# Digital Safety & Security Training

rntc media training centre

RNW media

# Camille

# AGENDA

**Introduction to Information Security**
(09:00-10:00)

**Travel Security**
(10:10-11:10)

**Protecting your Partners**
(11:20-12:20)

**Next Steps**
(13:20-14:00)

# Introduction

- What you need / etiquette
- Discussion of OLA exercise
- Our Approach
- Privacy and Security
- Principles

# WHAT YOU NEED

Camera on, mic off

Notebook and pen

OLA account

Smartphone

rntc

RNW media

# Training etiquette

- Be prepared
- Be attentive / show feedback
- Respect views of other participants
- No recordings or screenshots of training
- Be an active participant

# Introduction

What you need / Etiquette

Discussion of OLA Exercise

Our Approach

Privacy and Security

Principles

# Discussion
OLA exercise

## What might the short, medium and long-term impacts of such hacks be?

our websites/information to people can be manipulated

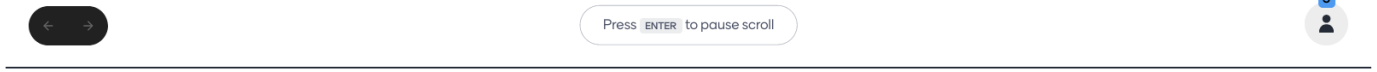
people will loose trust in our brand

people will stop supporting us

Long term: reputation damage, increased staff turnover, difficulty starting new projects with new partners, difficulty hiring new staff

Short term: Increased negative press attenion on us/partners, Government of partner country shows increased intereset in activities, operations are slowed down or stopped depending on nature of hack or type of information exposed.

Medium term: Disinformation campaigns, donor loss, breakdown of relationship with partner(s)




https://www.menti.com/alr4f3f7xakg

# “PREPARE TO BE HACKED”

*PS. Everything is going to be fine*

rntc

# Introduction

What you need / Etiquette

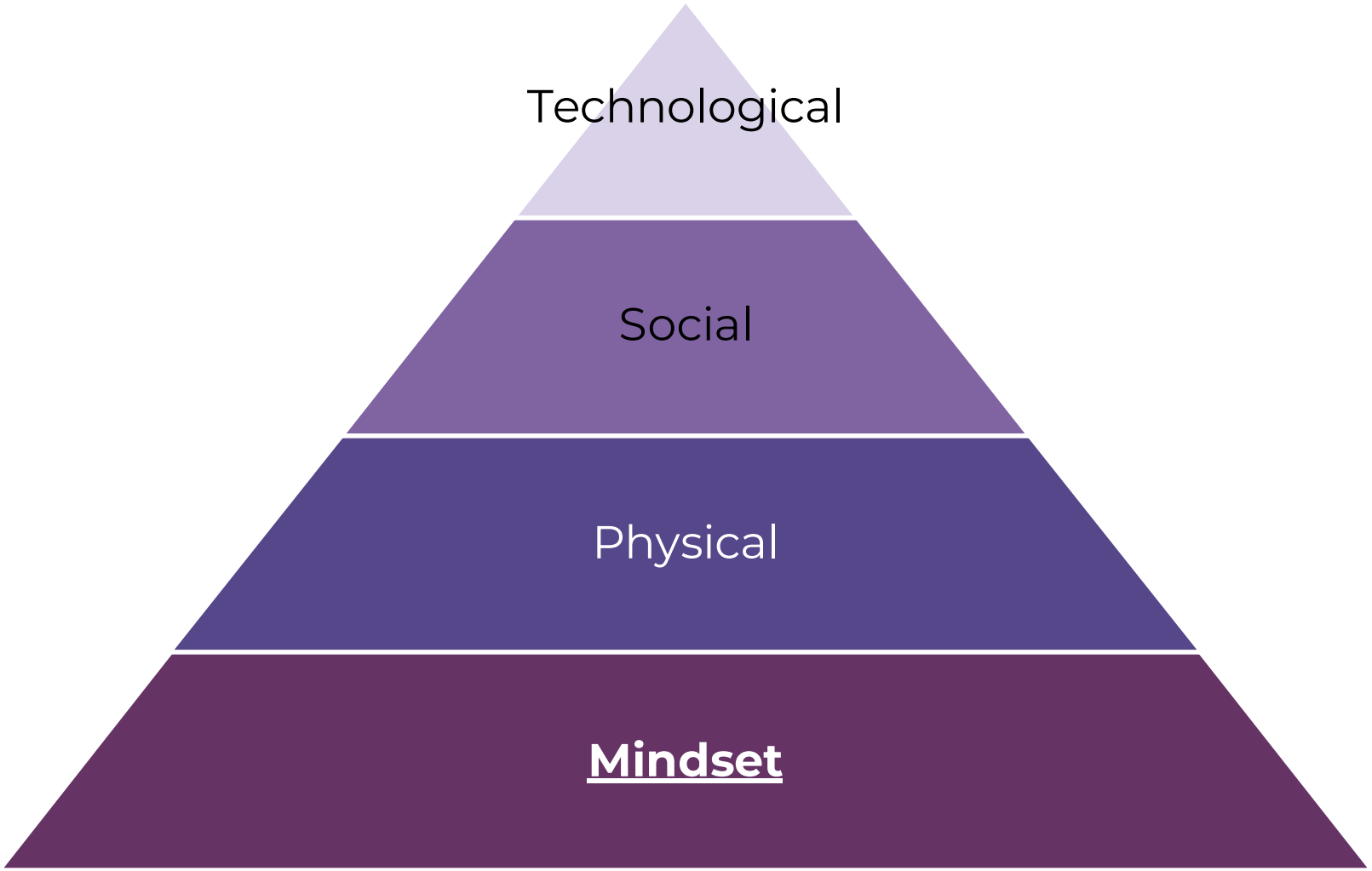
Discussion of OLA Exercise

Our Approach

Privacy and Security

Principles

# THE HOLISTIC SECURITY PYRAMID




rntc


# The Holistic Security Pyramid game

Go to **menti.com**, enter the code [X] and answer the following question:

