suffered suspected cracked ribs after she was attacked and called a "Marxist" while campaigning.

Several Labour campaigners said they suffered "unacceptable and unprovoked attacks" while delivering leaflets for the party in Bromyard, Herefordshire, on Saturday.

They said some activists were shouted at and told to "get out of the f****** county" as they were out campaigning in the town centre.

One woman, believed to be in her 70s, needed medical attentio she was attacked by a stranger in the morning, the party said.

Record number of environmental activists murdered

activists doxed uk

About 617,000 results (0.49 seconds)

Did you mean: activists *doxxed* uk

https://www.standard.co.uk › News › UK

No charges for trans activists accused of 'doxing' JK Rowling

17 Jan 2022 — Police on Monday said trans activists accused of "doxing" by JK Rowling have committed no criminal offence.

https://www.vice.com › Home › News

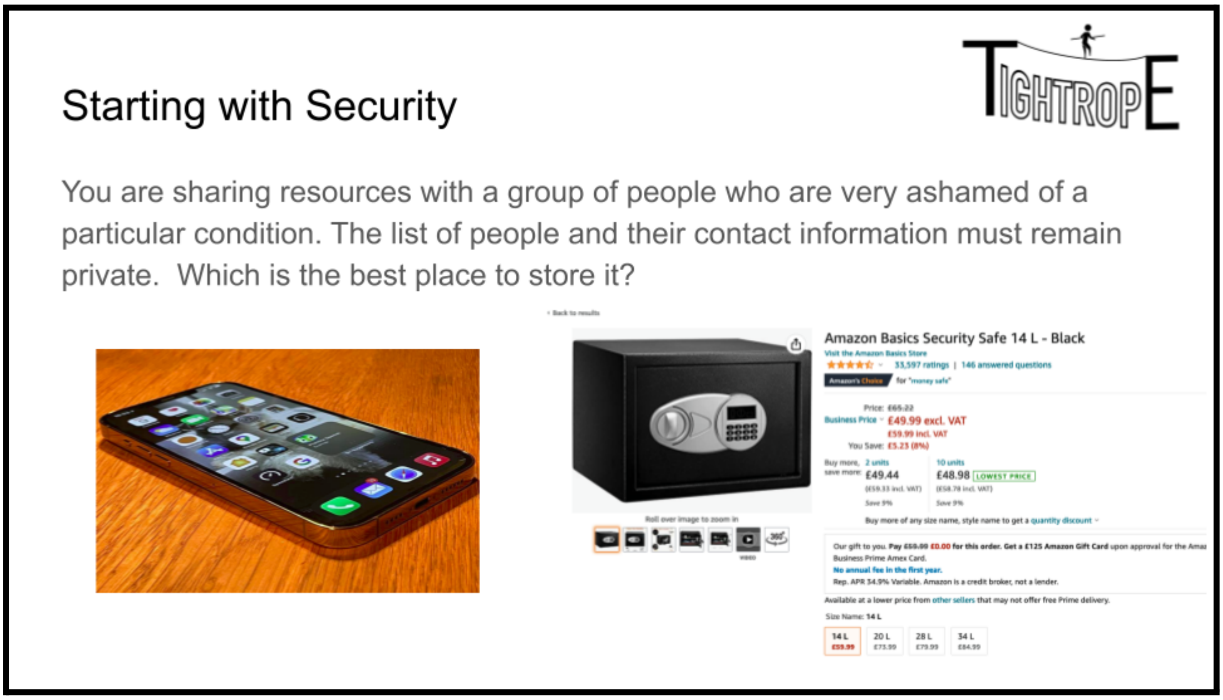
J.K. Rowling Ally Arrested for Allegedly Doxing a Trans Activist

6 Oct 2022 — One of J.K. Rowling's most prolific allies says she was arrested for posting transphobic messages on notorious hate website Kiwi Farms.

This section is examples of young people who have successfully created change and examples of changemakers who have faced harm. The first slide is an excellent one to localise for your school.

To drive home the 'risk of harm' point, we have scrolled through Wikipedia's list of attacks on people using India's freedom of information Law (https://en.wikipedia.org/wiki/Attacks_on_RTI_activists_in_India). It is worth mentioning at the time that later in this course we'll use the UK version of that law, and we'll examine the risks around it. It is also worth showing the students Amnesty International's review of the most dangerous types of activism (https://www.amnesty.org.uk/most-dangerous-activism)

Security Activity



Starting with Security

You are sharing resources with a group of people who are very ashamed of a particular condition. The list of people and their contact information must remain private. Which is the best place to store it?

< Back to results

Amazon Basics Security Safe 14 L - Black

Visit the Amazon Basics Store

33,597 ratings | 146 answered questions

Amazon's Choice for "money safe"

Price: ~~£65.22~~

Business Price £49.99 excl. VAT

£59.99 incl. VAT

You Save: £5.23 (8%)

Buy more, save more: 2 units £49.44 (£59.33 incl. VAT) Save 9% | 10 units £48.98 LOWEST PRICE (£58.78 incl. VAT) Save 9%

Buy more of any size name, style name to get a quantity discount

Our gift to you. Pay ~~£59.99~~ £0.00 for this order. Get a £125 Amazon Gift Card upon approval for the Amaz Business Prime Amex Card.

No annual fee in the first year.

Rep. APR 34.9% Variable. Amazon is a credit broker, not a lender.

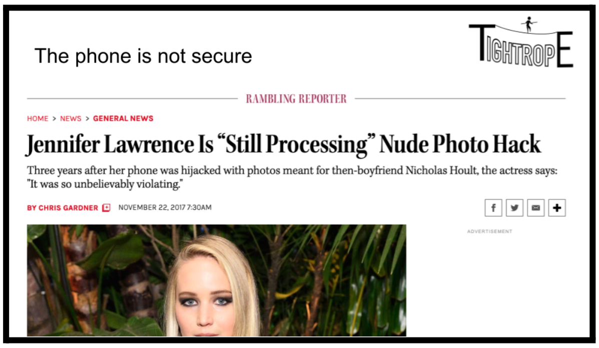
Available at a lower price from other sellers that may not offer free Prime delivery.

Size Name: 14 L

14 L	20 L	28 L	34 L
£59.99	£73.99	£79.99	£84.99

Give the students the prompt above and promote discussion - we have previously had the students vote on which one they thought was secure and then try and persuade the others. This can be pairs, whole class, or small groups.   Whenever you get a reasonable point, discuss it and put it on the board. The following slides cover the major points from a security point of view and should be used if the students don't get them on their own.

How many of these did we get?



The phone is not secure

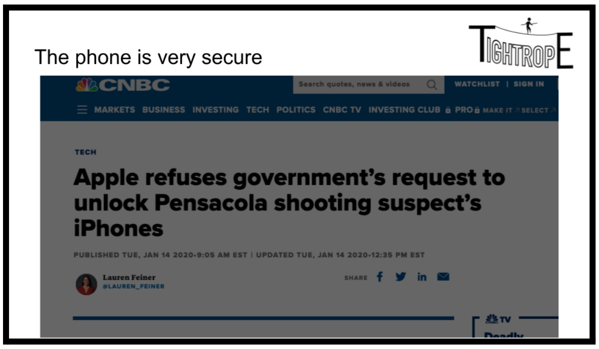
RAMBLING REPORTER

HOME > NEWS > GENERAL NEWS

Jennifer Lawrence Is "Still Processing" Nude Photo Hack

Three years after her phone was hijacked with photos meant for then-boyfriend Nicholas Hoult, the actress says: "It was so unbelievably violating."

BY CHRIS GARDNER   NOVEMBER 22, 2017 7:30AM



The phone is very secure

TECH

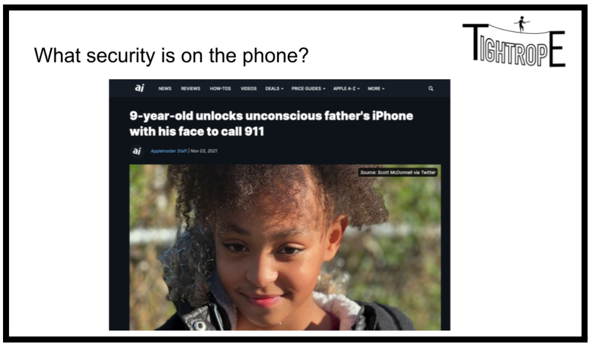
Apple refuses government's request to unlock Pensacola shooting suspect's iPhones

PUBLISHED TUE, JAN 14 2020·9:05 AM EST | UPDATED TUE, JAN 14 2020·12:35 PM EST

Lauren Feiner
@LAUREN_FEINER

CNBC
Search quotes, news & videos
WATCHLIST | SIGN IN
MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV INVESTING CLUB PRO MAKE IT SELECT
SHARE
TV
Deadly

For this set (discussing the circumstances where the phone is the secure and when it isn't) - it's worth familiarising yourself with https://en.wikipedia.org/wiki/2014_celebrity_nude_photo_leak and https://www.cnbc.com/2020/01/14/apple-refuses-barr-request-to-unlock-pensacola-shooters-iphones.html

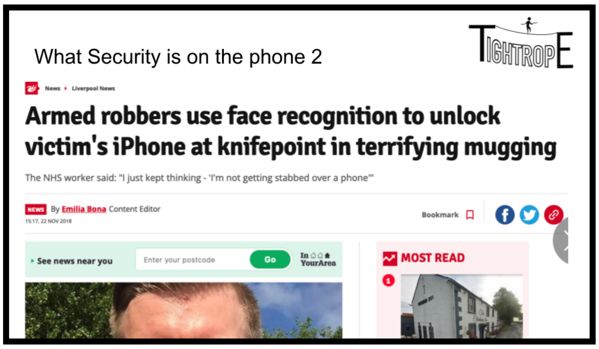


What security is on the phone?

9-year-old unlocks unconscious father's iPhone with his face to call 911

AppleInsider Staff | Nov 03, 2021

Source: Scott McDonnell via Twitter



What Security is on the phone 2

Armed robbers use face recognition to unlock victim's iPhone at knifepoint in terrifying mugging

The NHS worker said: "I just kept thinking - 'I'm not getting stabbed over a phone'"

By Emilia Bona Content Editor

15:17, 22 NOV 2018

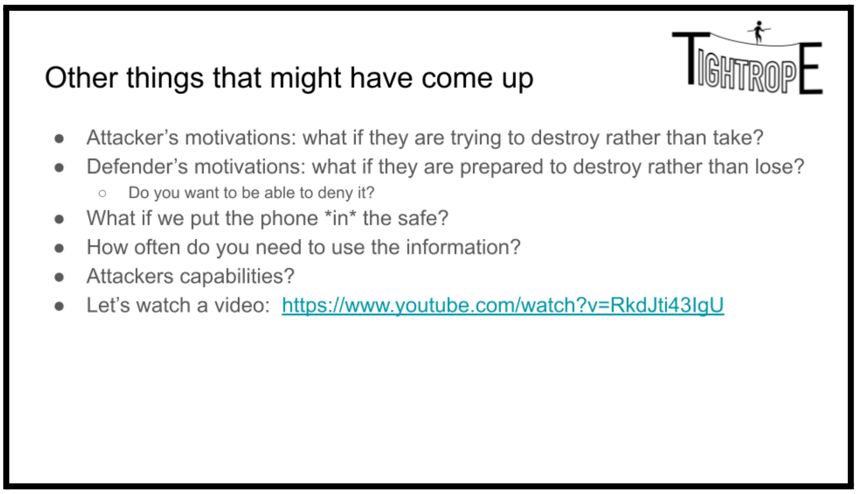
The above two are relatively self explanatory examples of the advantages and disadvantages of a particular type of security. However this is the point to drive home a key message of the course:

You make things secure by making them harder to use

Some of the key learning outcomes of this course for the students are recognising that statement and the effects on personal power, access to services, and the marginalisation of communities.

What if the attacker is in the house?

This slide will require some tact, particularly because we've only given the students a content warning a few minutes ago.   "A new report suggests that over half (61%) of women killed by men in the UK in 2018 were killed by a current or ex partner." https://www.bbc.co.uk/news/newsbeat-51572665 and issues like FGM and parental abuse, are serious.   We'll talk about digital intimacy later in the course but this is a good point to start a gentle discussion about abuse within the home. If you would like to avoid the conversation at this stage, then this slide is about how your phone is generally always with you, but a landlord or roommate might have access to it.



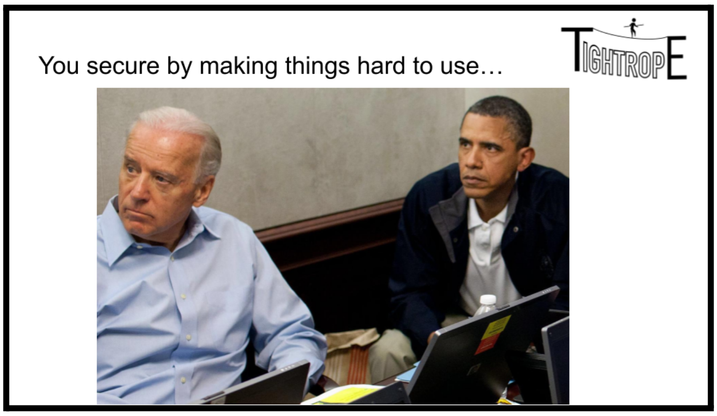
Other things that might have come up

- Attacker's motivations: what if they are trying to destroy rather than take?
- Defender's motivations: what if they are prepared to destroy rather than lose?
    - Do you want to be able to deny it?
- What if we put the phone *in* the safe?
- How often do you need to use the information?
- Attackers capabilities?
- Let's watch a video: https://www.youtube.com/watch?v=RkdJti43IgU

This is a short set of reminders for you about things that are worth discussing if you haven't already. The video is important - that model of safe wasn't chosen by accident. It's Amazon's recommended product at the time of writing and it's quite insecure. The video is a locksmith opening it extremely quickly. It's normally quite an effective way of getting some of Team Safe to change their minds.

The attacker's motivations part is something students normally miss. Ask people to put up their hands if they use a bike lock. Then ask them if that stops their tyres being slashed.

For your interest, there is some light stand-up comedy on the topic here: https://www.youtube.com/watch?v=SdoWHtNOd38



You secure by making things hard to use…

This is the slide that makes explicit what we mentioned earlier. A sample script might be:

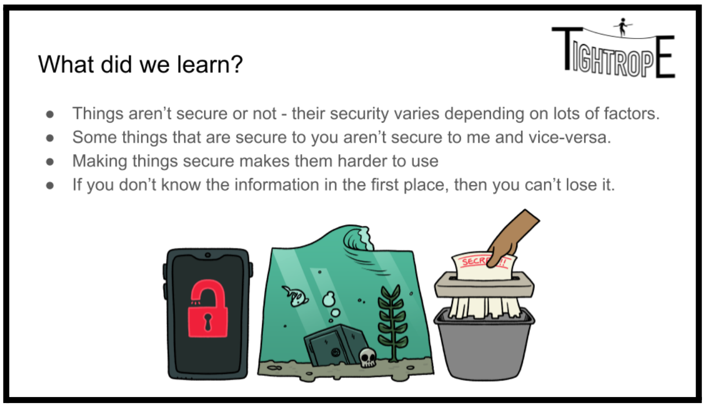
Maybe the best thing to do is to put the information on the phone, but the phone in the safe, weld the safe shut, put it in a pit and pour concrete over it, then install security cameras. That would be pretty secure right? Sure, but it's also hard to use. Like, if it's information you don't actually need, you should just destroy it.

This is a photo of two guys watching live updates on the killing of OBL - between them is a burn bag. A bag designed specifically so that you can quickly and effectively burn the *documents inside it.   Best way to keep something secret is to destroy it. The Film Argo, if anyone has seen it, spends quite a bit of time in the opening demonstrating how important this can be.*

Best way to keep a secret is not to know it or have access to it.   This is very true in business and in life. In fact it's one of the key parts of GDPR - you shouldn't collect data you aren't meant to have.

Literally nothing worth knowing starts with "I shouldn't tell you this". And if you remember nothing else from this talk remember this: the more secrets you have in your head, the harder your life is.

Now, I didn't give you the option to say "Actually I wouldn't do either" so it's a bit unfair, Sorry.



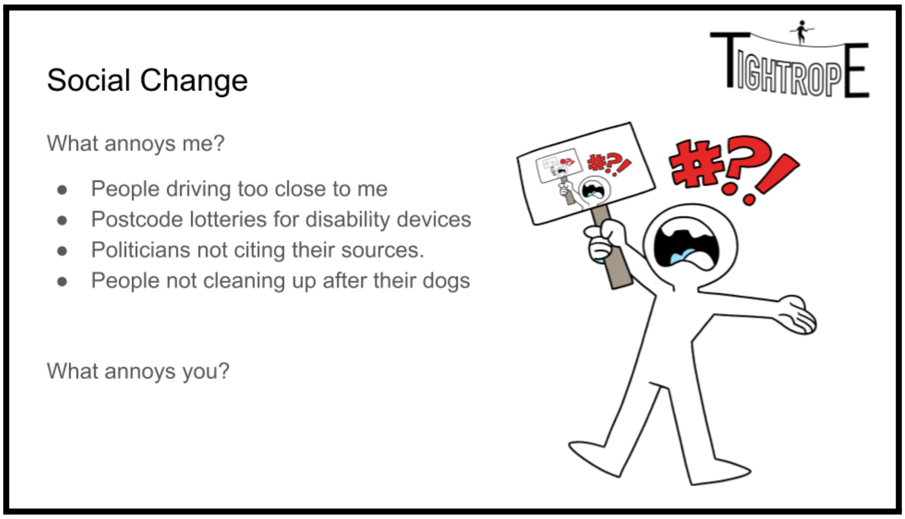
What did we learn?

- Things aren't secure or not - their security varies depending on lots of factors.
- Some things that are secure to you aren't secure to me and vice-versa.
- Making things secure makes them harder to use
- If you don't know the information in the first place, then you can't lose it.

This is a summary slide for the exercise.

Social Change Activity

The purpose of this activity is to get students to think about things they can change or influence locally. Some students may have arrived with a set of things they are already passionate about: that's great.



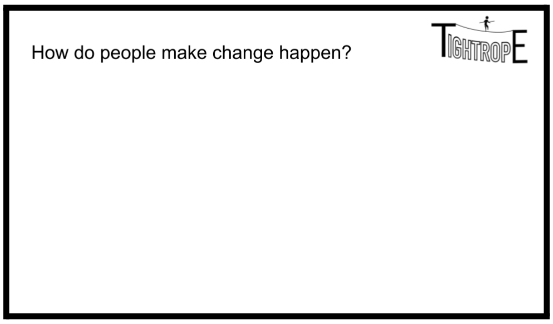
Social Change

What annoys me?