## Where does the 'action' fall on the holistic security Pyramid?

# Introduction

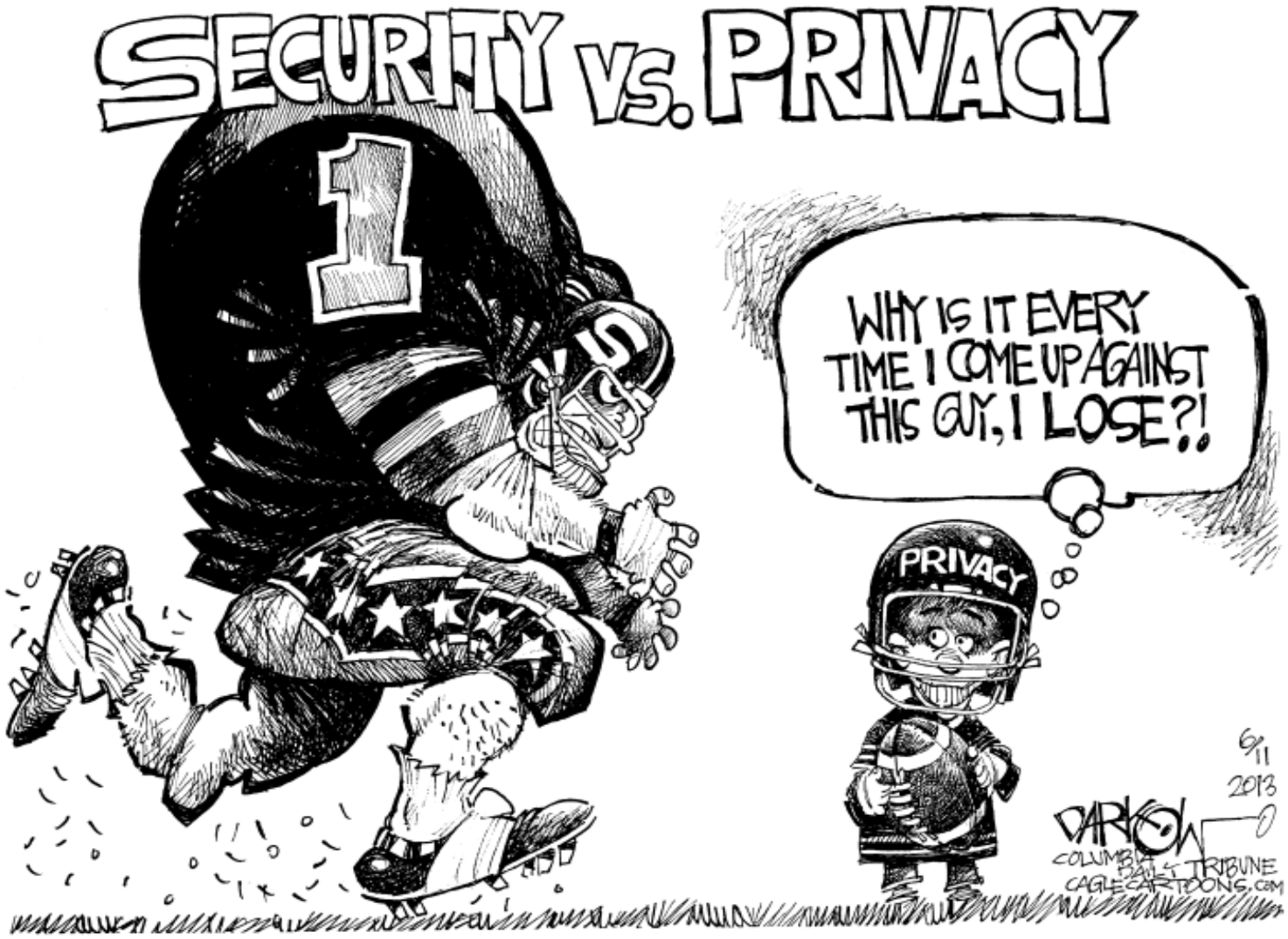
What you need / Etiquette

Discussion of OLA Exercise

Our Approach

Privacy and Security

Principles


SECURITY vs. PRIVACY
1
WHY IS IT EVERY TIME I COME UP AGAINST THIS GUY, I LOSE?!
PRIVACY
6/11
2013
DARKOW
COLUMBIA DAILY TRIBUNE
CAGLECARTOONS.COM

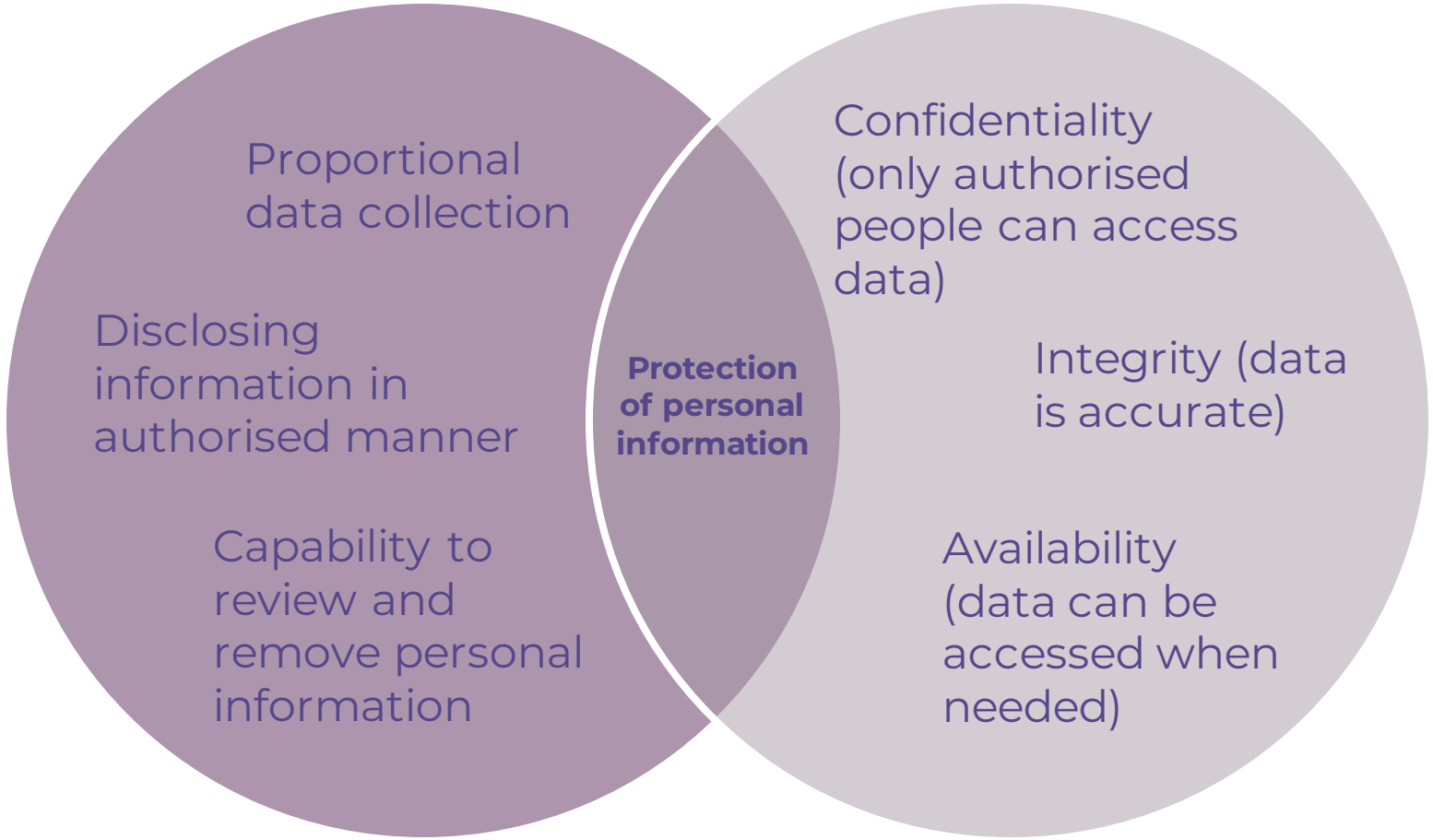
**“Security is freedom from, or resilience against, potential harm (or other unwanted coercive change) caused by others.”**

- Wikipedia

**“Privacy is the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively.”**

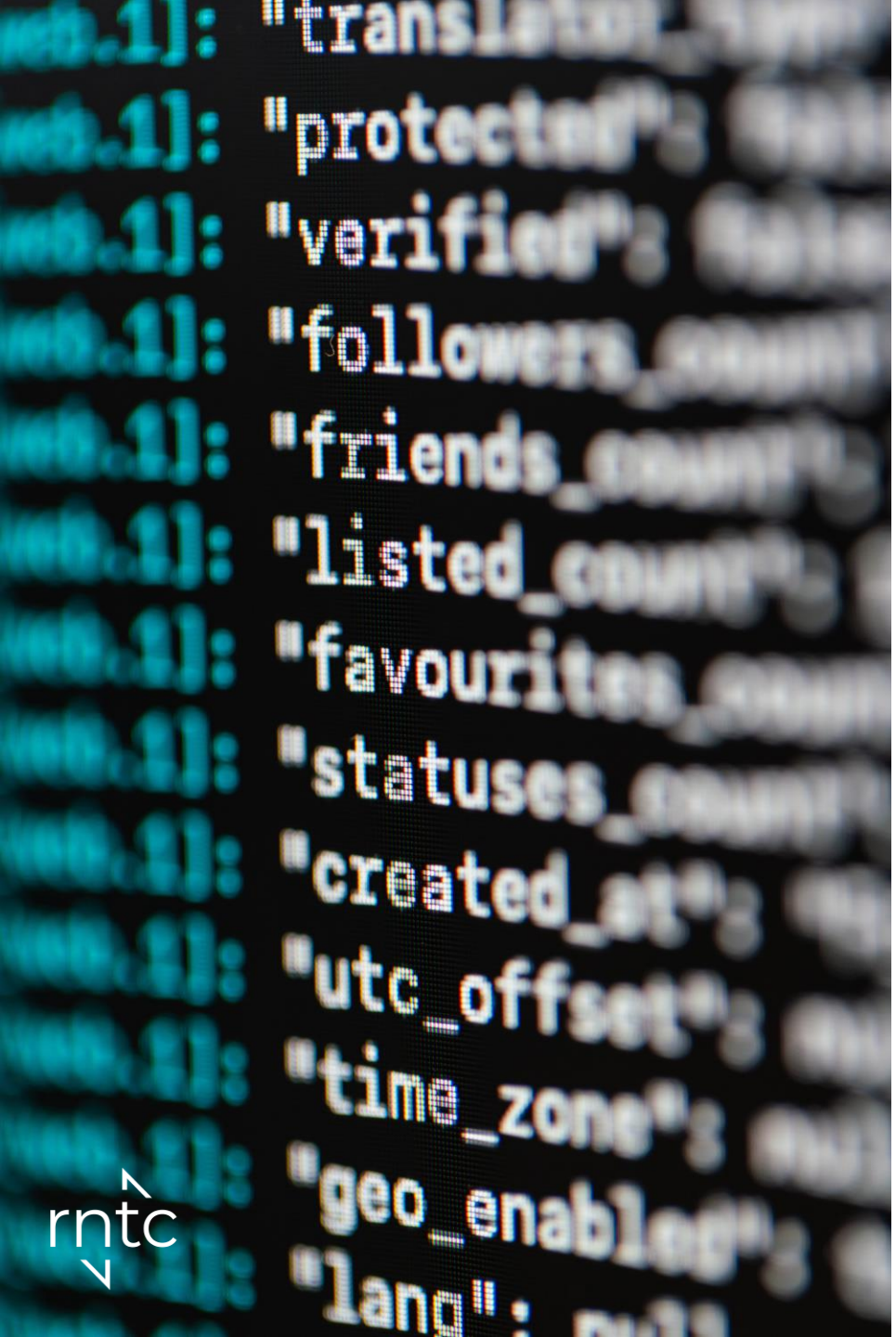
- Wikipedia

# DATA PRIVACY vs. DATA SECURITY



# Introduction

- What you need / Etiquette
- Discussion of OLA Exercise
- Our Approach
- Privacy and Security
- Principles




# Information security Principles

- Prepare to be hacked
- Humans are the weakest link
- Choose security by design
- If you can't protect it, don't collect it!