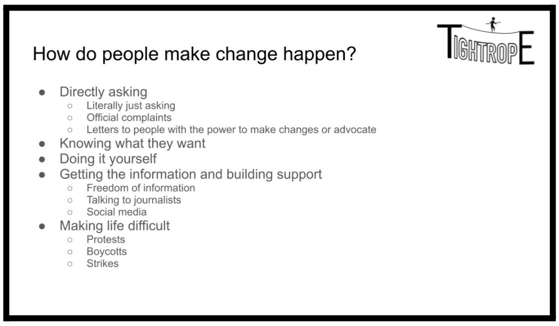
- People driving too close to me
- Postcode lotteries for disability devices
- Politicians not citing their sources.
- People not cleaning up after their dogs

What annoys you?

The first activity is to get the students to list things that annoy them. There will be some joke answers “My little brother”, “Transfer Windows”, but take them seriously and write them down - it will be useful for later. If the class isn’t warmed up, this might take a while. That’s okay.   In general you want some big things “Climate Change” and some small things “There should be a local woman’s running club” - it’s excellent if you get some that make good projects: “The school should have better lighting on the access path”



How do people make change happen?



How do people make change happen?

- Directly asking
  - Literally just asking
  - Official complaints
  - Letters to people with the power to make changes or advocate
- Knowing what they want
- Doing it yourself
- Getting the information and building support
  - Freedom of information
  - Talking to journalists
  - Social media
- Making life difficult
  - Protests
  - Boycotts
  - Strikes

This is another listing exercise.   The purpose is:

- To get the students to think about the different ways that change can happen.
- For one of the students to recommend violent protest, which is your cue to set the ground rule of “no illegal stuff”

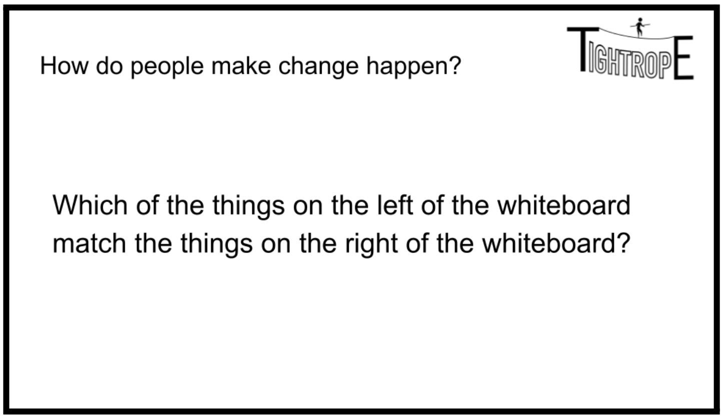
You can discuss this in more detail:

From: https://www.journalofdemocracy.org/articles/the-future-of-nonviolent-resistance-2/

“Among the 565 campaigns that have both begun and ended over the past 120 years, about 51 percent of the nonviolent campaigns have succeeded outright, while only about ***26 percent*** *of the violent ones have. Nonviolent resistance thus outperforms violence by a 2-to-1 margin.”*

But we can be clear that in the UK there is zero history of violence being successful.

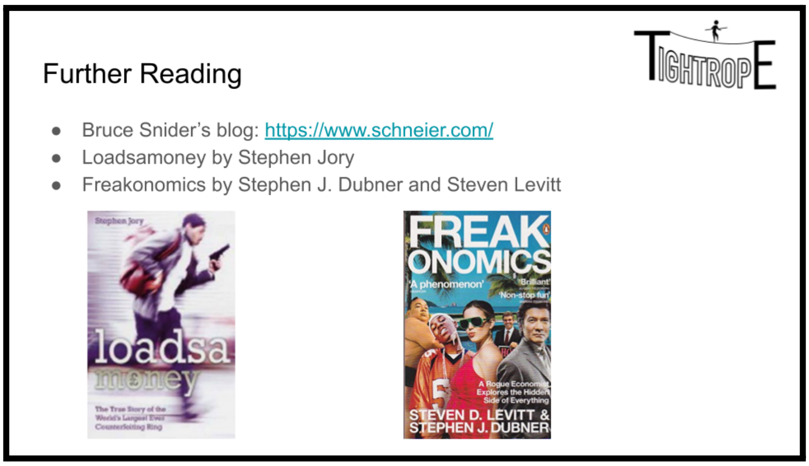
Once they have finished listing examples, move on to the second slide to talk about anything they might have missed.



How do people make change happen?

Which of the things on the left of the whiteboard match the things on the right of the whiteboard?

This is the last part of this set and you can use it to uncover causes they have missed (“What things would you use a boycott for?”) or methods they might have missed “So how are you going to get your parents to support your vegetarian diet?” If you have time, then it’s great to get into a conversation about *exactly* why it’s it would be ridiculous to use a petition (or any method) with one cause but not another. If they struggle to give examples of causes (they might be feeling vulnerable about things that are important to them) you can give out the cause cards as a prompt.

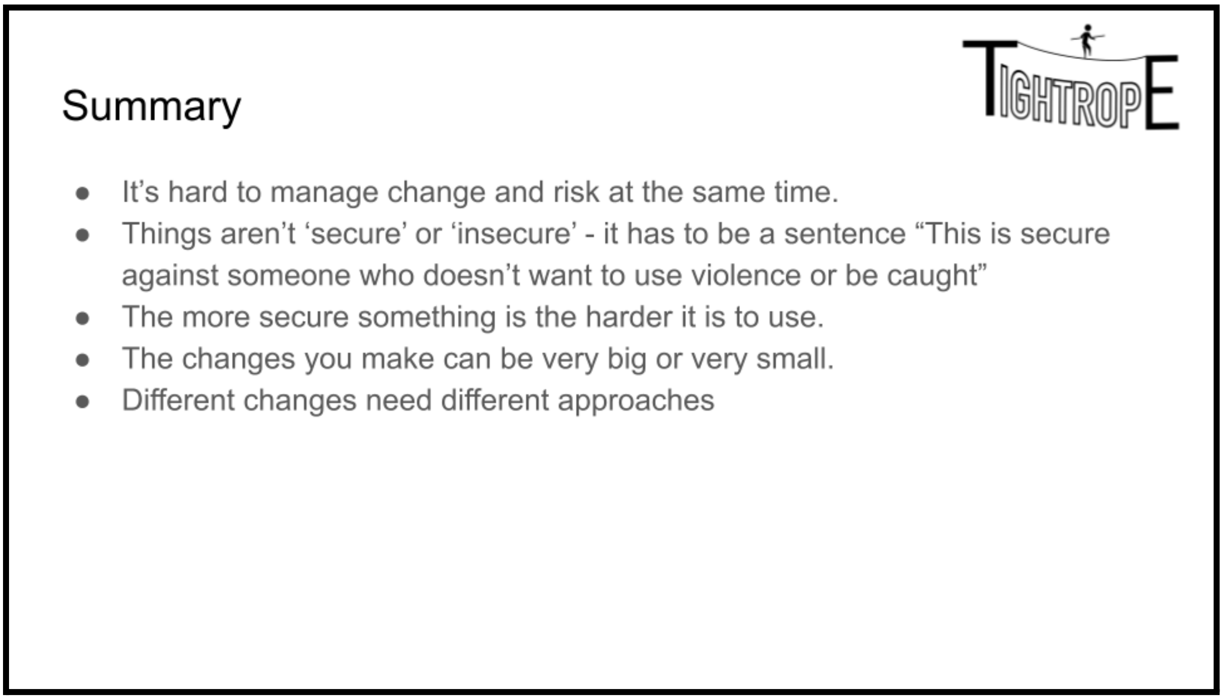


Further Reading

- Bruce Snider’s blog: https://www.schneier.com/
- Loadsamoney by Stephen Jory
- Freakonomics by Stephen J. Dubner and Steven Levitt

Stephen Jory
loadsa money
The True Story of the World's Largest Ever Counterfeiting Ring
FREAKONOMICS
'A phenomenon'
'Brilliant'
'Non-stop fun'
A Rogue Economist Explores the Hidden Side of Everything
STEVEN D. LEVITT & STEPHEN J. DUBNER

The blog is an excellent source of security news and commentary, and the books are the right level for bright high-schoolers. Loadsmoney is the autobiography of a ‘successful’ criminal and ends up covering a lot of security basics. Freakonomics also has a lot of focus on crime, but it’s value is mostly in terms of incentives.



Summary

- It’s hard to manage change and risk at the same time.
- Things aren’t ‘secure’ or ‘insecure’ - it has to be a sentence “This is secure against someone who doesn’t want to use violence or be caught”
- The more secure something is the harder it is to use.
- The changes you make can be very big or very small.
- Different changes need different approaches

Session 2: Four steps of change.

This session gives a four step framework for making changes and starts by asking the students to consider the difference between complaining and actually taking action to achieve change. The session focuses on ‘information’ and includes an introduction to Freedom of Information requests.

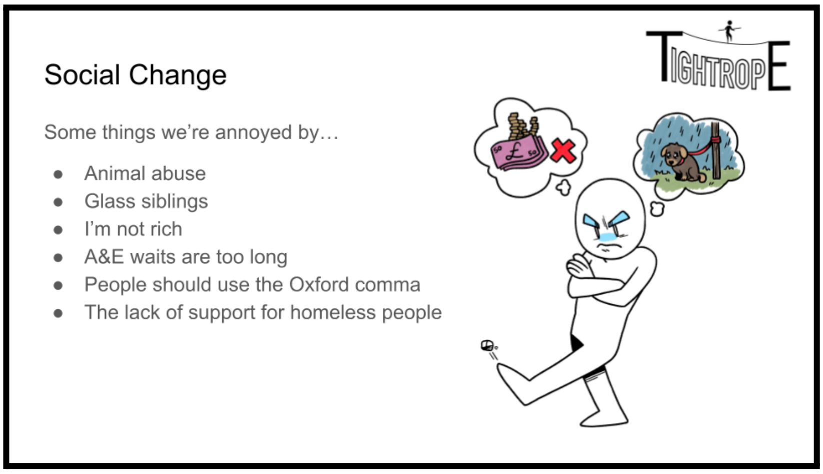
During this lesson you can make a Freedom of Information request with the class. This will require a little prep.

1. Register an account with https://www.theyworkforyou.com/
2. If you have something that is a personal interest, then you can find the relevant local authority and ask your question.
3. If the students have shown a clear passion for something local, then you can help them craft the request.
4. If you don’t want to share your own interests with the students, you can make a Freedom of Information Request directly to your own school.
    a. Talk to your admin staff first and agree something reasonable that might be worth requesting. This is an example of a request that isn’t much load on the admin team: https://www.whatdotheyknow.com/request/school_timetable_109#incoming-2159448 and this is one that is a little more interesting but still easy. https://www.whatdotheyknow.com/request/free_school_meals_data_31#incoming-1596107

The advantage of doing an FOI to your own admin staff is that you can be reasonably sure they will reply nicely and will do so before the end of the course. On the other hand, this also means that your students might get a false impression of how easy it is.

Definitely make sure that you are making the request as a teacher. Don't let the students sign it.

Introduction

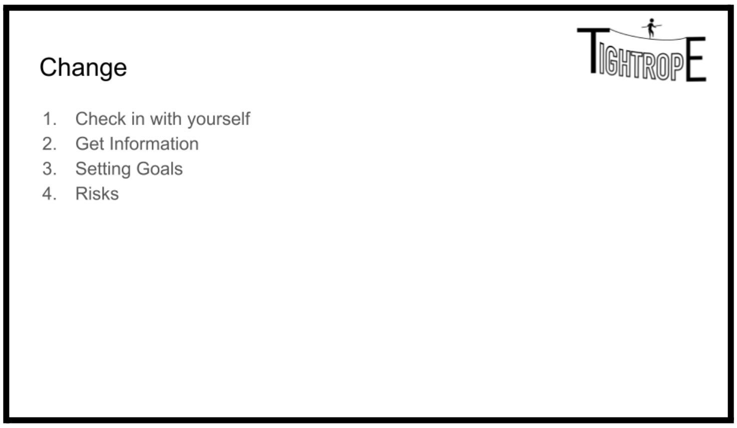


Social Change

Some things we're annoyed by…

- Animal abuse
- Glass siblings
- I'm not rich
- A&E waits are too long
- People should use the Oxford comma
- The lack of support for homeless people

Edit this slide (if you like) to remind the students of the things that they were passionate about in the last session.

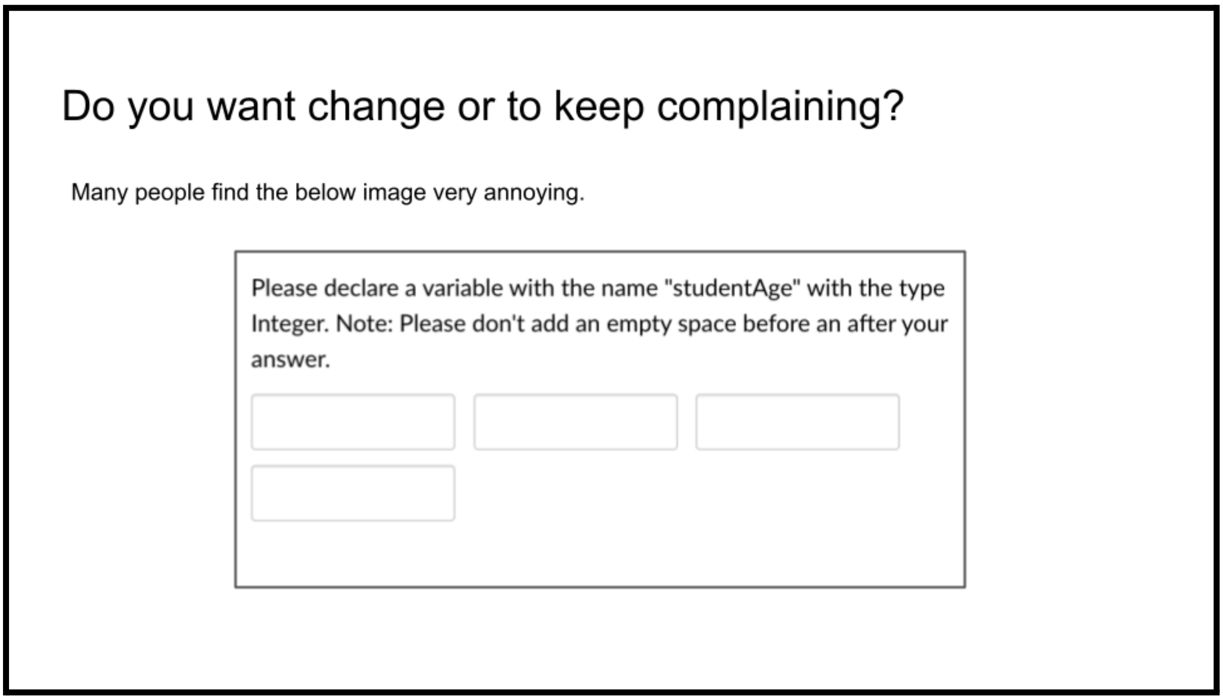


Change

1. Check in with yourself
2. Get Information
3. Setting Goals
4. Risks

We’re giving the students a four step plan to make change. You can be honest with the student that this isn’t based on any particular study - it’s just a way of separating out the things they need to know: in practice they’ll loop repeatedly through the list and often do several stages at once.

Complaining or Changing?



Do you want change or to keep complaining?

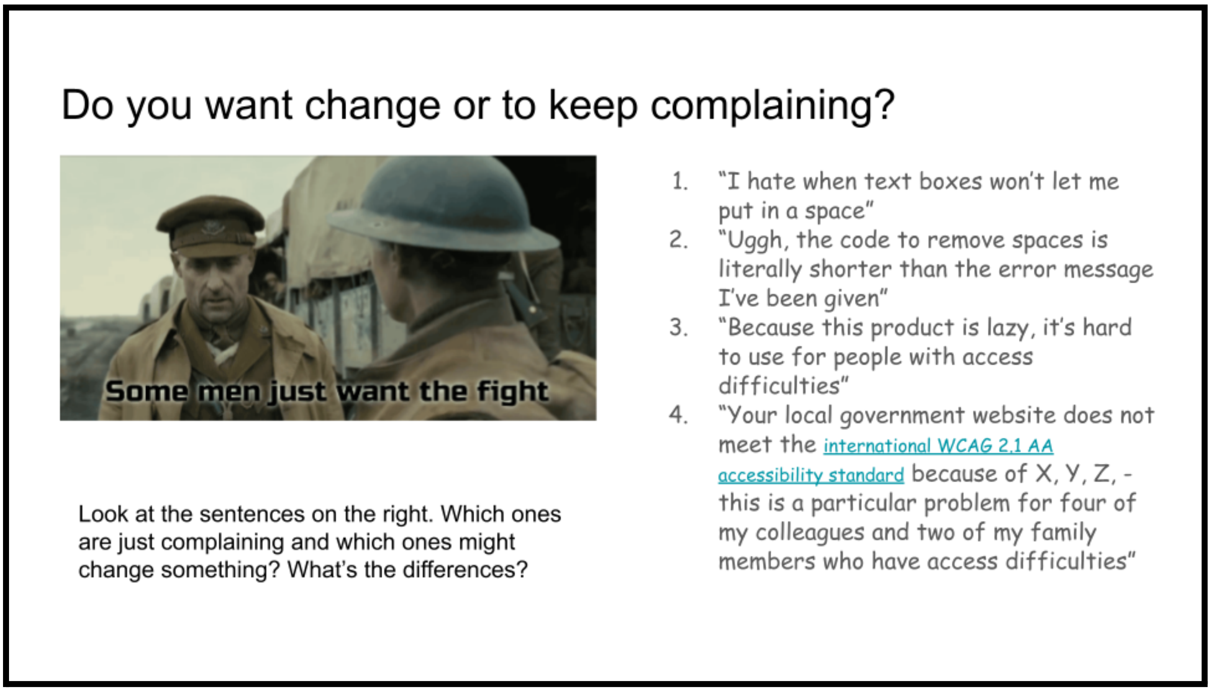
Many people find the below image very annoying.

Please declare a variable with the name "studentAge" with the type Integer. Note: Please don't add an empty space before an after your answer.

You can tell the students that the reason the image is upsetting is because the amount of typing the website design could have done to remove the annoying spaces (“.trim()”) is less typing than the message to the users.

We’re using this as an example of something that is annoying, but not particularly important.[5]

[5] It’s important to me. I’m just aware that there are other viewpoints.