# QUESTIONS

# COFFEE BREAK!

# TRAVEL SECURITY

rntc

# Travel Security

Travel Plan Exercise

Key Issues and Solutions

#1 Device confiscation

#2 Social engineering

#3 Hidden cameras

#4 Accommodation

#5 Working in public spaces

# Travel Plan Exercise

**Your team has been invited to the COP27 in Egypt. You have been tasked with developing a travel plan which needs to be reviewed by your manager. You have been warned that there is a high risk of government surveillance.**

For the plan, you need to establish:
- Which devices you will take with you to event
- Steps to protect any sensitive data on devices you are taking.
- Communication protocol (How often you will communicate with HQ, through which channels, whether there will be public communication)
- Accommodation arrangements
- Communication protocols with the media

In groups, solve the questions and then share in a plenary.

Each group has 15 minutes to prepare for the event and then 5 minutes to present their plan. We will then discuss some issues which you have or may not have identified in your plans.

# Travel Security

Case Study

Key Issues and Solutions

#1 Device confiscation

#2 Social engineering

#3 Hidden cameras

#4 Accommodation

#5 Working in public spaces

## Travel issues to be aware of

# #1 Device Confiscation

In many countries, there are laws which can be used to force you to hand over encryption passwords. Some countries which will not hesitate to simply take your phone and keep It. Once they have it, there are various data extraction and forensic technologies they can use to retrieve and analyse data from your phone and laptops. Even if your devices are returned, you can never be sure that spyware was not installed on them.


rntc

# How to plan for device confiscation

- Evaluate risk of device confiscation before travel.
- Have a data transfer strategy for sensitive information you or your partners need while traveling. You can use some of the following
  - Hard-drives or small USBs which are easier to hide ( but remember that some authorities will not hesitate to strip search you if they think you could be hiding something)
  - File transfer to partners prior to travel
  - Use of cloud services with
- Make sure Full-disk encryption is enabled.
  - Use file-level encryption for added level of protection for most sensitive information (Veracrypt is a good encryption software option)
- if you are comfortable sharing location data enable Find my iPhone/device so that you can remote wipe
- Consider setting up auto-wipe on phone
- Use a pin number on sim card
- Use burner laptops and phones if travelling to countries with high probability of device confiscation and spyware use.(n.b. be aware of some of limitations of using burner phones)

rntc

# “DON’T COLLECT WHAT YOU CAN’T PROTECT”

*Because sometimes less is more*

rntc

## Travel issues to be aware of

# #2 Social Engineering

Social engineering is the deliberate use of trust-generating psychological techniques to convince targets do something the 'engineer' wants. Social engineers will gather as much information as possible on you und create a perfect scenario to get the information they want from you. Beware of event organisers, journalists and friendly new acquaintances!

**Tinder was really popular at Davos this year — here's what it was like to use it**

Lara O'Reilly Jan 23, 2016, 11:52 AM

THOMSON REUTERS

**I Spy? COP27 delegates wary of Egyptian surveillance app**

# Countering social engineering

- "Check your trust" when speaking with a stranger. Too good to be true might just be that.
- Sanitize your public profile and make sure you are not inadvertently sharing information about yourself via apps.
- Prepare communication protocols for speaking to press
  - who is going to speak,
  - to whom,
  - what are key messages
- Be wary about anything you receive which involves connecting it in some way to your devices.
  - USB
  - Applications
  - Chargers
  - QR codes
- Find ways to share examples of social engineering attacks against NGOs while travelling so that you and colleagues can learn to recognise patterns in methods uses by adversaries.

# “HUMANS ARE THE WEAKEST LINK”

*So design accordingly*

rntc

Travel issues to be aware of

# #3 Hidden Cameras and tracking devices

There are a multitude of mini cameras, microphones and tracking devices  which can be placed in our environments  when we are travelling.  The recordings can then be used maliciously.

**“11% of the survey respondents located cameras in their short-term rentals [Airbnb]"**

- Financial services company IPX1031


rntc

# Countering hidden cameras

- Do room sweep to see If anything looks 'off'
- Pay particular attention to common locations. Household items such as phones, tv, lamps chargers, mirrors and sensitive areas such as around bed or bathroom
- Cover peep holes if there is one
- If you  find camera/ camera do not try to touch or remove it (particularly if it is installed in smoke detector). Cover with tape and contact authorities / manager.
- Possible camera detection equipment/tools
  - Wireless network checker (app)
  - Infrared cameras
  - Wireless Radio detector
- Change room last minute if you think secret recording is very likely.
- 'Behave' and adapt your behavior strategically.
- You can use this article for more information about spotting hidden cameras/

Travel issues to be aware of

# #4 Accommodation

We book accommodation for travel and trust the hotels to take care of our security. However, the security at many hotels simply does not exist. Take for example the fact that many hotels do not change the master passwords of their hotel safes or allow any member of staff to use their master keys.


rntc

# How to deal with poor hotel security

- Spend time doing research about hotel accommodation before trip.

See if you can find any complaints about the hotel online.

- If you know hotel layout, book a room that is not easily accessible by public.
- Do not open doors for people / or let them in elevator if you are not 100% sure they are guests.
- Keep devices and valuables on you as much as possible.
- In certain countries, 'informal' accommodation arrangements can be more secure than

booking rooms at famous hotel companies.

- Use portable door locks to secure hotel door
- Use strategies to limit entrance to room.
    - Place do not disturb on door or sign saying that you are quarantined
    - Turn on TV to simulate presence in room
- Set up intrusion detection systems.
    - Place piece of paper between door and door frame.
    - Using earphones on belonging and taking before/after shots.
    - Use Haven app on spare Android device.
- Do not use hotel safes unless you are sure of hotel security protocols and absolutely

need to leave something in room. A portable travel safe
can also help you avoid the hotel safe.