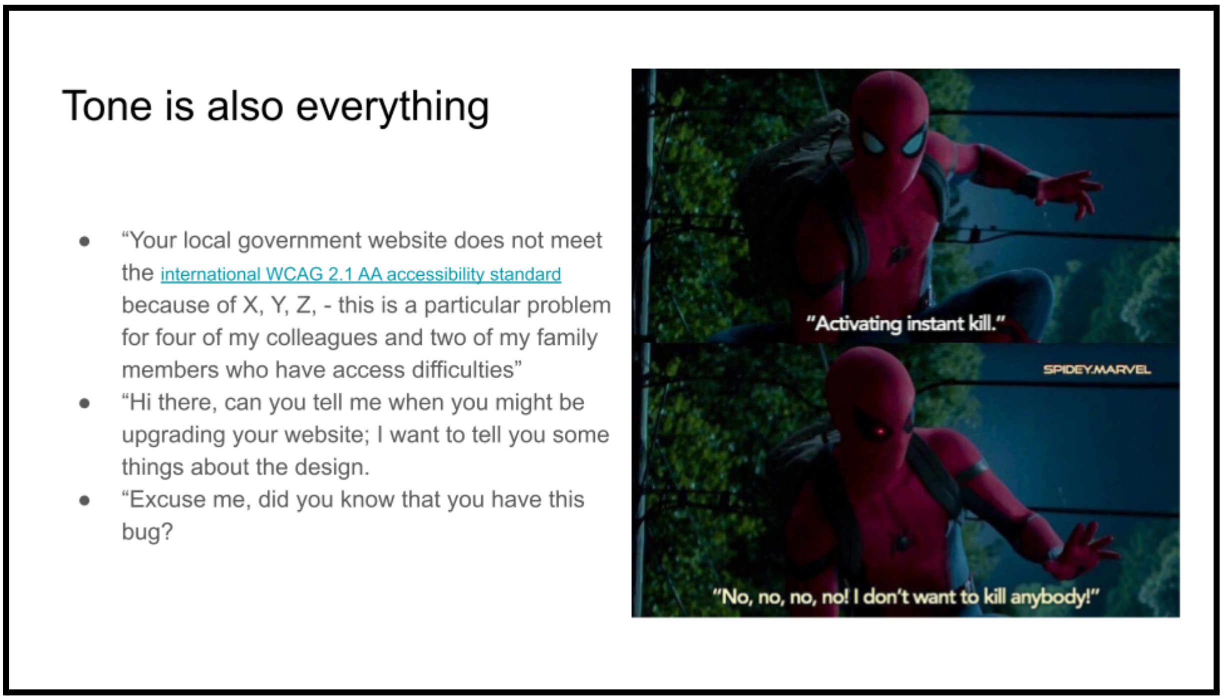


Do you want change or to keep complaining?

Look at the sentences on the right. Which ones are just complaining and which ones might change something? What's the differences?

1. "I hate when text boxes won't let me put in a space"
2. "Uggh, the code to remove spaces is literally shorter than the error message I've been given"
3. "Because this product is lazy, it's hard to use for people with access difficulties"
4. "Your local government website does not meet the international WCAG 2.1 AA accessibility standard because of X, Y, Z, - this is a particular problem for four of my colleagues and two of my family members who have access difficulties"

The slide is relatively clear - point out to the students that the examples get progressively more informative and make it easy for the recipient to change things. "Information is everything".



Tone is also everything

- "Your local government website does not meet the international WCAG 2.1 AA accessibility standard because of X, Y, Z, - this is a particular problem for four of my colleagues and two of my family members who have access difficulties"
- "Hi there, can you tell me when you might be upgrading your website; I want to tell you some things about the design.
- "Excuse me, did you know that you have this bug?

"Activating instant kill."
SPIDEY.MARVEL
"No, no, no, no! I don't want to kill anybody!"

This is the other side of “Are you complaining or are you changing”. The key message for the students is “Start politely and helpfully”.

This is an excellent point for a personal anecdote - if you can give the students examples of something you just enjoy complaining about and something you actually want to change then it’s easy to see the difference.

Getting information

There are two ways to run this next session. It works through a set of example ‘problems’ to find out how big or serious they are’. The first is to follow the example slides that contain problems students gave us in the testing. The second is to take the list of problems the students gave you in the last session and do no more than five minutes Googling on each to see what you can find. The point you are making is that you can make a surprising amount of progress in five minutes.

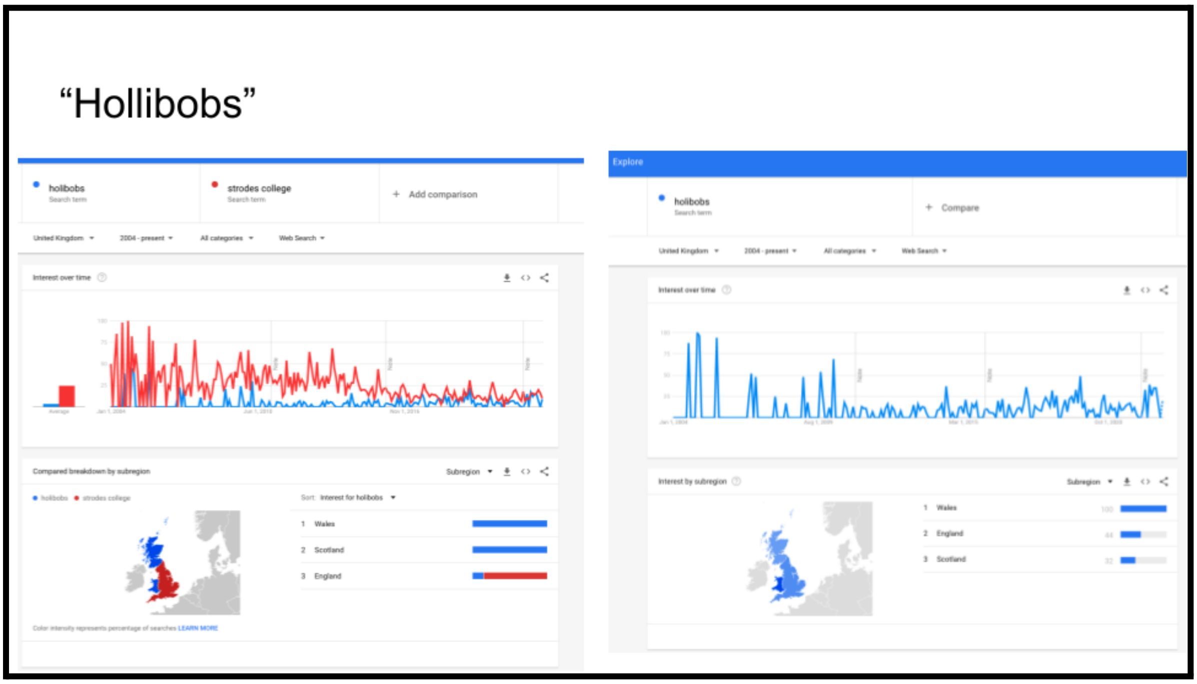
TIGHTROPE

Getting information

Information

Information is everything. Always will be.

- Is the thing you are complaining about, an actual issue?
- Does it affect other people?
- Is anyone else mad about it?



“Hollibobs”

● holibobs
Search term

● strodes college
Search term

+ Add comparison

United Kingdom ▾ 2004 - present ▾ All categories ▾ Web Search ▾

Interest over time

Compared breakdown by subregion

Subregion ▾

● holibobs ● strodes college

Sort: Interest for holibobs ▾

1 Wales

2 Scotland

3 England

Color intensity represents percentage of searches LEARN MORE

Explore

● holibobs
Search term

+ Compare

United Kingdom ▾ 2004 - present ▾ All categories ▾ Web Search ▾

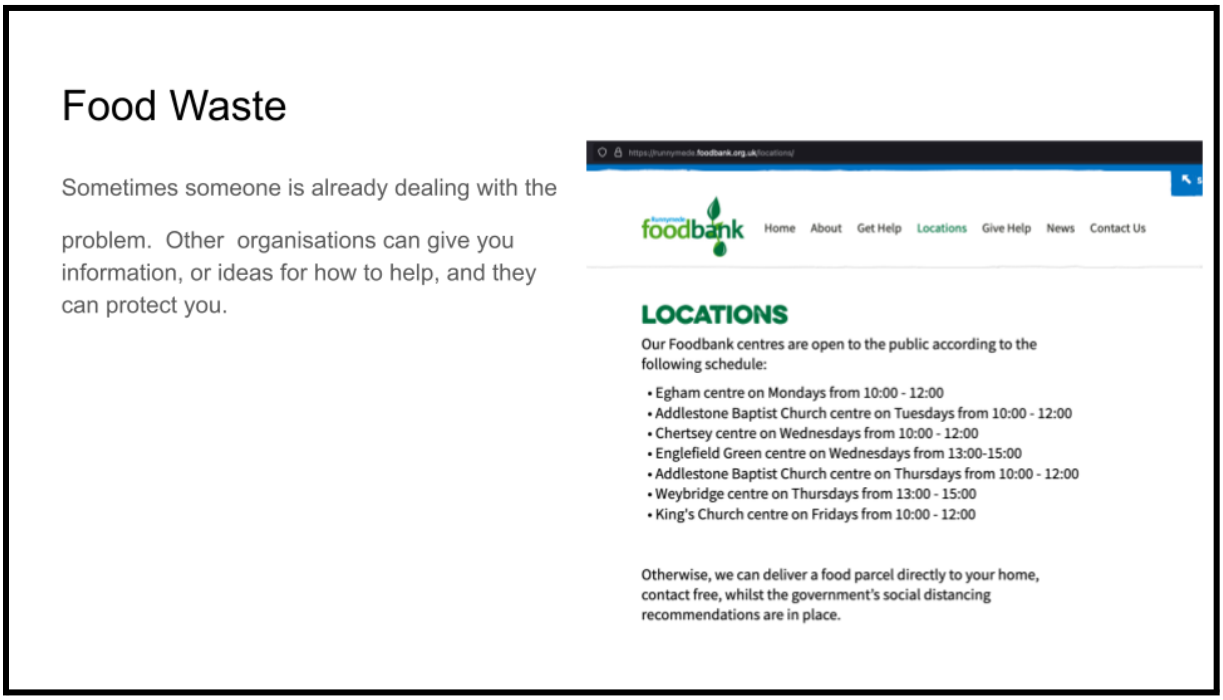
Interest over time

Interest by subregion

Subregion ▾

1	Wales	100
2	England	44
3	Scotland	32

In a previous session, a student complained about the use of the word ‘Hollibobs’ to mean holidays. Here we’ve used Google Trends to point out it’s not that common a thing and they can probably relax about it.[6]



Food Waste

Sometimes someone is already dealing with the problem. Other organisations can give you information, or ideas for how to help, and they can protect you.

LOCATIONS

Our Foodbank centres are open to the public according to the following schedule:

- Egham centre on Mondays from 10:00 - 12:00
- Addlestone Baptist Church centre on Tuesdays from 10:00 - 12:00
- Chertsey centre on Wednesdays from 10:00 - 12:00
- Englefield Green centre on Wednesdays from 13:00-15:00
- Addlestone Baptist Church centre on Thursdays from 10:00 - 12:00
- Weybridge centre on Thursdays from 13:00 - 15:00
- King's Church centre on Fridays from 10:00 - 12:00

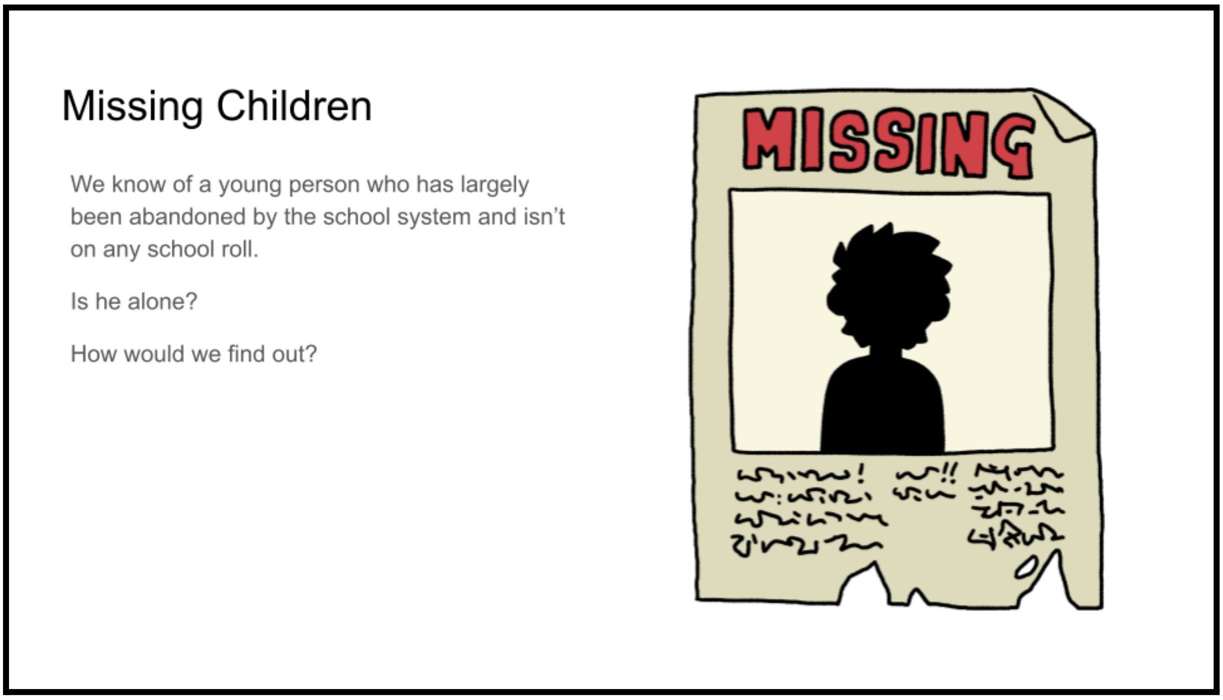
Otherwise, we can deliver a food parcel directly to your home, contact free, whilst the government's social distancing recommendations are in place.

A student passionate about food waste was surprised to find that there was a food bank to volunteer at just down the street. It lead to a discussion about a project were the college itself formed links with the food bank.

Freedom of Information

This is a fun session with a bit of a twist. We’re going to introduce a problem, then we are going to move away from it to talk about Freedom of Information, and then we are going to come back to see that Freedom of Information might help.

[6] Obviously, it’s also not that big of a problem if it was common. Some things are never going to be big problems.



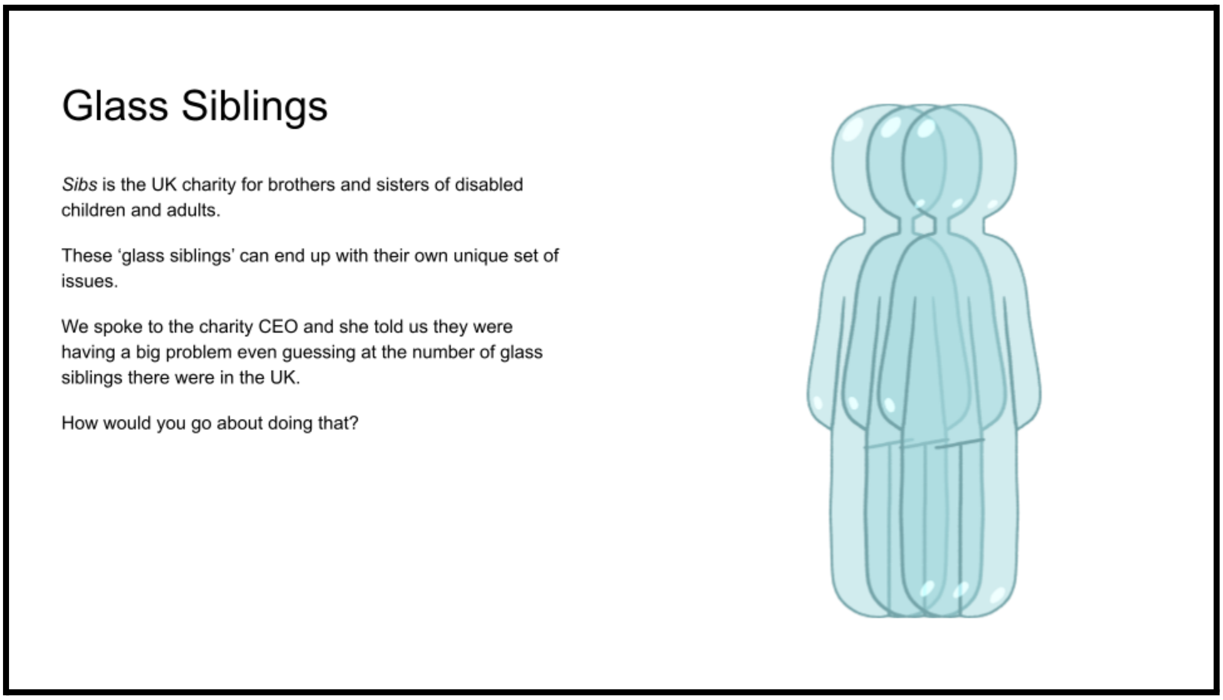
Missing Children

We know of a young person who has largely been abandoned by the school system and isn't on any school roll.

Is he alone?

How would we find out?

Present this slide to the students and ask how they would find out information about this. Maybe it's a big problem, maybe it isn't. How do we find out? Take as much time as you like.



Glass Siblings

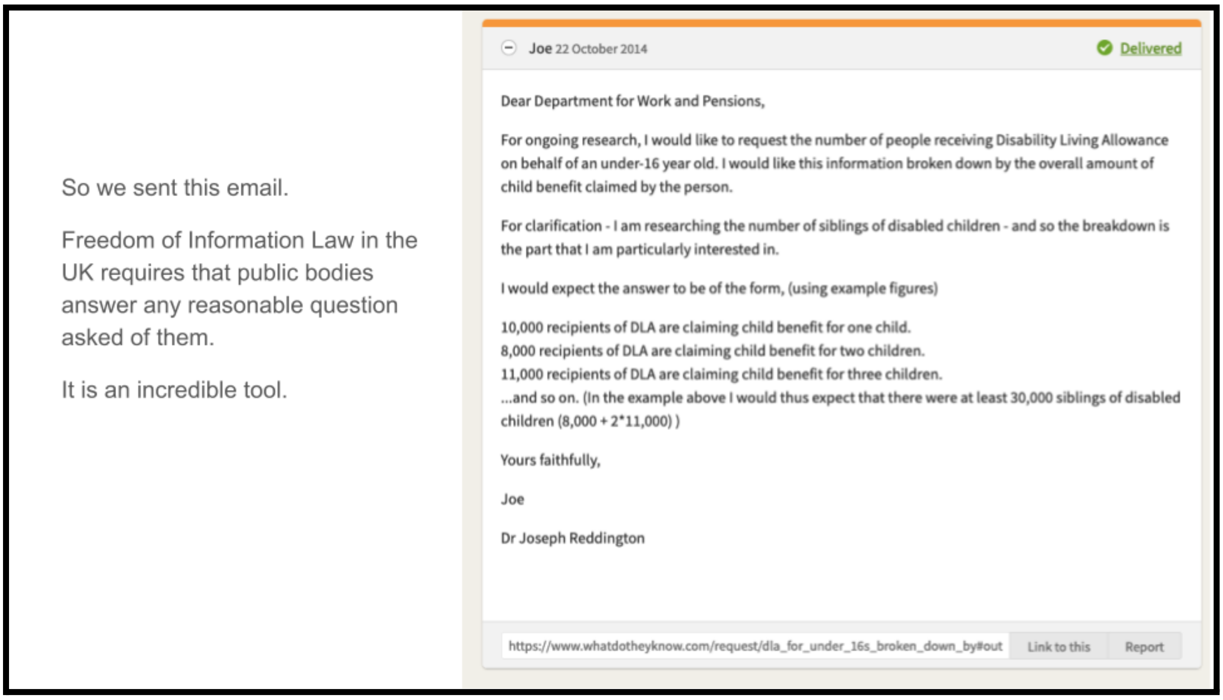
Sibs is the UK charity for brothers and sisters of disabled children and adults.

These 'glass siblings' can end up with their own unique set of issues.

We spoke to the charity CEO and she told us they were having a big problem even guessing at the number of glass siblings there were in the UK.

How would you go about doing that?

Now we move onto a different problem. The issue of Glass Siblings. Again ask the students for ideas. Surveys are the obvious answer - point out to the students how inaccurate and expensive they can be (particular nationally) but concede that might be the best approach (it was the one the CEO was planning on).



So we sent this email.

Freedom of Information Law in the UK requires that public bodies answer any reasonable question asked of them.

It is an incredible tool.

Dear Department for Work and Pensions,

For ongoing research, I would like to request the number of people receiving Disability Living Allowance on behalf of an under-16 year old. I would like this information broken down by the overall amount of child benefit claimed by the person.

For clarification - I am researching the number of siblings of disabled children - and so the breakdown is the part that I am particularly interested in.

I would expect the answer to be of the form, (using example figures)

10,000 recipients of DLA are claiming child benefit for one child.
8,000 recipients of DLA are claiming child benefit for two children.
11,000 recipients of DLA are claiming child benefit for three children.
...and so on. (In the example above I would thus expect that there were at least 30,000 siblings of disabled children (8,000 + 2*11,000))

Yours faithfully,

Joe

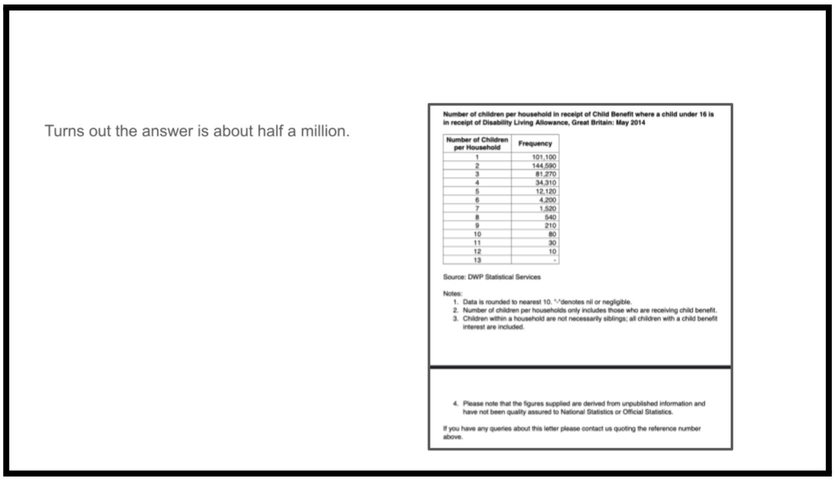
Dr Joseph Reddington

https://www.whatdotheyknow.com/request/dla_for_under_16s_broken_down_by#out
Link to this
Report

You should read through the first few pages of https://www.whatdotheyknow.com/help/about - the questions will come up.

Talk them through the maths of this. This is a fairly complex FOI request and it only worked because it was clear that

- It was for a good cause - the majority of FOI requests are from journalists who want to write about something embarrassing, or sales staff trying to generate leads. It was something that a data scientist in DWP would find interesting.
- It was clearly written and patiently followed up. Lots of FOIs are straight up abusive.



Turns out the answer is about half a million.

Number of children per household in receipt of Child Benefit where a child under 16 is in receipt of Disability Living Allowance, Great Britain: May 2014

Number of Children per Household	Frequency
1	101,100
2	144,590
3	81,270
4	34,310
5	12,120
6	4,200
7	1,520
8	540
9	210
10	80
11	30
12	10
13	-

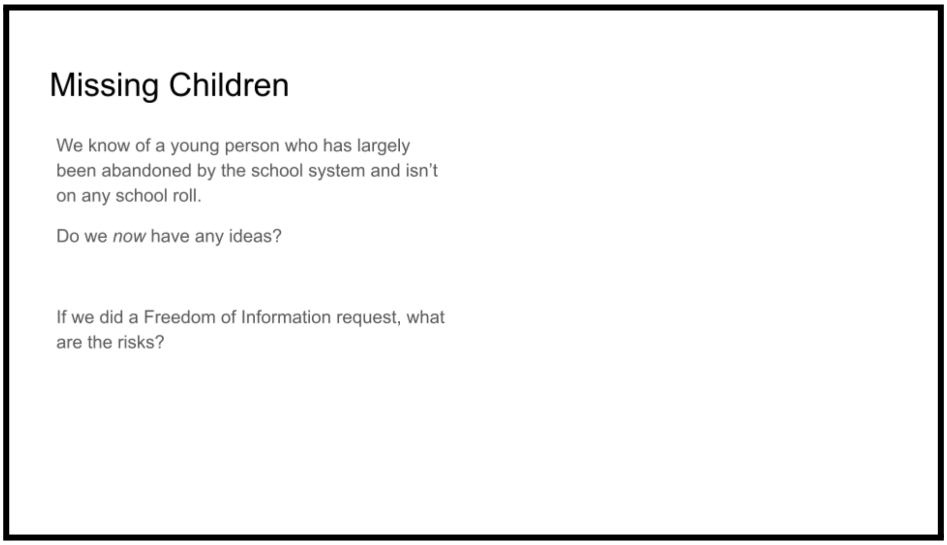
Source: DWP Statistical Services

Notes:
1. Data is rounded to nearest 10. "-"denotes nil or negligible.
2. Number of children per households only includes those who are receiving child benefit.
3. Children within a household are not necessarily siblings; all children with a child benefit interest are included.

4. Please note that the figures supplied are derived from unpublished information and have not been quality assured to National Statistics or Official Statistics.

If you have any queries about this letter please contact us quoting the reference number above.

Happily the request was successful, the charity went on to use it a lot and it was much cheaper and more accurate than a survey.



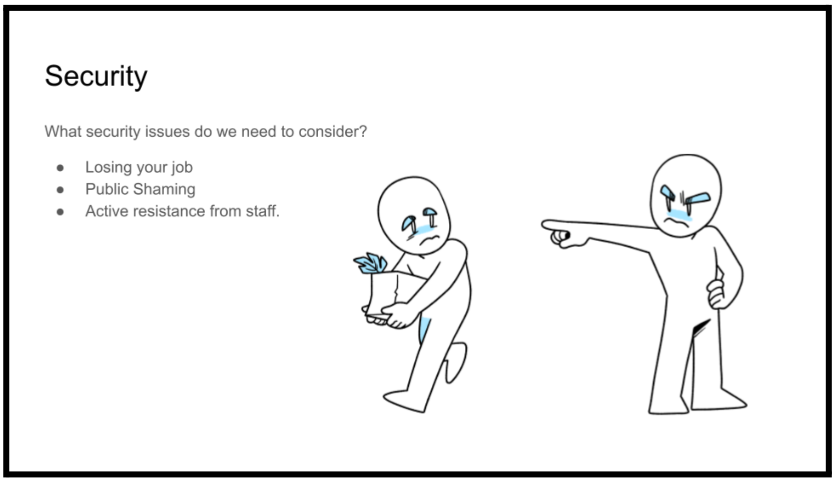
Missing Children

We know of a young person who has largely been abandoned by the school system and isn't on any school roll.

Do we *now* have any ideas?

If we did a Freedom of Information request, what are the risks?

Back to this problem - the students should now be reasonably likely to suggest an FOI request. But they should work out who (the local educational authority needs to record the removal from rolls so that's who), and how to write it out.   The whole theme here is that the more information you get the easier it is to get even more information.



Security

What security issues do we need to consider?

- Losing your job
- Public Shaming
- Active resistance from staff.

Ask the students what can go wrong for them personally if they make a freedom of information request. You want them to come up with specific problems that might happen. Once they are done, tell them that the person who did the Glass Sibling FOI request, and who also went on to use FOI to identify a postcode lottery in a particular type of NHS provision, ended up leaving his job at a university over it and changing careers completely.[7] It's possible (and, indeed, likely), that you'll annoy people by asking questions that they don't want public.

[7] It was me, It was also probably for the best.

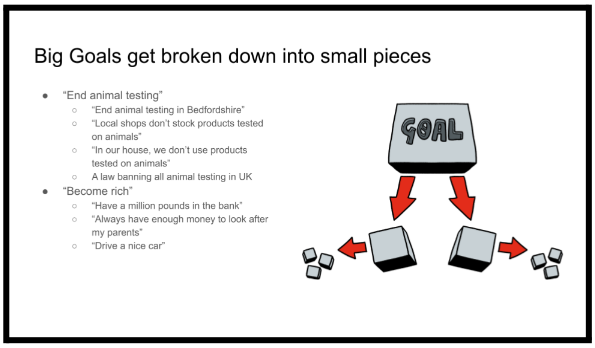
Now there are three paths from here:

- You can show the students a FOI request made (as part of this course) about the missing children here: https://www.whatdotheyknow.com/request/children_removed_from_school_rol#incoming-2213595. Point out the background section and how polite but specific the request is. Look at the replies that came in and the eventual pdf file - you can see that it's a surprisingly large number and *nobody seems to know why*.
- You make your own missing children FOI request, using ours as a template, to your local authority. Please email us before you do this, because it's quite possible someone already made the request in your area and it's not nice to keep making the same requests over and over again.
- You make a request of your own, live, in front of the students.

Setting Goals

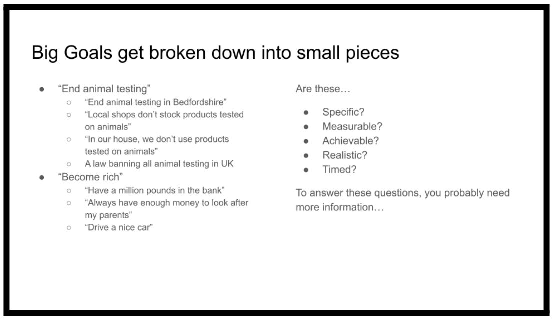
This is a fairly simple section - get the students to set some goals for changes they want (this is a good point to use the Change Cards). They'll discover they need more information and they'll go around the 'set goals, get information, change goals' loop a couple of times.

Step 3: Setting Goals



Big Goals get broken down into small pieces

- "End animal testing"
  - "End animal testing in Bedfordshire"
  - "Local shops don't stock products tested on animals"
  - "In our house, we don't use products tested on animals"
  - A law banning all animal testing in UK
- "Become rich"
  - "Have a million pounds in the bank"
  - "Always have enough money to look after my parents"
  - "Drive a nice car"



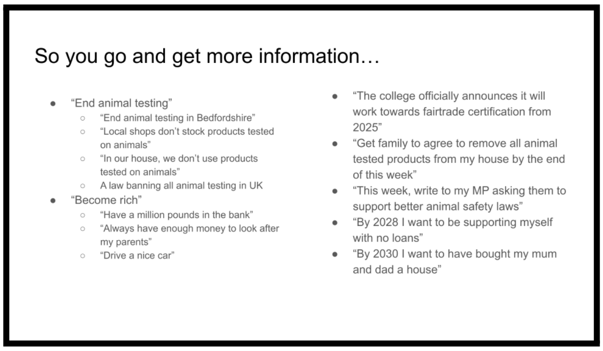
Big Goals get broken down into small pieces

- "End animal testing"
  - "End animal testing in Bedfordshire"
  - "Local shops don't stock products tested on animals"
  - "In our house, we don't use products tested on animals"
  - A law banning all animal testing in UK
- "Become rich"
  - "Have a million pounds in the bank"
  - "Always have enough money to look after my parents"
  - "Drive a nice car"

Are these…

- Specific?
- Measurable?
- Achievable?
- Realistic?
- Timed?

To answer these questions, you probably need more information…



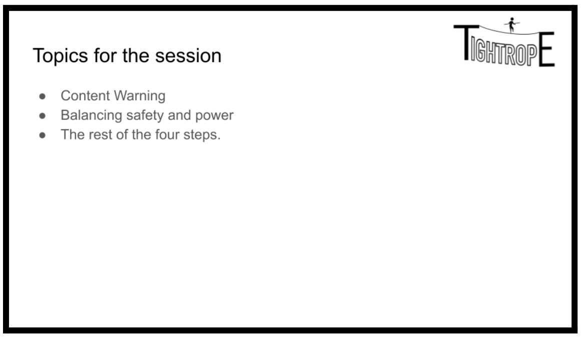
So you go and get more information…

- "End animal testing"
  - "End animal testing in Bedfordshire"
  - "Local shops don't stock products tested on animals"
  - "In our house, we don't use products tested on animals"
  - A law banning all animal testing in UK
- "Become rich"
  - "Have a million pounds in the bank"
  - "Always have enough money to look after my parents"
  - "Drive a nice car"

- "The college officially announces it will work towards fairtrade certification from 2025"
- "Get family to agree to remove all animal tested products from my house by the end of this week"
- "This week, write to my MP asking them to support better animal safety laws"
- "By 2028 I want to be supporting myself with no loans"
- "By 2030 I want to have bought my mum and dad a house"

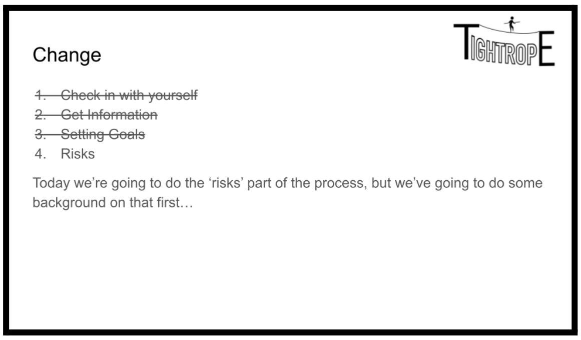
Sessions 3: Privacy and Threat Modelling.

This session examines a group of different activists and invites the students to understand why some conceal their identity and some don't. It examines a case study of a very traumatic harassment campaign against an activist for trans-rights and discusses the production of risk assessments.



Topics for the session

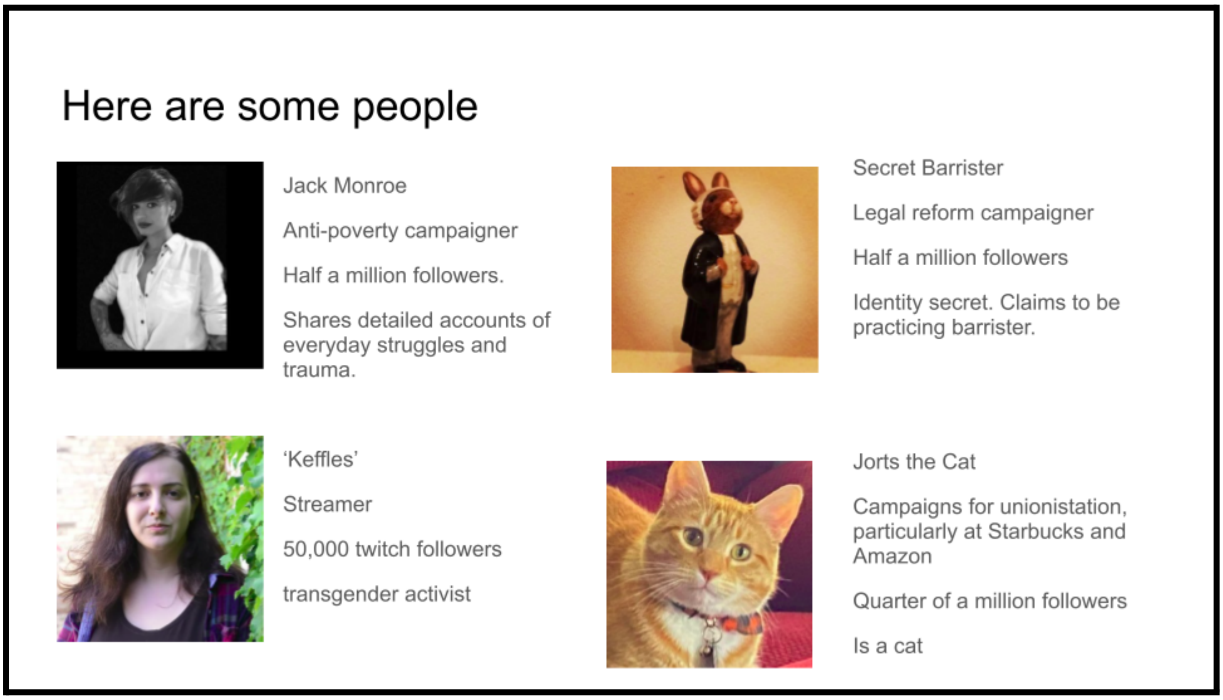
- Content Warning
- Balancing safety and power
- The rest of the four steps.



Change

1. ~~Check in with yourself~~
2. ~~Get Information~~
3. ~~Setting Goals~~
4. Risks

Today we're going to do the 'risks' part of the process, but we've going to do some background on that first…



Here are some people

Jack Monroe

Anti-poverty campaigner

Half a million followers.

Shares detailed accounts of everyday struggles and trauma.

Secret Barrister

Legal reform campaigner

Half a million followers

Identity secret. Claims to be practicing barrister.

'Keffles'

Streamer

50,000 twitch followers

transgender activist

Jorts the Cat

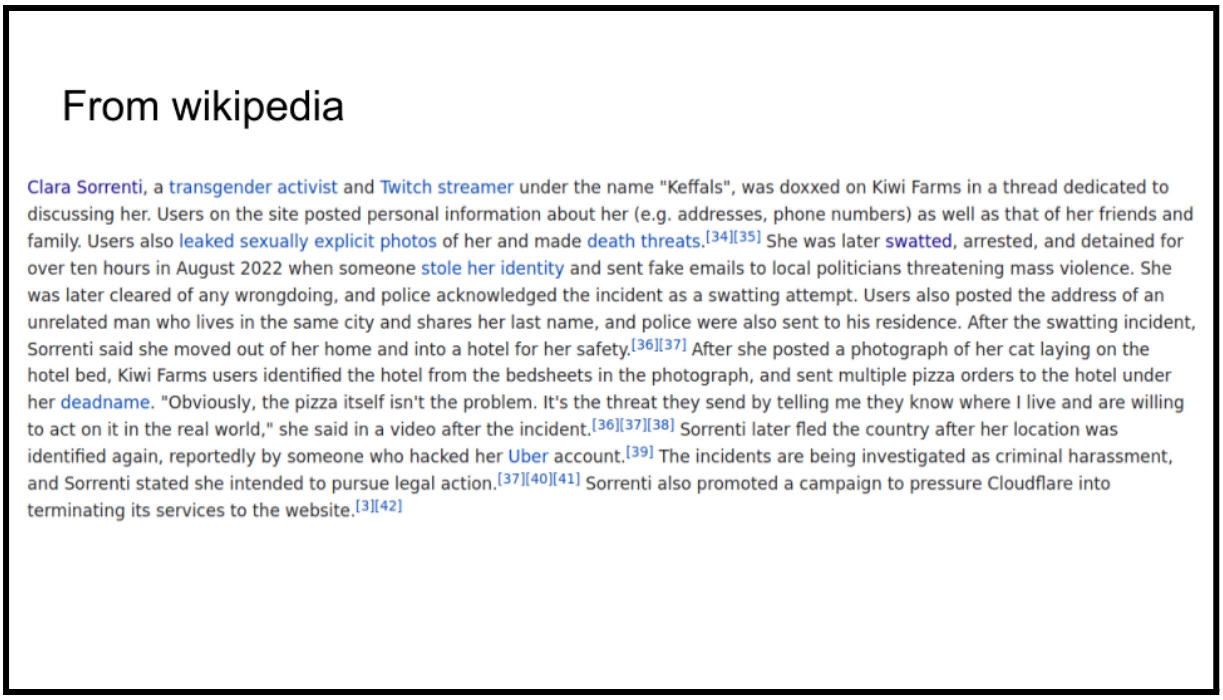
Campaigns for unionistation, particularly at Starbucks and Amazon

Quarter of a million followers

Is a cat

Have a look at these people's social media before the session. Work through them and then ask the class why some of them are very private and why some of them share all of their daily struggles and trama.