Travel issues to be aware of

# #5 Working in public spaces

Working in coworking spaces or cafes has become more and more common. However, there are many threats linked to public spaces. Our devices are more vulnerable in public spaces, and we rely on Wi-Fi networks set up by strangers to connect to the internet.

rntc

# Working in public spaces

- Be careful about your presentation.
  - Dress to fit it.
  - Show situational awareness
  - Avoid showing people where you are storing valuables.
- Be wary about what CCTV cameras could be capturing.
- Avoid typing in passwords when there are people around.
- Use privacy screen
- Check certificate fingerprints of important Use a VPN on device and/or use VPN on travel router
- Avoid using public USB ports (if you must, use data blockers )
- Have a bag packing strategy
  - Keep work/life essential items in bag which you never leave.
  - Anything non-essential can stay in bag which you are ready to 'sacrifice'
- Carry bait wallet with some cash but nothing which identifies you.
- Make sure your device is not broadcasting too much information
  - Make sure you are using most updated OS on laptop/phone.
  - Turn off Bluetooth/ Wi-Fi connections when not using them
  - Disable Wi-Fi autojoin
  - For more detailed information about the how your devices broadcast information which can be used to track you, see this article.

# COFFEE BREAK!

# Protecting your Partners

Find the Information bombs Exercise

Questions to Ask Yourself When Collaborating With Partners

Account Management Deep Dive

Phishing

# “Choose security by design”

*Analyse, plan, monitor and adapt*

rntc

**Partners are vulnerable when their perceived association with us can harm their ability to operate.**

**Therefore, we need to evaluate the harm which information from the past, present or future could cause.**

rntc

**And take steps to prevent any leaks, breaches or media coverage which could harm your partners.**

# Exercise “Find the information bombs”

In your assigned group, try and identify types of information which could harm your partners if disclosed to unauthorised parties ("information bombs")

Rate them in terms of harm to partners and likelihood of occurrence. You can place the information bombs in a table like the one below.

You have 10 minutes to prepare and 5 minutes to present your conclusions to the rest of the group,.

| Nbr. | Information bomb | Harm to partners (1-5) | Likelihood (1-5) |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

# Some potential 'information bombs" you should have taken into consideration

| Past Information Bombs | Present Information Bombs | Future Information Bombs |
| --- | --- | --- |
| • Prior historic activity<br>• Online footprint<br>• Colleagues who quit / were fired | • Contracts<br>• Personal data<br>• Project communication<br>• Event organisation | • Evolving socio-political context<br>• Business development /new relationships<br>• Press coverage<br>• Colleagues on verge of burnout |

rntc

# Protecting Partners

Find the Information bombs Exercise

Questions to Ask Yourself When Collaborating With Partners

Account Management Deep Dive

Phishing

Cybersecurity and **reputation management** go hand in hand.

The following slides suggests some questions NGOs need to ask themselves to properly manage their reputation and its impact on partners.

# Collaborating with partners

# Questions to ask yourself (1)

- Do I understand the socio-political context well enough to take informed decisions and 'Do no harm'?
  - What is perception of your organisation in country you intend to work in or are working in?
  - What are social norms of working with foreigners and how might those impact project?
  - Are local socio-political trends likely to worsen/ improve perception of my organisation?
  - What is likelihood of disinformation being problem?
  - Does the involvement of my organisation produce more benefits than disadvantages.

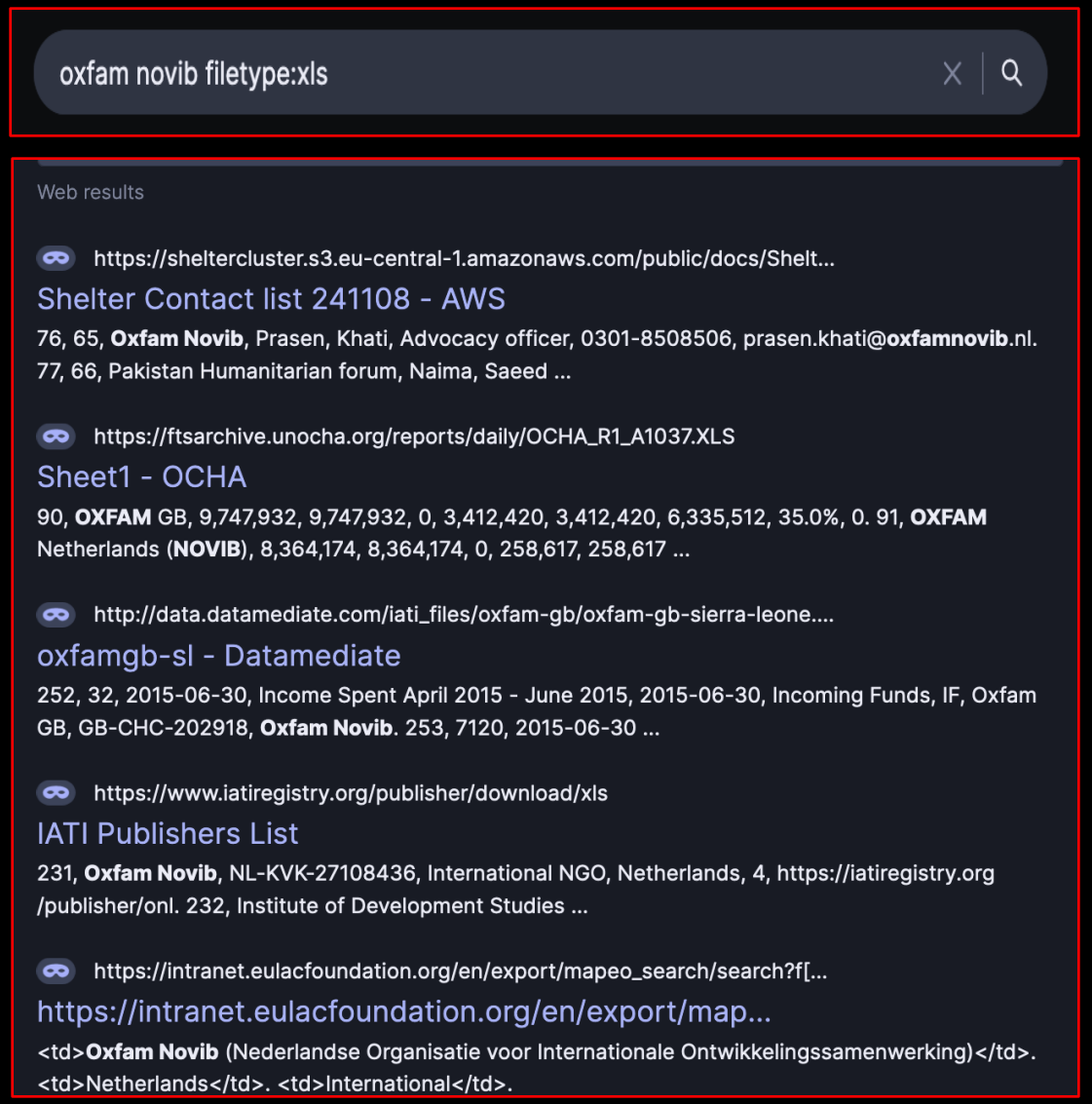
- Note from trainer: NGOs tend to rely on their partners for the information about context but it always important to nurture relationships with local actors who are not part of aa project so that they can provide an external independent viewpoint.

  Sadly, many NGOs do not engage with these questions in a serious way simply because there is so much pressure to get project going. This leads to problem where projects have to be significantly modified as the project hits the wall of reality in order to deal with security threats.

rntc

RNW media

As the screenshot below shows, It was possible to do a quick search to find old Oxfram Novib budgets. Such pieces of information can appear innocus but they can easily be manipulated by actors who can recast the informaiton in a different light. Before starting an important project, one of the first actions you should take is a reverse due diligence exerciese t remove and / or mask information which could negatively impact your partners.



# Collaborating with Partners

# Questions to ask yourself (2)

- How can I secure data which I collect or generate over the course of our collaboration > *see upcoming account management deep dive*.
  - Note from trainer:  think creatively  how can you reduce or decentralise data collection for travel and/or events. (Remember "Don't collect what you cannot protect" principle)
- How is our communication architecture designed?*> see upcoming account management deep dive*.

# Protecting Partners

Find the Information bombs Exercise

Questions to Ask Yourself When Collaborating With Partners

Account Management Deep Dive

Phishing

rntc

- **The first rule of account management is to use a password manager.**
- Use it to create and memorise a few good master passwords for your:
    - Login password
    - Full disk encryption password
    - Password manager
- Generate the rest of your passwords using password manger
- Use the password manager to record important account information
    - Aliases
    - Answers to security questions.
    - Old passwords
    - Contact information for contacts
- Have a password back up strategy.
- Avoid state-less password managers.
- Go slowly when you start using a password manager. Start changing passwords in small manageable batches so you can get used to software and avoid errors.

rntc

# Account Management Deep Dive

**Tips (1): You need a password manager**

RNW media

# Password manager recommendations.


Bitwarden is a great open-source cloud password managers with lots of features at the free tier. For people dealing with a more extreme threat model, then KeepassXC is a good local open-source option.

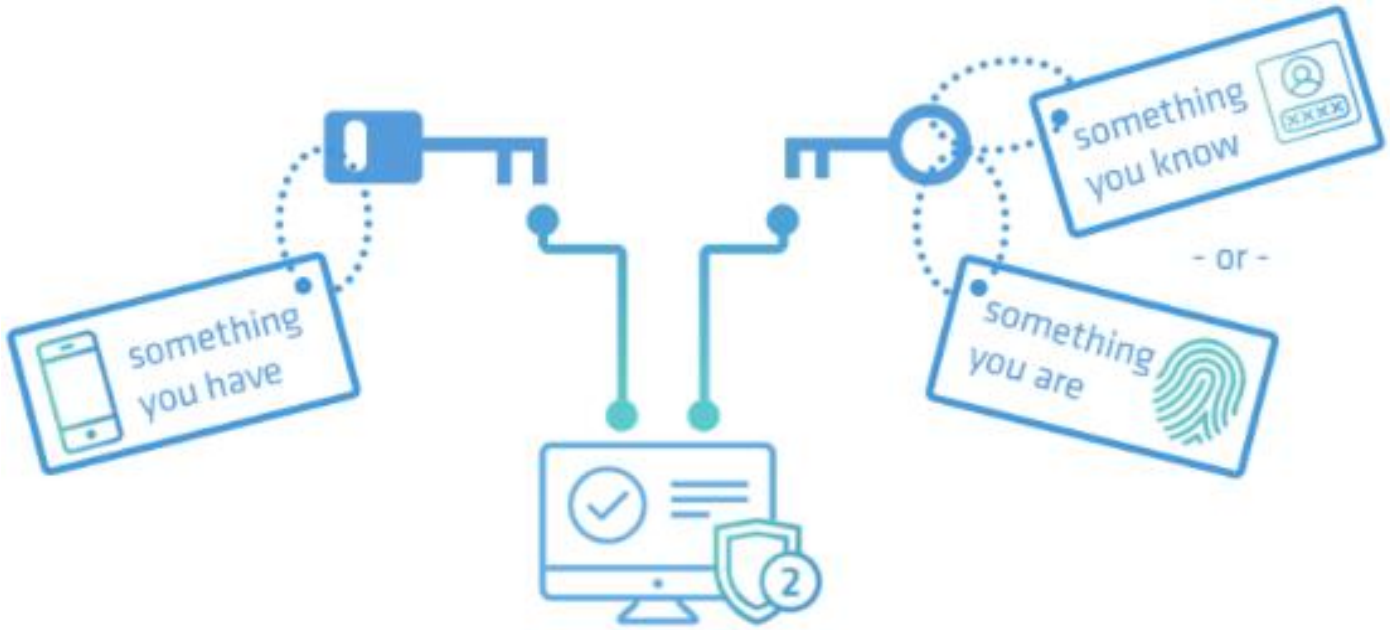
*You could use both: use Bitwarden as your everyday password manager and backup those passwords on a separate hard drive or USB using KeepassXC.*

- **The second rule of account management is that all accounts should be protected by two-factor authentication**
  - Make a list of some of your most important accounts and check whether you have two-factor authentication enabled. Slowly start adding your factor of choice to these accounts and when you are done, repeat the exercise for another set of accounts.
  - If possible, choose something better than SMS two-factor Authentication. but SMS is better than nothing! (For more information see https://www.pcmag.com/news/sms-based-multi-factor-authentication-what-could-go-wrong-plenty)

# Account Management Deep Dive

**Tips (2): You need to start using Two-factor Authentication**

# Two-factor Authentication (2FA)




There are three authentication factors. Two-factor authentication requires the use of two different factors to be truly in place.