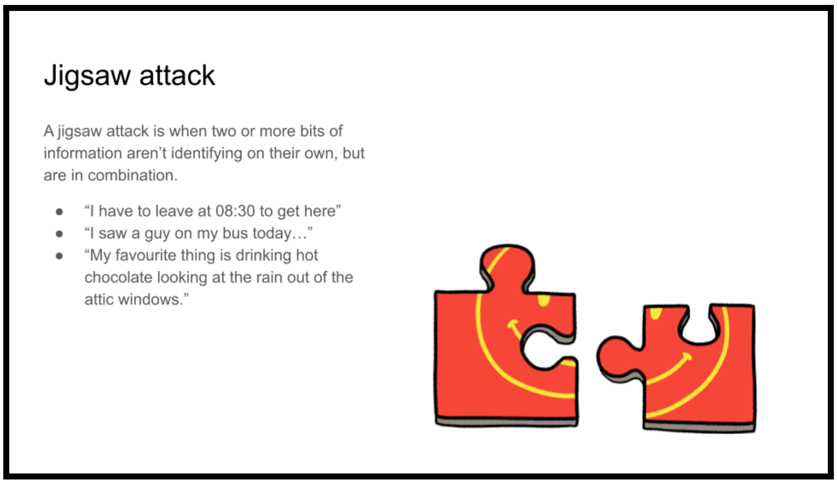
The conclusion that you want them to reach is "There is a balance of power and privacy. When you give up privacy to gain power, you can do more but you expose yourself to more risk". It's an extension to the idea of "When you secure things you make them harder to use"



From wikipedia

Clara Sorrenti, a transgender activist and Twitch streamer under the name "Keffals", was doxxed on Kiwi Farms in a thread dedicated to discussing her. Users on the site posted personal information about her (e.g. addresses, phone numbers) as well as that of her friends and family. Users also leaked sexually explicit photos of her and made death threats.[34][35] She was later swatted, arrested, and detained for over ten hours in August 2022 when someone stole her identity and sent fake emails to local politicians threatening mass violence. She was later cleared of any wrongdoing, and police acknowledged the incident as a swatting attempt. Users also posted the address of an unrelated man who lives in the same city and shares her last name, and police were also sent to his residence. After the swatting incident, Sorrenti said she moved out of her home and into a hotel for her safety.[36][37] After she posted a photograph of her cat laying on the hotel bed, Kiwi Farms users identified the hotel from the bedsheets in the photograph, and sent multiple pizza orders to the hotel under her deadname. "Obviously, the pizza itself isn't the problem. It's the threat they send by telling me they know where I live and are willing to act on it in the real world," she said in a video after the incident.[36][37][38] Sorrenti later fled the country after her location was identified again, reportedly by someone who hacked her Uber account.[39] The incidents are being investigated as criminal harassment, and Sorrenti stated she intended to pursue legal action.[37][40][41] Sorrenti also promoted a campaign to pressure Cloudflare into terminating its services to the website.[3][42]

We have them read this in silence. Familiarise yourself with Sorrenti's wikipedia article in advance and also the one for Kwiw Farms in case you get any questions on it.

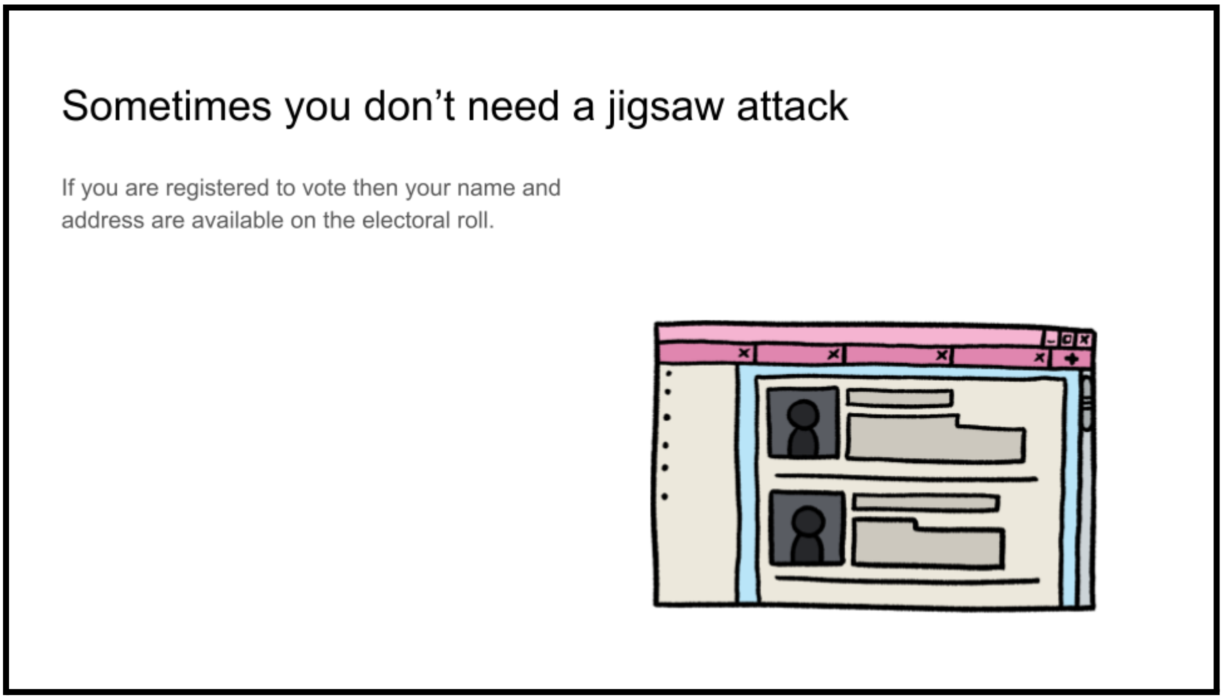


Jigsaw attack

A jigsaw attack is when two or more bits of information aren't identifying on their own, but are in combination.

- "I have to leave at 08:30 to get here"
- "I saw a guy on my bus today…"
- "My favourite thing is drinking hot chocolate looking at the rain out of the attic windows."

Talk a little bit about the information they reveal every day that tells us more about them, and which can contribute to a Jigsaw attack like that suffered by the streamer.



Sometimes you don’t need a jigsaw attack

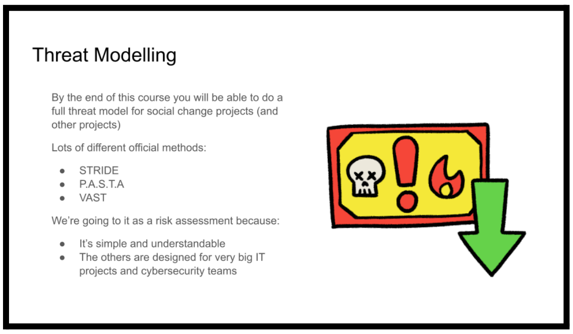
If you are registered to vote then your name and address are available on the electoral roll.

This is a good time to point out to them that their (or more likely, their parent’s) names and addresses are likely on the electoral roll - and you can wander in look people up.[8]

The point we are making here is that sometimes we can focus on the wrong part of security: people can worry about how strong their door lock is, when a thief might otherwise just break a window. This is preparation for the introduction of risk statements next.

[8] I have done this to get the names of my neighbours’ correct when I moved into a new area. I got the impression that nobody had ever asked before.

Risk Statements



Threat Modelling

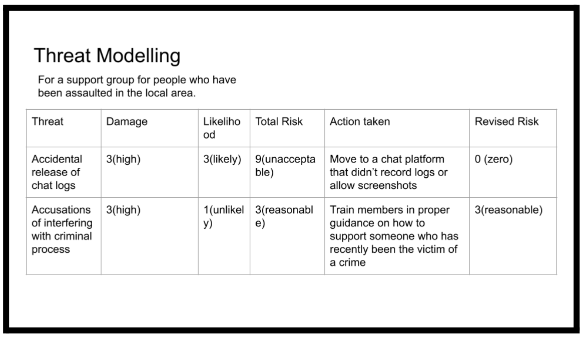
By the end of this course you will be able to do a full threat model for social change projects (and other projects)

Lots of different official methods:

- STRIDE
- P.A.S.T.A
- VAST

We're going to it as a risk assessment because:

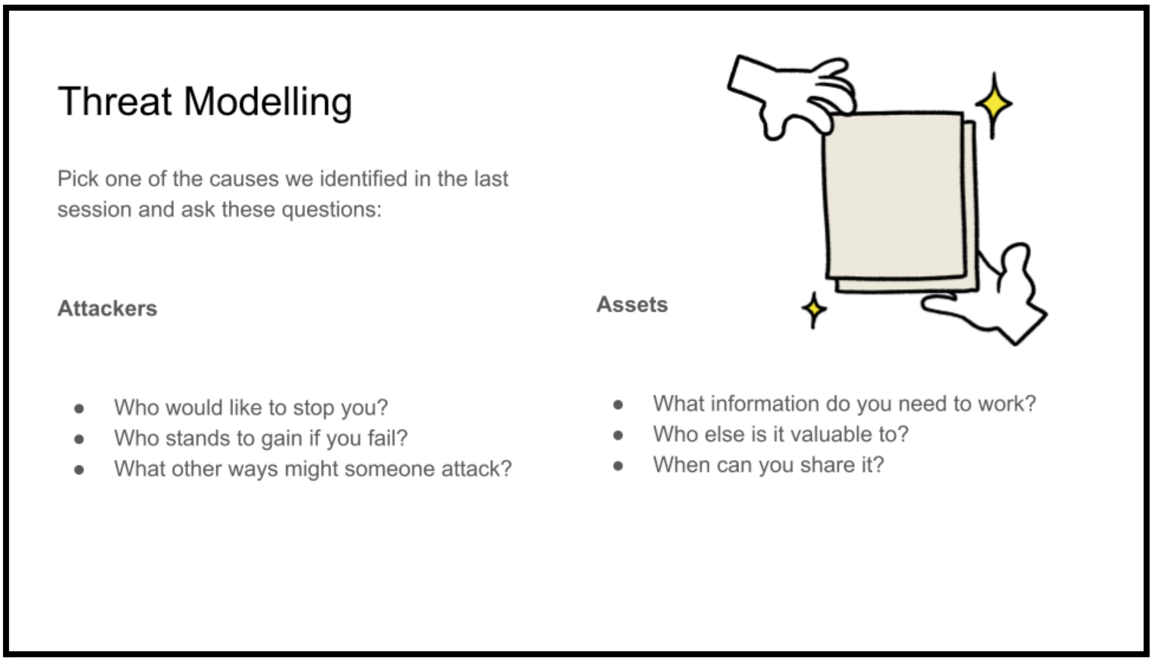
- It's simple and understandable
- The others are designed for very big IT projects and cybersecurity teams



Threat Modelling

For a support group for people who have been assaulted in the local area.

Threat	Damage	Likelihood	Total Risk	Action taken	Revised Risk
Accidental release of chat logs	3(high)	3(likely)	9(unacceptable)	Move to a chat platform that didn't record logs or allow screenshots	0 (zero)
Accusations of interfering with criminal process	3(high)	1(unlikely)	3(reasonable)	Train members in proper guidance on how to support someone who has recently been the victim of a crime	3(reasonable)



Threat Modelling

Pick one of the causes we identified in the last session and ask these questions:

Attackers

- Who would like to stop you?
- Who stands to gain if you fail?
- What other ways might someone attack?

Assets

- What information do you need to work?
- Who else is it valuable to?
- When can you share it?

This exercise is risk statement writing. Give them each a Change Card and get them to write out 20 risks.[9] Get them to be specific. Then they estimate how likely each of them are on a scale of 1-5, then how bad each one would be on a scale of 1-5 and so on in classic risk assessment style

Take them through the process in your remaining time. One game is that works well is putting them in pairs and getting them to come up with a risk that isn't on the other person's list. They get a point each time they do so.

The things that you want them to take from this are:

- There are lots of risks
- The first few they thought of were not the ones with the biggest impact.

[9] It is surprising but outwardly cynical and jaded teenagers often can't actually think of a single specific thing that might go wrong.

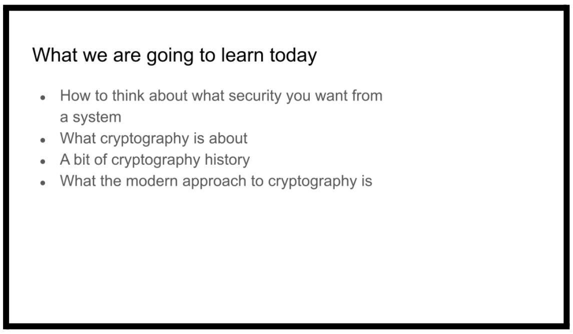
- It works a lot better to write down specific worries and the mitigating actions than it does to just worry.[10]

Session 4 Cryptography

This session aims at introducing the notion of cryptography and what cryptography can provide in terms of security. There will be a bit of history as well, which is intended to show how our understanding of security has evolved. Some parts of the session are a bit technical, but hopefully this guide will support in running through these.

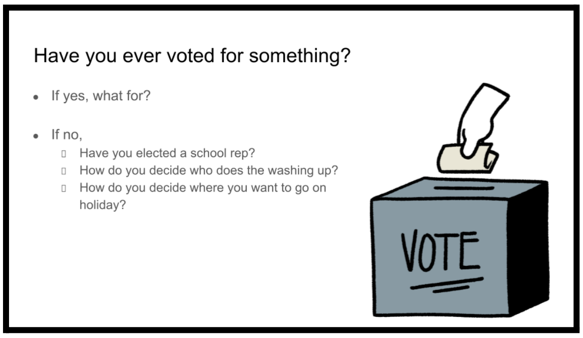
Session 4

Cryptography



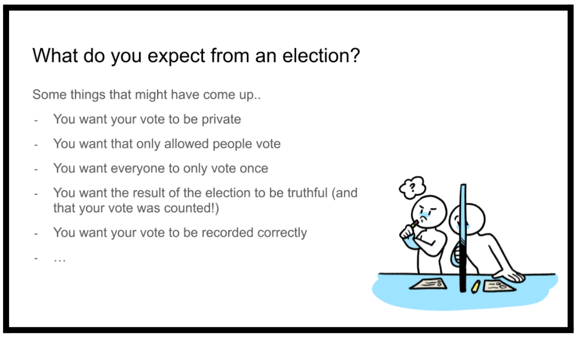
What we are going to learn today

- How to think about what security you want from a system
- What cryptography is about
- A bit of cryptography history
- What the modern approach to cryptography is



Have you ever voted for something?

- If yes, what for?
- If no,
  - Have you elected a school rep?
  - How do you decide who does the washing up?
  - How do you decide where you want to go on holiday?



What do you expect from an election?

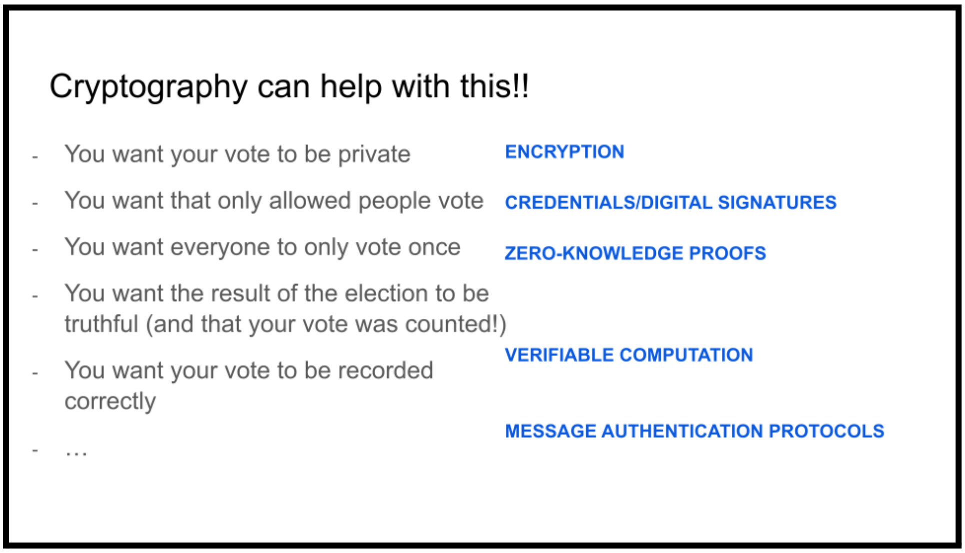
Some things that might have come up..

- You want your vote to be private
- You want that only allowed people vote
- You want everyone to only vote once
- You want the result of the election to be truthful (and that your vote was counted!)
- You want your vote to be recorded correctly
- …

A motivating example that we use to engage with students is thinking about an election.

We ask the students whether they have ever voted for something, and to think about what *security* properties they expect from this process. Possible answers to this are made explicit on slide 4.

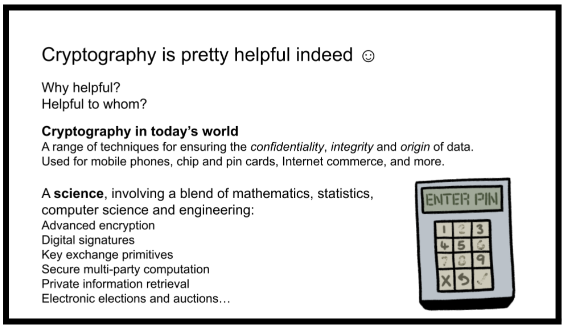
[10] Particularly when we've already established that they are probably worrying about the wrong thing.



Cryptography can help with this!!

- You want your vote to be private — ENCRYPTION
- You want that only allowed people vote — CREDENTIALS/DIGITAL SIGNATURES
- You want everyone to only vote once — ZERO-KNOWLEDGE PROOFS
- You want the result of the election to be truthful (and that your vote was counted!) — VERIFIABLE COMPUTATION
- You want your vote to be recorded correctly — MESSAGE AUTHENTICATION PROTOCOLS
- …

This is a technical slide, where we highlight what cryptographic tool (or primitive) can be used to achieve the properties identified earlier. In particular, *encryption* will help in keeping information private, *credential/digital signatures* will ensure only eligible people can vote, *zero-knowledge proofs* enable a user to prove that they have voted only once without revealing who they voted for, *verifiable computation* makes sure the final result is indeed the correct output. There is no need to go into details of each of the primitives, just naming them should expose the students to the breadth of the discipline and the variety of security properties it can provide.