# Protecting Partners

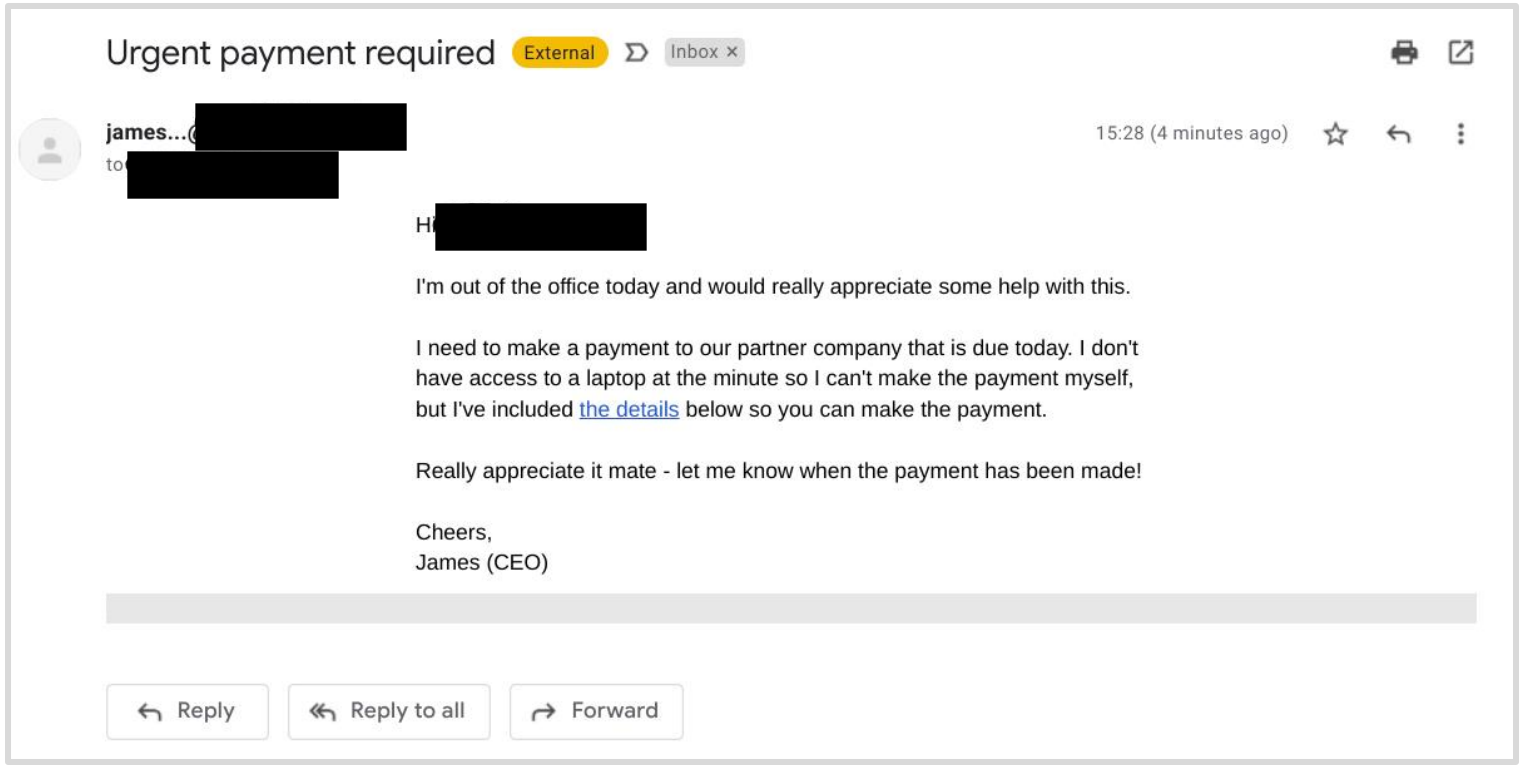
Find the Information bombs Exercise

Questions to Ask Yourself When Collaborating With Partners

Account Management Deep Dive

Phishing

# Phishing




On a scale of 1-5, how confident are you in your abilities to spot when you are being phished?

rntc

# Test your skills!

## Can you spot when you're being phished?

Identifying phishing can be harder than you think. Phishing is an attempt to trick you into giving up your personal information by pretending to be someone you know. Can you tell what's fake?