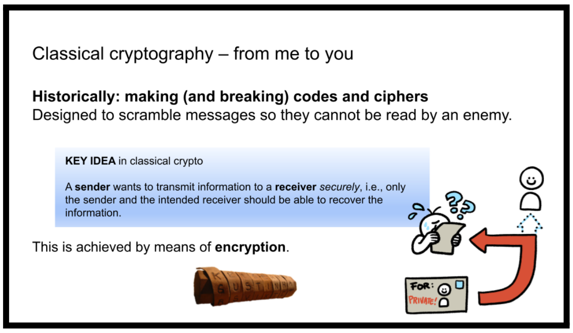


Cryptography is pretty helpful indeed ☺

Why helpful?
Helpful to whom?

Cryptography in today's world
A range of techniques for ensuring the *confidentiality*, *integrity* and *origin* of data.
Used for mobile phones, chip and pin cards, Internet commerce, and more.

A **science**, involving a blend of mathematics, statistics, computer science and engineering:
Advanced encryption
Digital signatures
Key exchange primitives
Secure multi-party computation
Private information retrieval
Electronic elections and auctions…



Classical cryptography – from me to you

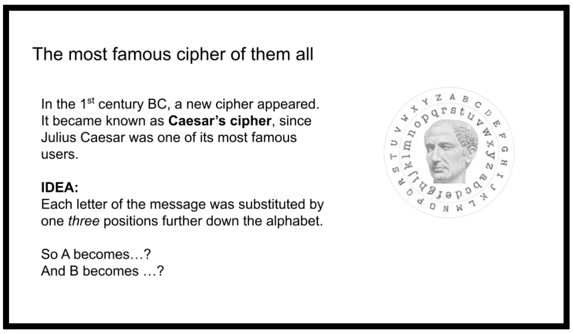
Historically: making (and breaking) codes and ciphers
Designed to scramble messages so they cannot be read by an enemy.

KEY IDEA in classical crypto

A **sender** wants to transmit information to a **receiver** *securely*, i.e., only the sender and the intended receiver should be able to recover the information.

This is achieved by means of **encryption**.

FOR:
PRIVATE!

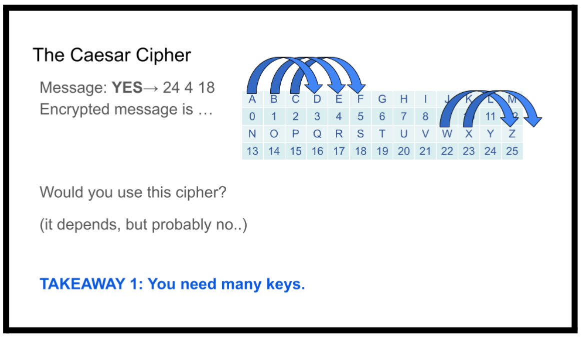


The most famous cipher of them all

In the 1st century BC, a new cipher appeared. It became known as **Caesar's cipher**, since Julius Caesar was one of its most famous users.

IDEA:
Each letter of the message was substituted by one *three* positions further down the alphabet.

So A becomes…?
And B becomes …?



The Caesar Cipher

Message: **YES**→ 24 4 18
Encrypted message is …

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	[illegible]	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

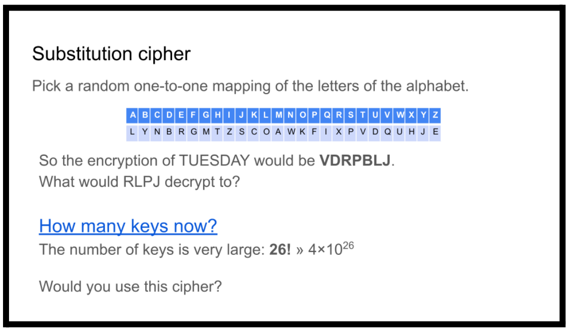
Would you use this cipher?

(it depends, but probably no..)

TAKEAWAY 1: You need many keys.

The above example should motivate why cryptography is useful, leading to a historical dive into the subject, which nowadays is no longer an art, but a full-on scientific discipline, blend of mathematics, computer science, engineering..

Cryptography’s history dates a long way back, and the students may be familiar with some examples of classical cryptography such as the Caesar cipher.
A brief description of it is provided, along with an explanation as to why this is not a very strong cipher, i.e., there are only 26 keys, so you can guess and soon you will find the right one. So takeaway message 1 is that you need many keys for security.



Substitution cipher

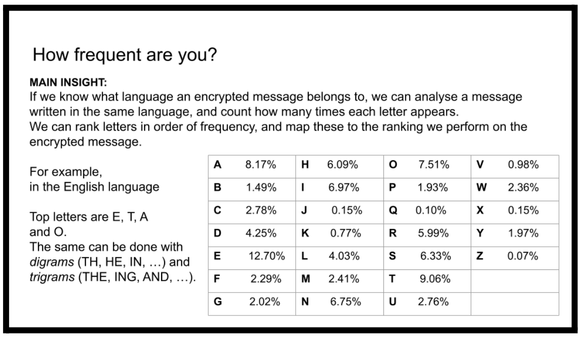
Pick a random one-to-one mapping of the letters of the alphabet.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
L	Y	N	B	R	G	M	T	Z	S	C	O	A	W	K	F	I	X	P	V	D	Q	U	H	J	E

So the encryption of TUESDAY would be **VDRPBLJ**.
What would RLPJ decrypt to?

How many keys now?
The number of keys is very large: **26!** » 4×10^{26}

Would you use this cipher?



How frequent are you?

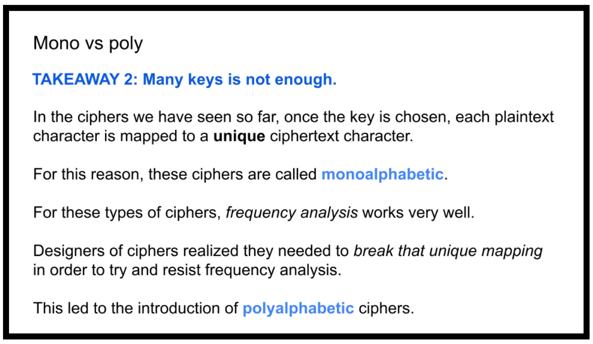
MAIN INSIGHT:
If we know what language an encrypted message belongs to, we can analyse a message written in the same language, and count how many times each letter appears.
We can rank letters in order of frequency, and map these to the ranking we perform on the encrypted message.

For example,
in the English language

Top letters are E, T, A and O.
The same can be done with *digrams* (TH, HE, IN, …) and *trigrams* (THE, ING, AND, …).

A	8.17%	**H**	6.09%	**O**	7.51%	**V**	0.98%
B	1.49%	**I**	6.97%	**P**	1.93%	**W**	2.36%
C	2.78%	**J**	0.15%	**Q**	0.10%	**X**	0.15%
D	4.25%	**K**	0.77%	**R**	5.99%	**Y**	1.97%
E	12.70%	**L**	4.03%	**S**	6.33%	**Z**	0.07%
F	2.29%	**M**	2.41%	**T**	9.06%		
G	2.02%	**N**	6.75%	**U**	2.76%		

This leads to the study of another classical cipher, which overcomes the first issue. Indeed, the substitution cipher has now many keys, but still suffers from a limitation. The students are exposed to the concept of frequency analysis, and the fact that if you consistently map a letter to the same letter, the frequency pattern is maintained, leaking some information. So takeaway message 2 is that a lot of keys is not enough for security.
This eventually led to the shift towards polyalphabetic ciphers, where such pattern is meant to be broken.



Mono vs poly

TAKEAWAY 2: Many keys is not enough.

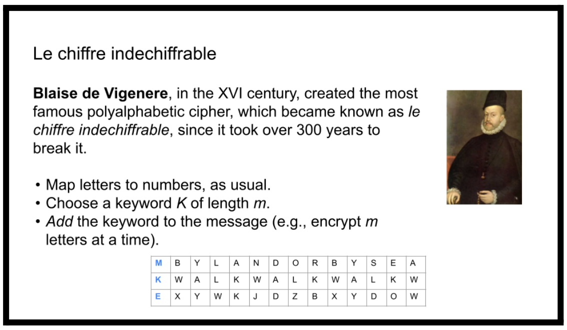
In the ciphers we have seen so far, once the key is chosen, each plaintext character is mapped to a **unique** ciphertext character.

For this reason, these ciphers are called **monoalphabetic**.

For these types of ciphers, *frequency analysis* works very well.

Designers of ciphers realized they needed to *break that unique mapping* in order to try and resist frequency analysis.

This led to the introduction of **polyalphabetic** ciphers.



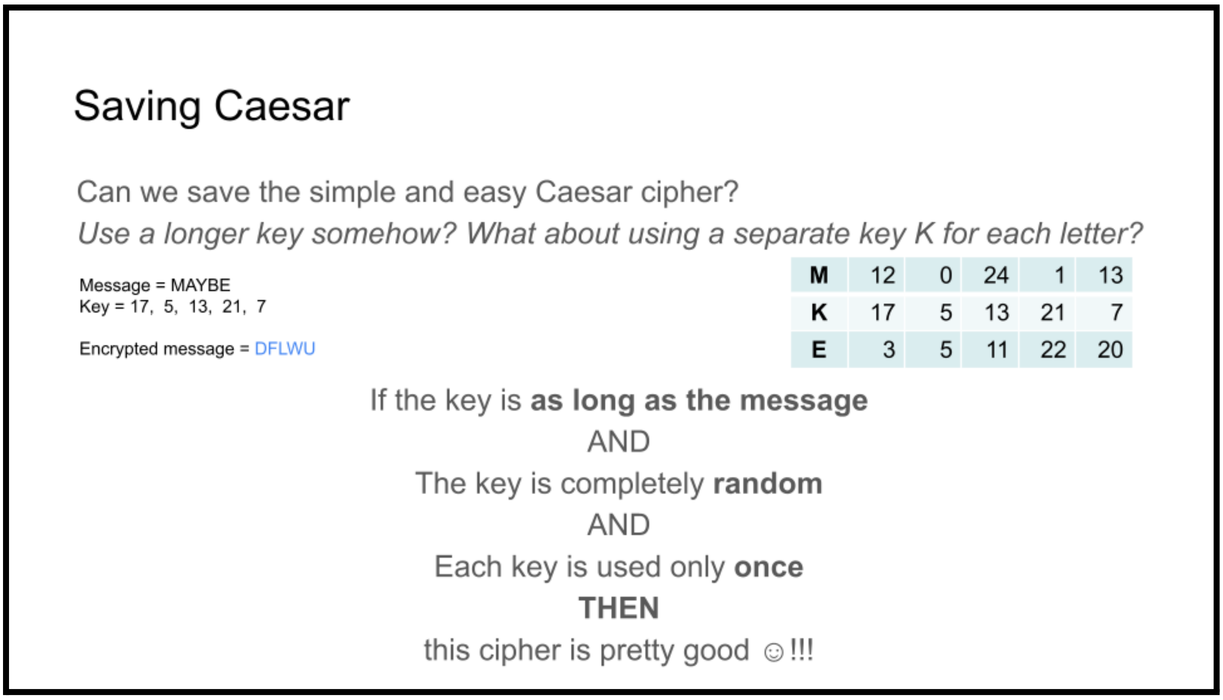
Le chiffre indechiffrable

Blaise de Vigenere, in the XVI century, created the most famous polyalphabetic cipher, which became known as *le chiffre indechiffrable*, since it took over 300 years to break it.

- Map letters to numbers, as usual.
- Choose a keyword *K* of length *m*.
- *Add* the keyword to the message (e.g., encrypt *m* letters at a time).

M	B	Y	L	A	N	D	O	R	B	Y	S	E	A
K	W	A	L	K	W	A	L	K	W	A	L	K	W
E	X	Y	W	K	J	D	Z	B	X	Y	D	O	W

We introduce another very famous cipher, the Vigenere cipher also known as the *unbreakable* cipher, which ironically was indeed broken – 300 years after it was proposed. This cipher attempted to break the pattern we earlier identified as a weakness, but unsuccessfully. The lesson learnt here is that believing a cipher is secure is not enough - we need some formal guarantee and a rigorous framework within which to reason about security properties.



Saving Caesar

Can we save the simple and easy Caesar cipher?

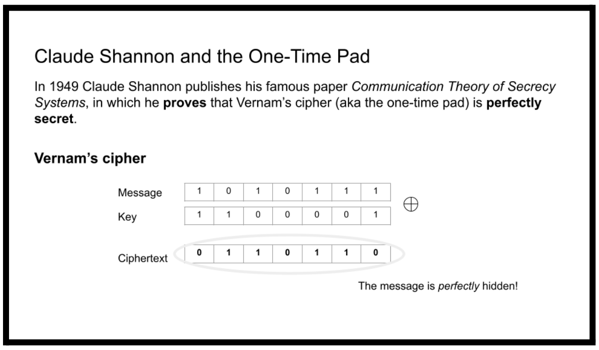
Use a longer key somehow? What about using a separate key K for each letter?

Message = MAYBE
Key = 17, 5, 13, 21, 7

Encrypted message = DFLWU

M	12	0	24	1	13
K	17	5	13	21	7
E	3	5	11	22	20

If the key is **as long as the message**
AND
The key is completely **random**
AND
Each key is used only **once**
THEN
this cipher is pretty good ☺!!!



Claude Shannon and the One-Time Pad

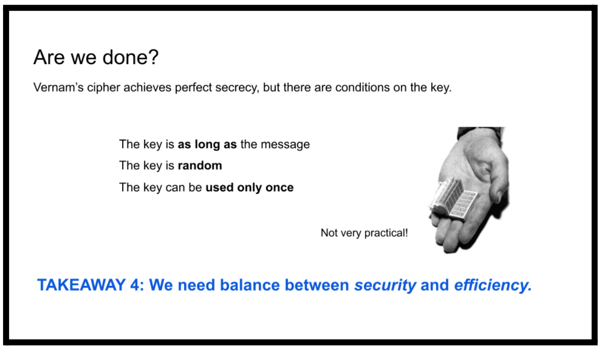
In 1949 Claude Shannon publishes his famous paper *Communication Theory of Secrecy Systems*, in which he **proves** that Vernam's cipher (aka the one-time pad) is **perfectly secret**.

Vernam's cipher

Message	1	0	1	0	1	1	1
Key	1	1	0	0	0	0	1
Ciphertext	**0**	**1**	**1**	**0**	**1**	**1**	**0**

⊕

The message is *perfectly* hidden!



Are we done?

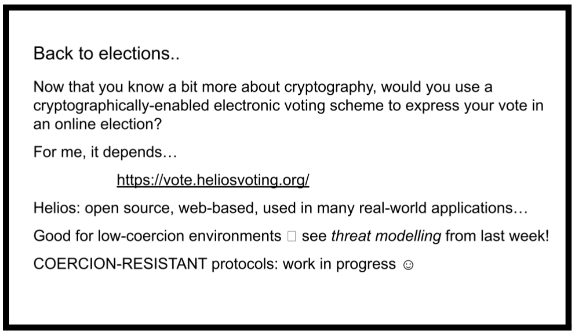
Vernam's cipher achieves perfect secrecy, but there are conditions on the key.

The key is **as long as** the message
The key is **random**
The key can be **used only once**

Not very practical!

TAKEAWAY 4: We need balance between *security* and *efficiency.*

The quick historical voyage finally introduces one of the stepping stones in modern cryptography, which is the introduction of a formal definition of secrecy, allowing to formally prove a cipher is secret. This is (one of) the great contributions of Claude Shannon, in the field of Information Theory. Thanks to this, for the first time, a proof of security was provided for the One Time Pad (OTP), a perfectly secret cipher.
A description of OTP is given, along with the caveats for security, namely that perfect secrecy is achieved only under certain conditions, which severely impact its use in practice. This leads to the motivation behind all modern cryptography, which is to find a balance between security and efficiency.



Back to elections..

Now that you know a bit more about cryptography, would you use a cryptographically-enabled electronic voting scheme to express your vote in an online election?

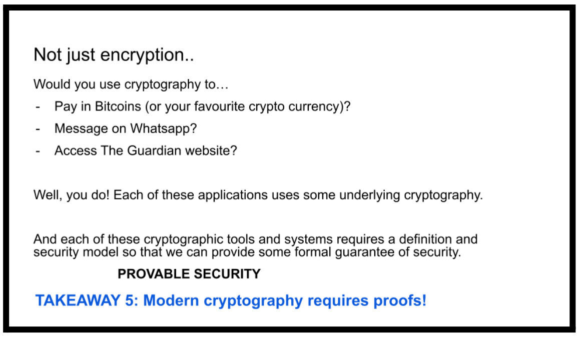
For me, it depends…

https://vote.heliosvoting.org/

Helios: open source, web-based, used in many real-world applications…

Good for low-coercion environments see *threat modelling* from last week!

COERCION-RESISTANT protocols: work in progress ☺



Not just encryption..

Would you use cryptography to…

- Pay in Bitcoins (or your favourite crypto currency)?
- Message on Whatsapp?
- Access The Guardian website?

Well, you do! Each of these applications uses some underlying cryptography.

And each of these cryptographic tools and systems requires a definition and security model so that we can provide some formal guarantee of security.

PROVABLE SECURITY

TAKEAWAY 5: Modern cryptography requires proofs!

This theme is ever present in today's cryptography, and the driving force behind much of its progress. The final slides of this lecture go back to the election examples, and challenge the student to think about whether cryptography is ready to achieve in practice what is needed. And further examples are explored too - highlighting that, whether it is ready or not, we are already using it! And attacks and fixes to issues occur on a regular basis.

The hope is that this session inspires the students to think critically about what security they believe is needed in specific contexts, and question the guarantees that are promised. Understanding the tool behind many of these applications is vital to understand what security can truly be provided.

Session 5: Complete Systems

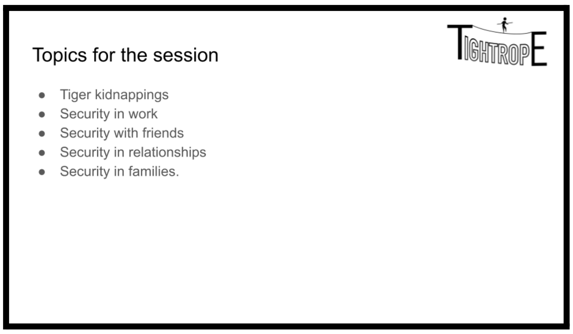
Tiger kidnappings

TIGHTROPE

Session 5

Complex Systems

equalitytime
ROYAL HOLLOWAY UNIVERSITY OF LONDON

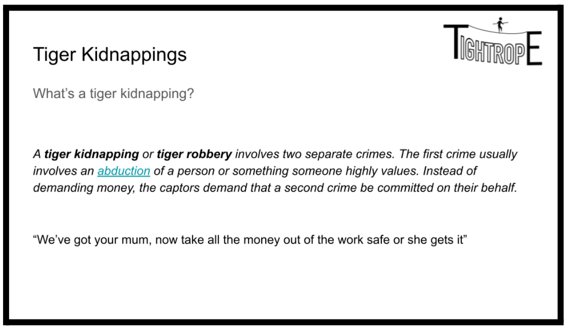


Topics for the session

- Tiger kidnappings
- Security in work
- Security with friends
- Security in relationships
- Security in families.

Tiger Kidnappings

What's a tiger kidnapping?



Tiger Kidnappings

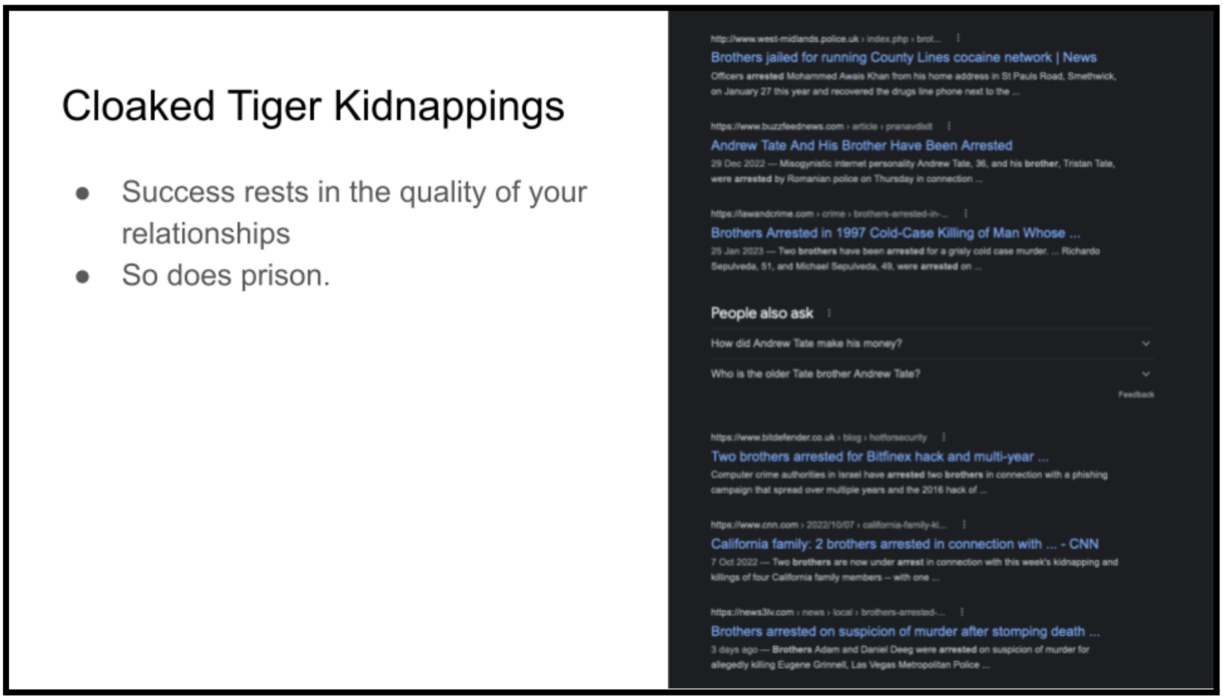
What's a tiger kidnapping?

A ***tiger kidnapping*** *or* ***tiger robbery*** *involves two separate crimes. The first crime usually involves an abduction of a person or something someone highly values. Instead of demanding money, the captors demand that a second crime be committed on their behalf.*

"We've got your mum, now take all the money out of the work safe or she gets it"

This is a simple introduction to Tiger Kidnappings. It's worth reading https://en.wikipedia.org/wiki/Securitas_depot_robbery and https://en.m.wikipedia.org/wiki/Northern_Bank_robbery in advance. The key takeaways are:

- It's almost impossible for a business to effectively defend against a Tiger kidnapping. Employees won't take the risks (and we wouldn't want them to)
- Thus the burden of the 'security' is on the police - can they regularly catch people *after* a Tiger Kidnapping so that it's not as attractive an option.



Cloaked Tiger Kidnappings

- Success rests in the quality of your relationships
- So does prison.

http://www.west-midlands.police.uk › index.php › brot...

Brothers jailed for running County Lines cocaine network | News

Officers arrested Mohammed Awais Khan from his home address in St Pauls Road, Smethwick, on January 27 this year and recovered the drugs line phone next to the ...

https://www.buzzfeednews.com › article › pranavdixit

Andrew Tate And His Brother Have Been Arrested

29 Dec 2022 — Misogynistic internet personality Andrew Tate, 36, and his brother, Tristan Tate, were arrested by Romanian police on Thursday in connection ...

https://lawandcrime.com › crime › brothers-arrested-in-...

Brothers Arrested in 1997 Cold-Case Killing of Man Whose ...

25 Jan 2023 — Two brothers have been arrested for a grisly cold case murder. ... Richardo Sepulveda, 51, and Michael Sepulveda, 49, were arrested on ...

People also ask

How did Andrew Tate make his money?

Who is the older Tate brother Andrew Tate?

Feedback

https://www.bitdefender.co.uk › blog › hotforsecurity

Two brothers arrested for Bitfinex hack and multi-year ...

Computer crime authorities in Israel have arrested two brothers in connection with a phishing campaign that spread over multiple years and the 2016 hack of ...

https://www.cnn.com › 2022/10/07 › california-family-ki...

California family: 2 brothers arrested in connection with ... - CNN

7 Oct 2022 — Two brothers are now under arrest in connection with this week's kidnapping and killings of four California family members -- with one ...

https://news3lv.com › news › local › brothers-arrested-...

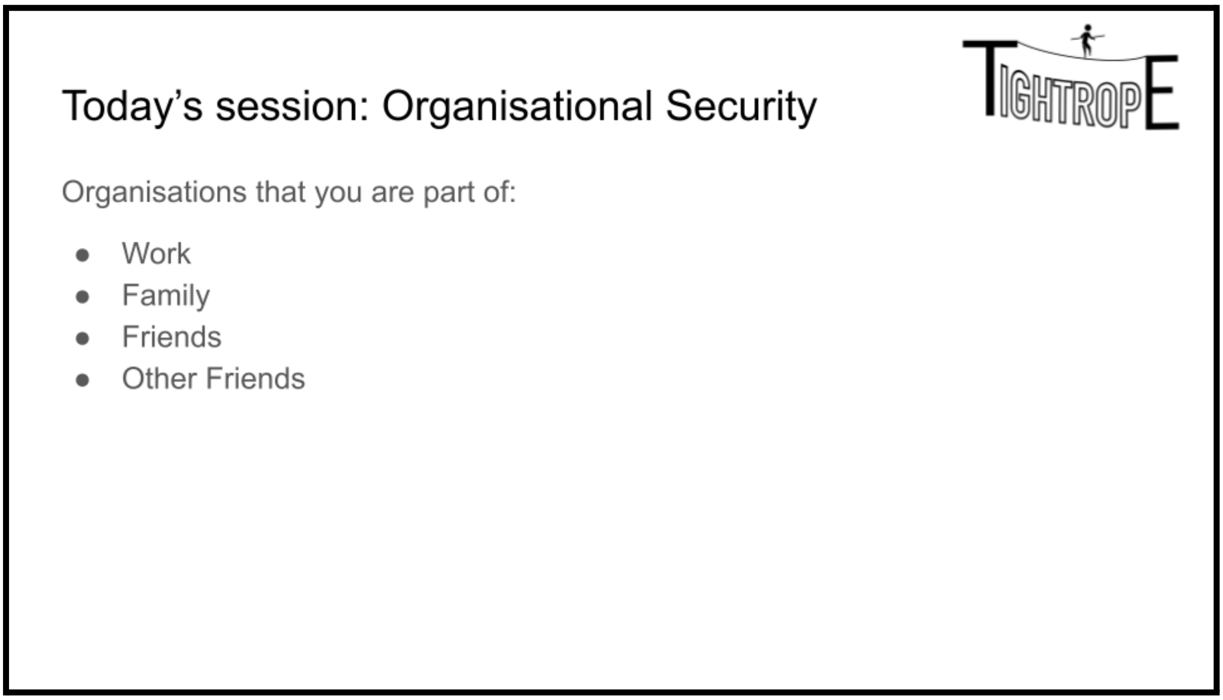
Brothers arrested on suspicion of murder after stomping death ...

3 days ago — Brothers Adam and Daniel Deeg were arrested on suspicion of murder for allegedly killing Eugene Grinnell, Las Vegas Metropolitan Police ...

The image on the right is just a google should for 'brothers' and 'prison'.

The point this slide makes (to foreground some things for later) is that some social situations can end up as effective tiger kidnapings. Examples include - feeling pressured to give an alibi for a family member, or being put in a situation of general harm. This is especially obvious from talking to prison inmates.

Complex Systems

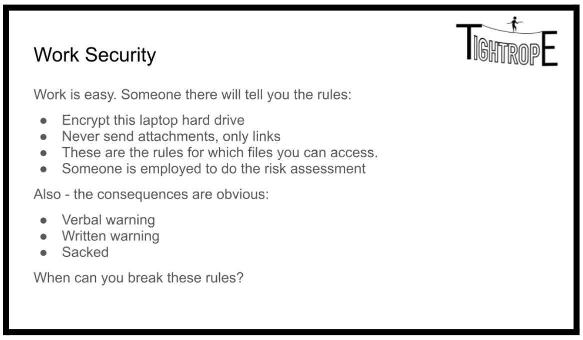


Today’s session: Organisational Security

Organisations that you are part of:

- Work
- Family
- Friends
- Other Friends

Ask the students which of the above are hardest to make secure. Normally we get a 50-50 split between Work and Family.   Tell them that Work is easily and we’re going to work through the sets in order of how hard they are to make secure.



Work Security

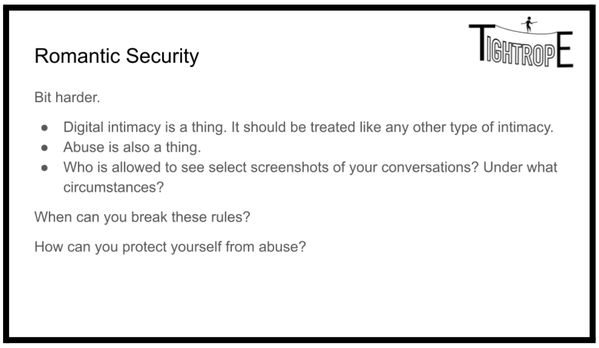
Work is easy. Someone there will tell you the rules:

- Encrypt this laptop hard drive
- Never send attachments, only links
- These are the rules for which files you can access.
- Someone is employed to do the risk assessment

Also - the consequences are obvious:

- Verbal warning
- Written warning
- Sacked

When can you break these rules?



Romantic Security

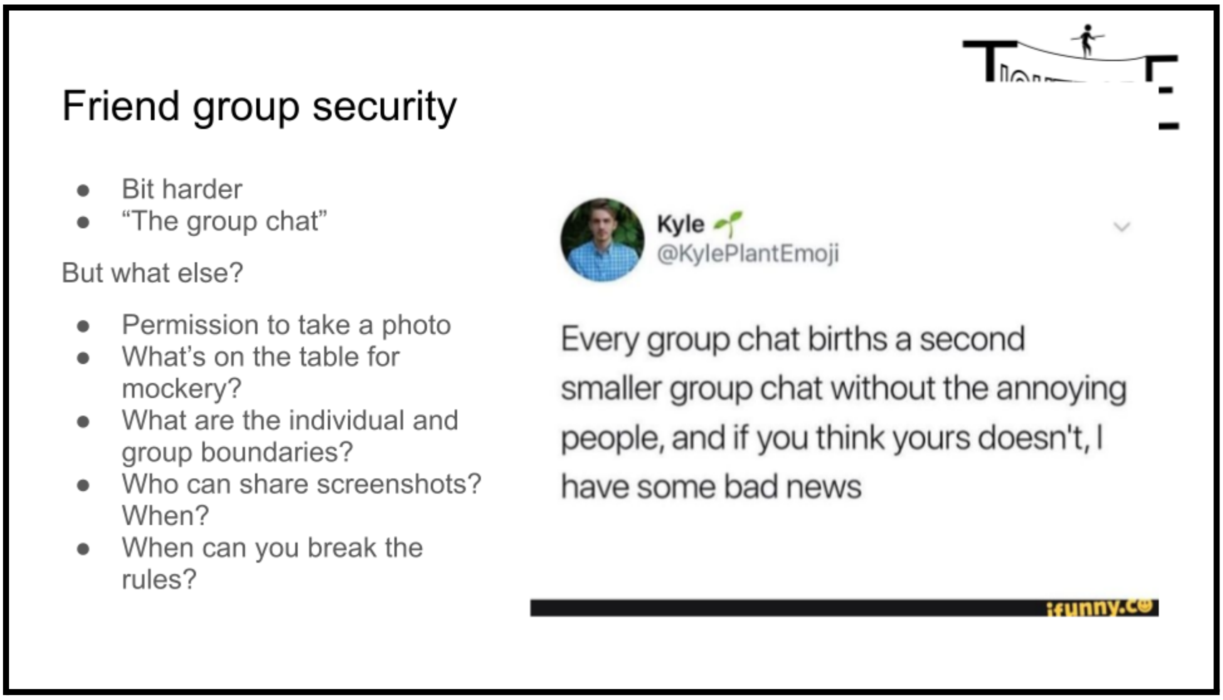
Bit harder.

- Digital intimacy is a thing. It should be treated like any other type of intimacy.
- Abuse is also a thing.
- Who is allowed to see select screenshots of your conversations? Under what circumstances?

When can you break these rules?

How can you protect yourself from abuse?

The work security slide is for general conversation. Some tact and age-appropriate conversation is needed for romance slide, but it’s an important one for the students - they should think hard about digital intimacy.



Friend group security

- Bit harder
- “The group chat”

But what else?

- Permission to take a photo
- What’s on the table for mockery?
- What are the individual and group boundaries?
- Who can share screenshots? When?
- When can you break the rules?

Kyle
@KylePlantEmoji

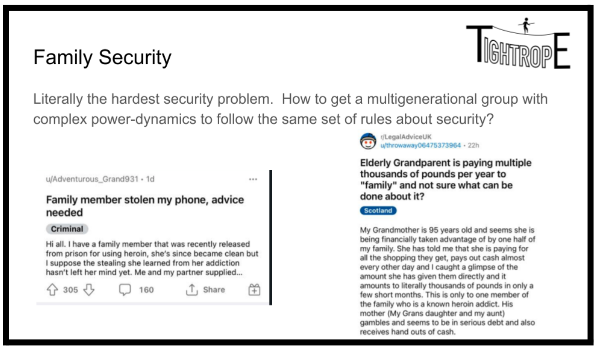
Every group chat births a second smaller group chat without the annoying people, and if you think yours doesn't, I have some bad news

ifunny.co

Have a general conversation about the rules and ask if they have talked about them, and if they think everybody understands the rules the same way.

Once they are comfortable with it, talk to them about the Warick Group Chat scandal (triggering for threats of sexual violence https://www.bbc.co.uk/news/uk-48366835).

If you have time, broaden the conversation out to ‘group chat of the people trying to make a change with you’ and ask how it’s different.



Family Security

Literally the hardest security problem. How to get a multigenerational group with complex power-dynamics to follow the same set of rules about security?

u/Adventurous_Grand931 • 1d

Family member stolen my phone, advice needed

Criminal

Hi all. I have a family member that was recently released from prison for using heroin, she’s since became clean but I suppose the stealing she learned from her addiction hasn’t left her mind yet. Me and my partner supplied...

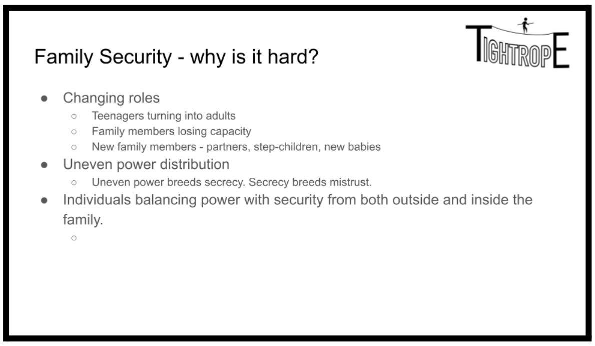
305 160 Share

r/LegalAdviceUK
u/throwaway06475373964 • 22h

Elderly Grandparent is paying multiple thousands of pounds per year to "family" and not sure what can be done about it?

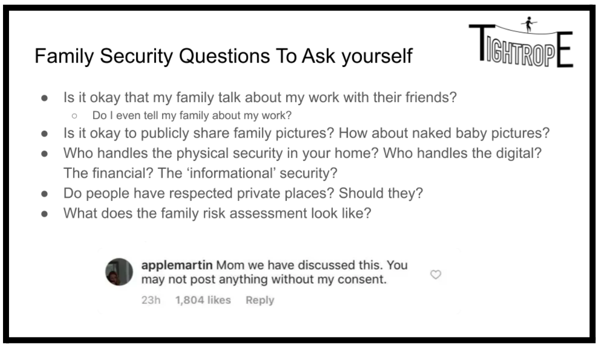
Scotland

My Grandmother is 95 years old and seems she is being financially taken advantage of by one half of my family. She has told me that she is paying for all the shopping they get, pays out cash almost every other day and I caught a glimpse of the amount she has given them directly and it amounts to literally thousands of pounds in only a few short months. This is only to one member of the family who is a known heroin addict. His mother (My Grans daughter and my aunt) gambles and seems to be in serious debt and also receives hand outs of cash.



Family Security - why is it hard?

- Changing roles
  - Teenagers turning into adults
  - Family members losing capacity
  - New family members - partners, step-children, new babies
- Uneven power distribution
  - Uneven power breeds secrecy. Secrecy breeds mistrust.
- Individuals balancing power with security from both outside and inside the family.
  -



Family Security Questions To Ask yourself

- Is it okay that my family talk about my work with their friends?
  - Do I even tell my family about my work?
- Is it okay to publicly share family pictures? How about naked baby pictures?
- Who handles the physical security in your home? Who handles the digital? The financial? The ‘informational’ security?
- Do people have respected private places? Should they?
- What does the family risk assessment look like?

applemartin Mom we have discussed this. You may not post anything without my consent.
23h 1,804 likes Reply

Lead a gentle conversation about risk in family situations and how it’s managed.   The ‘applemartin’ screenshot is Gwyneth Paltrow’s daughter commenting on a photo her mum put up.

Session 6: Scams and Magic

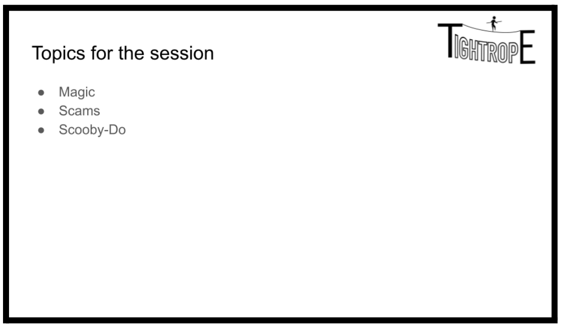
TIGHTROPE

Session 6

Scams and Magic

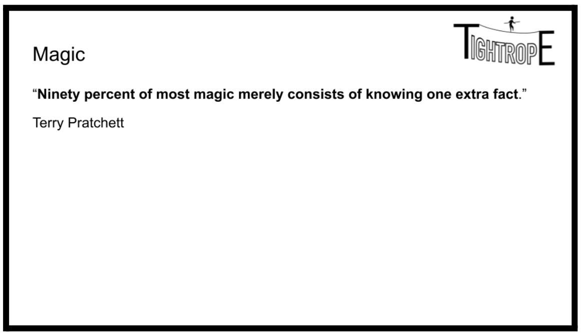
equalitytime

ROYAL HOLLOWAY UNIVERSITY OF LONDON



Topics for the session

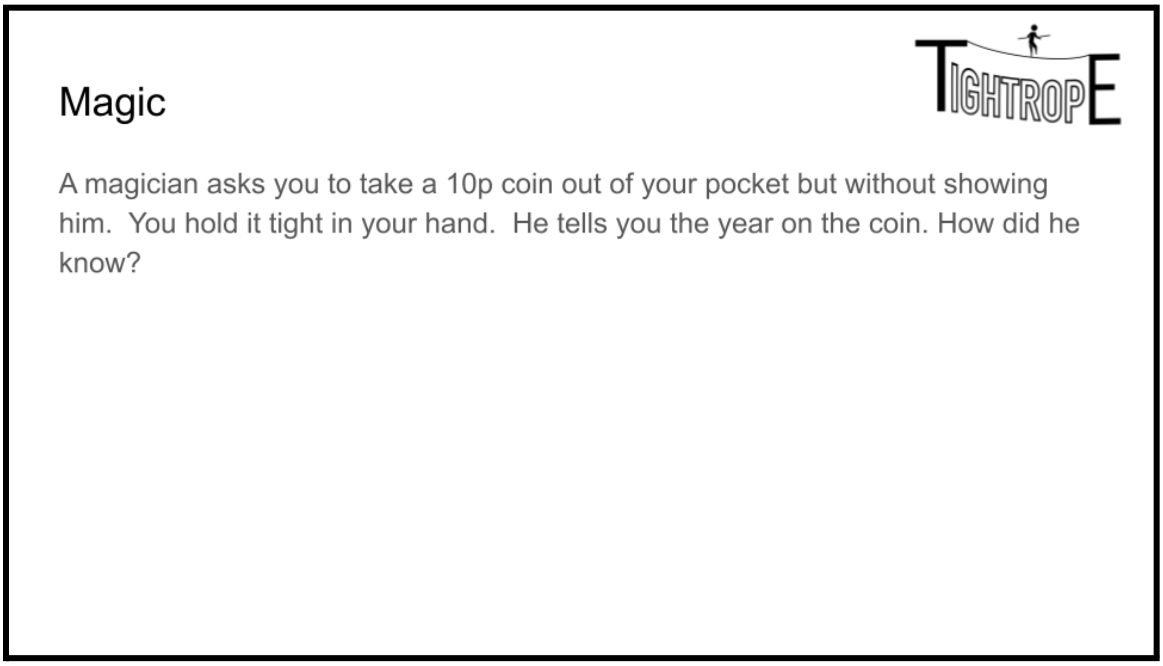
- Magic
- Scams
- Scooby-Do



Magic

“**Ninety percent of most magic merely consists of knowing one extra fact.**”

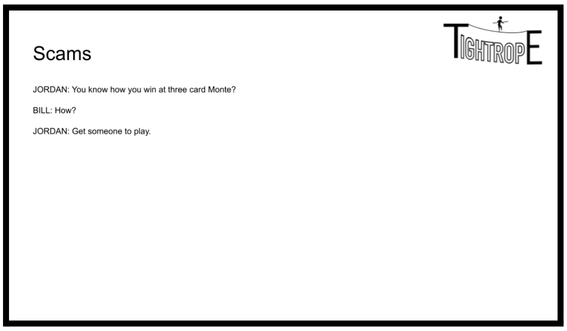
Terry Pratchett



Magic

A magician asks you to take a 10p coin out of your pocket but without showing him. You hold it tight in your hand. He tells you the year on the coin. How did he know?

The UK changed to a smaller 10p in 1992, so the vast majority of 10p coins in circulation have this year on them. That’s the one additional fact mentioned before (This is a Derren Brown trick, but let the student’s know he doesn’t use it any more because it’s getting increasingly unreliable)

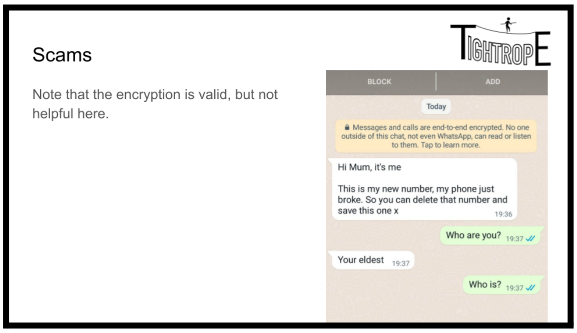


Scams

JORDAN: You know how you win at three card Monte?

BILL: How?

JORDAN: Get someone to play.



Scams

Note that the encryption is valid, but not helpful here.

Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

Hi Mum, it's me

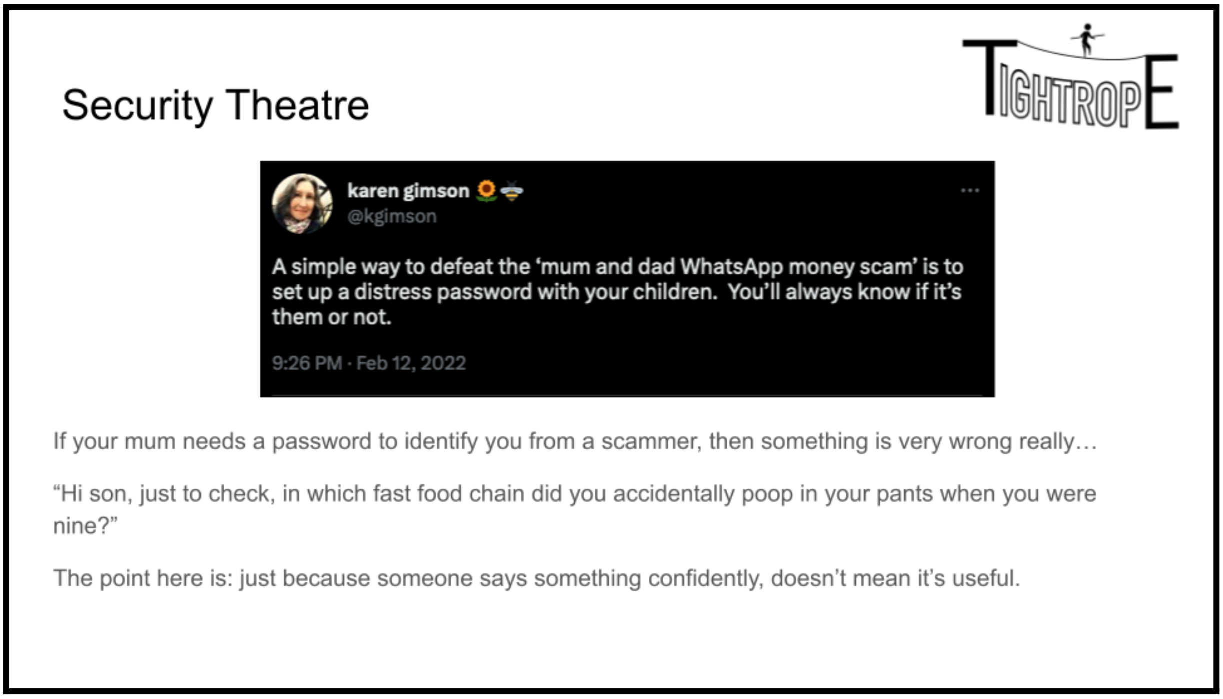
This is my new number, my phone just broke. So you can delete that number and save this one x 19:36

Who are you? 19:37

Your eldest 19:37

Who is? 19:37

Ask the students if their parents would fall for this, and what would happen. Then tactfully broaden it out to grandparents.



Security Theatre

karen gimson 🌻🐝
@kgimson

A simple way to defeat the 'mum and dad WhatsApp money scam' is to set up a distress password with your children. You'll always know if it's them or not.

9:26 PM · Feb 12, 2022

If your mum needs a password to identify you from a scammer, then something is very wrong really…

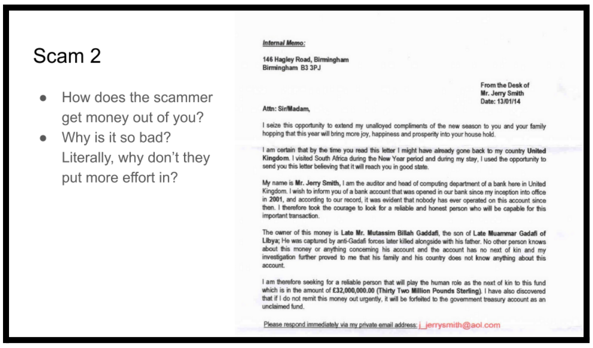
"Hi son, just to check, in which fast food chain did you accidentally poop in your pants when you were nine?"

The point here is: just because someone says something confidently, doesn't mean it's useful.

This is a great time to introduce the concept of 'security theatre' (there is a not particularly good wikipedia article here: https://en.wikipedia.org/wiki/Security_theater).

'Security Theatre' are practices that don't help with security (a good example is when a website has particularly strange password rules) but looks like it does to reassure people.

Advance Fee Fraud



Scam 2

- How does the scammer get money out of you?
- Why is it so bad? Literally, why don't they put more effort in?

Internal Memo:

146 Hagley Road, Birmingham
Birmingham B3 3PJ

From the Desk of
Mr. Jerry Smith
Date: 13/01/14

Attn: Sir/Madam,

I seize this opportunity to extend my unalloyed compliments of the new season to you and your family hopping that this year will bring more joy, happiness and prosperity into your house hold.

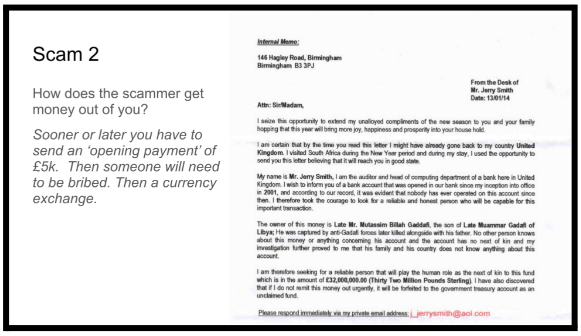
I am certain that by the time you read this letter I might have already gone back to my country **United Kingdom**. I visited South Africa during the New Year period and during my stay, I used the opportunity to send you this letter believing that it will reach you in good state.

My name is **Mr. Jerry Smith,** I am the auditor and head of computing department of a bank here in United Kingdom. I wish to inform you of a bank account that was opened in our bank since my inception into office in **2001**, and according to our record, it was evident that nobody has ever operated on this account since then. I therefore took the courage to look for a reliable and honest person who will be capable for this important transaction.

The owner of this money is **Late Mr. Mutassim Billah Gaddafi**, the son of **Late Muammar Gadafi of Libya;** He was captured by anti-Gadafi forces later killed alongside with his father. No other person knows about this money or anything concerning his account and the account has no next of kin and my investigation further proved to me that his family and his country does not know anything about this account.

I am therefore seeking for a reliable person that will play the human role as the next of kin to this fund which is in the amount of **£32,000,000.00 (Thirty Two Million Pounds Sterling)**. I have also discovered that if I do not remit this money out urgently, it will be forfeited to the government treasury account as an unclaimed fund.

Please respond immediately via my private email address: j_jerrysmith@aol.com



Scam 2

How does the scammer get money out of you?

Sooner or later you have to send an 'opening payment' of £5k. Then someone will need to be bribed. Then a currency exchange.

Internal Memo:

146 Hagley Road, Birmingham
Birmingham B3 3PJ

From the Desk of
Mr. Jerry Smith
Date: 13/01/14

Attn: Sir/Madam,

I seize this opportunity to extend my unalloyed compliments of the new season to you and your family hopping that this year will bring more joy, happiness and prosperity into your house hold.

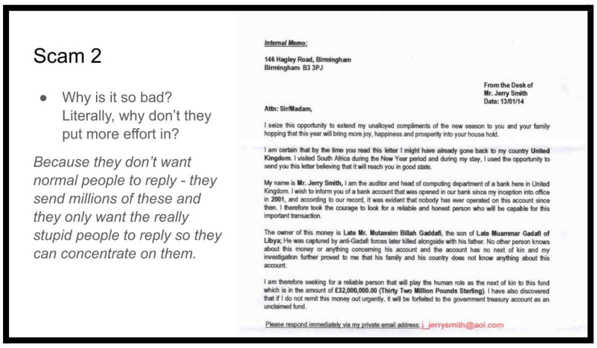
I am certain that by the time you read this letter I might have already gone back to my country **United Kingdom**. I visited South Africa during the New Year period and during my stay, I used the opportunity to send you this letter believing that it will reach you in good state.

My name is **Mr. Jerry Smith,** I am the auditor and head of computing department of a bank here in United Kingdom. I wish to inform you of a bank account that was opened in our bank since my inception into office in **2001**, and according to our record, it was evident that nobody has ever operated on this account since then. I therefore took the courage to look for a reliable and honest person who will be capable for this important transaction.

The owner of this money is **Late Mr. Mutassim Billah Gaddafi**, the son of **Late Muammar Gadafi of Libya;** He was captured by anti-Gadafi forces later killed alongside with his father. No other person knows about this money or anything concerning his account and the account has no next of kin and my investigation further proved to me that his family and his country does not know anything about this account.

I am therefore seeking for a reliable person that will play the human role as the next of kin to this fund which is in the amount of **£32,000,000.00 (Thirty Two Million Pounds Sterling)**. I have also discovered that if I do not remit this money out urgently, it will be forfeited to the government treasury account as an unclaimed fund.

Please respond immediately via my private email address: j_jerrysmith@aol.com



Scam 2

- Why is it so bad? Literally, why don't they put more effort in?

Because they don't want normal people to reply - they send millions of these and they only want the really stupid people to reply so they can concentrate on them.

Internal Memo:

146 Hagley Road, Birmingham
Birmingham B3 3PJ

From the Desk of
Mr. Jerry Smith
Date: 13/01/14

Attn: Sir/Madam,

I seize this opportunity to extend my unalloyed compliments of the new season to you and your family hopping that this year will bring more joy, happiness and prosperity into your house hold.

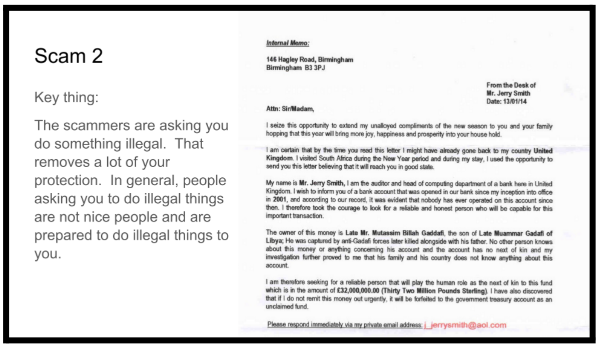
I am certain that by the time you read this letter I might have already gone back to my country **United Kingdom**. I visited South Africa during the New Year period and during my stay, I used the opportunity to send you this letter believing that it will reach you in good state.

My name is **Mr. Jerry Smith,** I am the auditor and head of computing department of a bank here in United Kingdom. I wish to inform you of a bank account that was opened in our bank since my inception into office in **2001**, and according to our record, it was evident that nobody has ever operated on this account since then. I therefore took the courage to look for a reliable and honest person who will be capable for this important transaction.

The owner of this money is **Late Mr. Mutassim Billah Gaddafi**, the son of **Late Muammar Gadafi of Libya;** He was captured by anti-Gadafi forces later killed alongside with his father. No other person knows about this money or anything concerning his account and the account has no next of kin and my investigation further proved to me that his family and his country does not know anything about this account.

I am therefore seeking for a reliable person that will play the human role as the next of kin to this fund which is in the amount of **£32,000,000.00 (Thirty Two Million Pounds Sterling)**. I have also discovered that if I do not remit this money out urgently, it will be forfeited to the government treasury account as an unclaimed fund.

Please respond immediately via my private email address: j_jerrysmith@aol.com



Scam 2

Key thing:

The scammers are asking you do something illegal. That removes a lot of your protection. In general, people asking you to do illegal things are not nice people and are prepared to do illegal things to you.

Internal Memo:

146 Hagley Road, Birmingham
Birmingham B3 3PJ

From the Desk of
Mr. Jerry Smith
Date: 13/01/14

Attn: Sir/Madam,

I seize this opportunity to extend my unalloyed compliments of the new season to you and your family hopping that this year will bring more joy, happiness and prosperity into your house hold.

I am certain that by the time you read this letter I might have already gone back to my country **United Kingdom**. I visited South Africa during the New Year period and during my stay, I used the opportunity to send you this letter believing that it will reach you in good state.

My name is **Mr. Jerry Smith,** I am the auditor and head of computing department of a bank here in United Kingdom. I wish to inform you of a bank account that was opened in our bank since my inception into office in **2001**, and according to our record, it was evident that nobody has ever operated on this account since then. I therefore took the courage to look for a reliable and honest person who will be capable for this important transaction.

The owner of this money is **Late Mr. Mutassim Billah Gaddafi**, the son of **Late Muammar Gadafi of Libya;** He was captured by anti-Gadafi forces later killed alongside with his father. No other person knows about this money or anything concerning his account and the account has no next of kin and my investigation further proved to me that his family and his country does not know anything about this account.

I am therefore seeking for a reliable person that will play the human role as the next of kin to this fund which is in the amount of **£32,000,000.00 (Thirty Two Million Pounds Sterling)**. I have also discovered that if I do not remit this money out urgently, it will be forfeited to the government treasury account as an unclaimed fund.

Please respond immediately via my private email address: j_jerrysmith@aol.com

An overview of advance-fee fraud. Worth reading https://en.wikipedia.org/wiki/Advance-fee_scam first and definitely https://gizmodo.com/why-nigerian-scammers-say-theyre-from-nigeria-5919818

If you want to find out more you can also look at https://en.wikipedia.org/wiki/419eater.com, which is a strange community all of its own.

Cyber Security

So yes, you've been learning Cyber Security all this time. The course follows CyBOK, which sounds like a Marvel Supervillain, but is actually the national syllabus for learning cyber security.

What we did, was change the examples to ones that are interesting to people who want to make change, instead of examples for people who like things to stay as they are.

Cyber Security

Cyber Security needs people like you. It has contains too many people that want the world to stay as it is.

You can do a lot of good by internalising the principles in this course and taking them with you - but you could also find out more about this stuff by studying Cyber Security more seriously.