TAKE THE QUIZ

Quiz: https://phishingquiz.withgoogle.com/

# Some solutions for dealing with Phishing

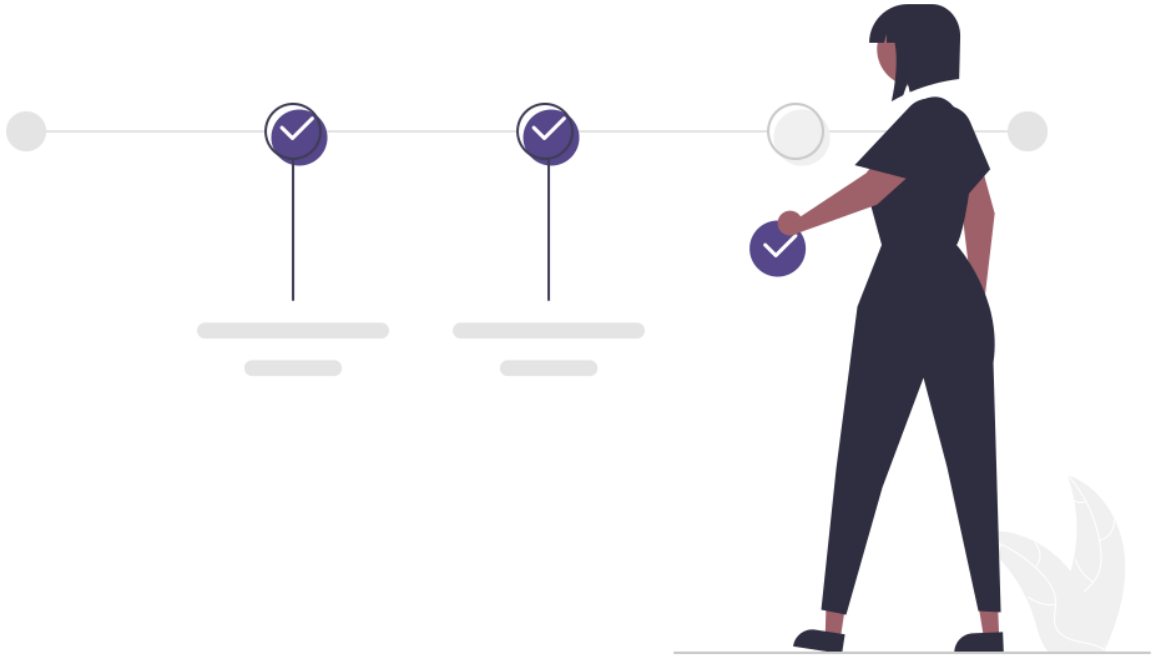
- When visiting a website:
  - Study website URL carefully for suspicious domains, strange spellings etc.. (Beware of Browser in the Browser attacks which use popup pages to generate seemingly legitimate URLs)
  - You should avoid sharing any information with sites that do not use HTTPS (i.e. the padlock icon) but just because a site has HTTPS, does not mean you can automatically trust it.
  - Always pause to think before you click and hover over hyperlinks to inspect URL
- If you start having suspicions about the website you are on.
  - Use URL / file scanners like Virus Total
  - Inspect SSL certificates of website to check for suspicious information.
  - Compare fingerprints of certificate using GRC
- If you are downloading security software:
  - Check integrity of downloads (see OLA resource)
  - Verify authenticity of downloads via signatures (see OLA resources)
- If you have doubts about an email you have received, scan the email header.
- To 'prepare to be hacked':
  - Use cloud services to upload suspicious documents.
  - Use the password manager auto-fill functionality to detect and avoid phishing attacks
  - Configure browser to block malicious downloads.
  - Configure browser to ask how to handle downloads once you click to introduce a pause **after** you click!
  - Use two-factor authentication on everything!
  - Make sure software of all your devices is updated (laptop, phone, smart devices, router etc...)

# Consider hardware authentication devices


For [added security](#) against phishing, use hardware authentication devices such as Yubikey.

# LUNCH

# NEXT STEPS



rntc

# “Choose security by design”

*So analyse, plan and monitor*

# Next Steps

Principles

Useful Resources

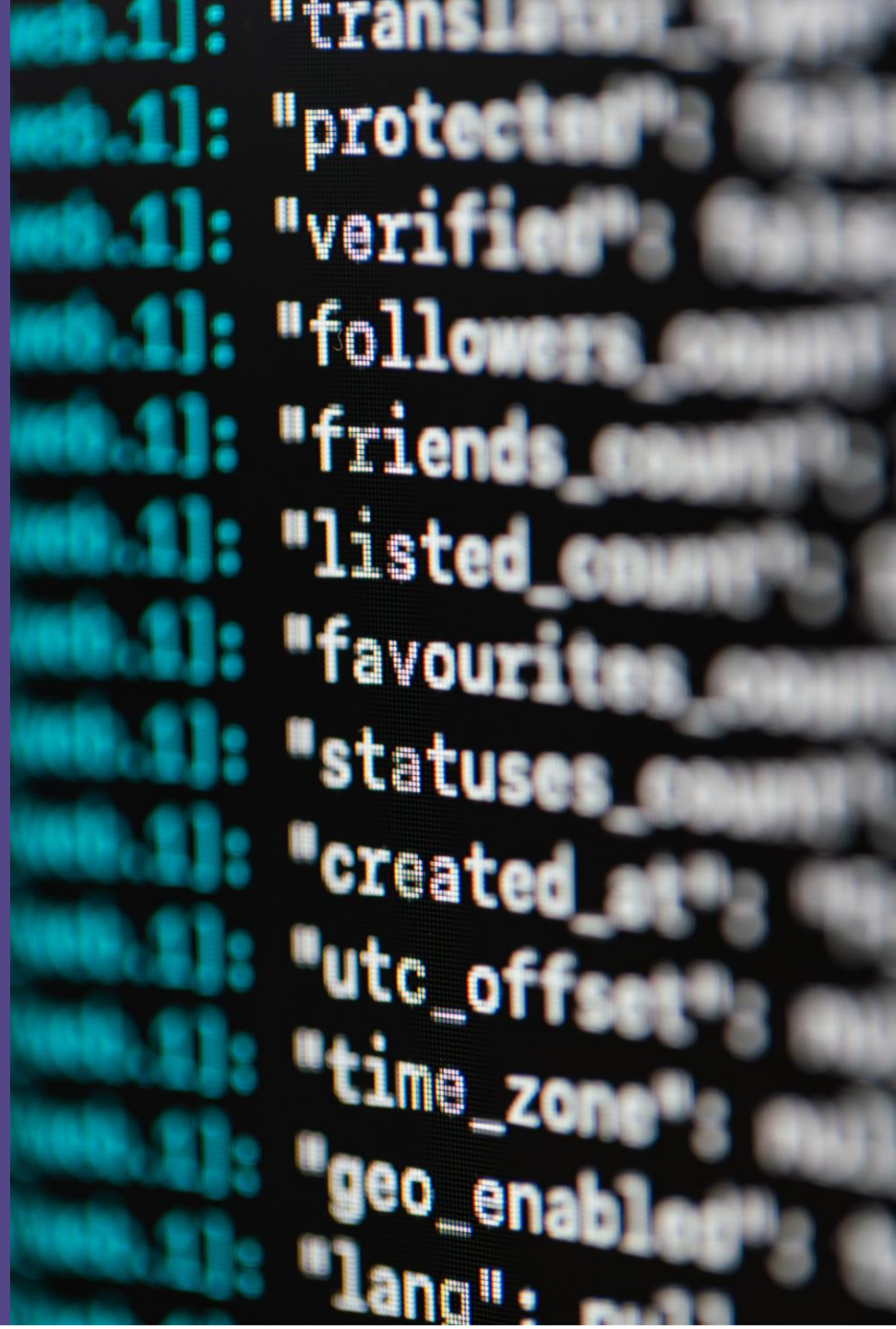
Information Security Planning

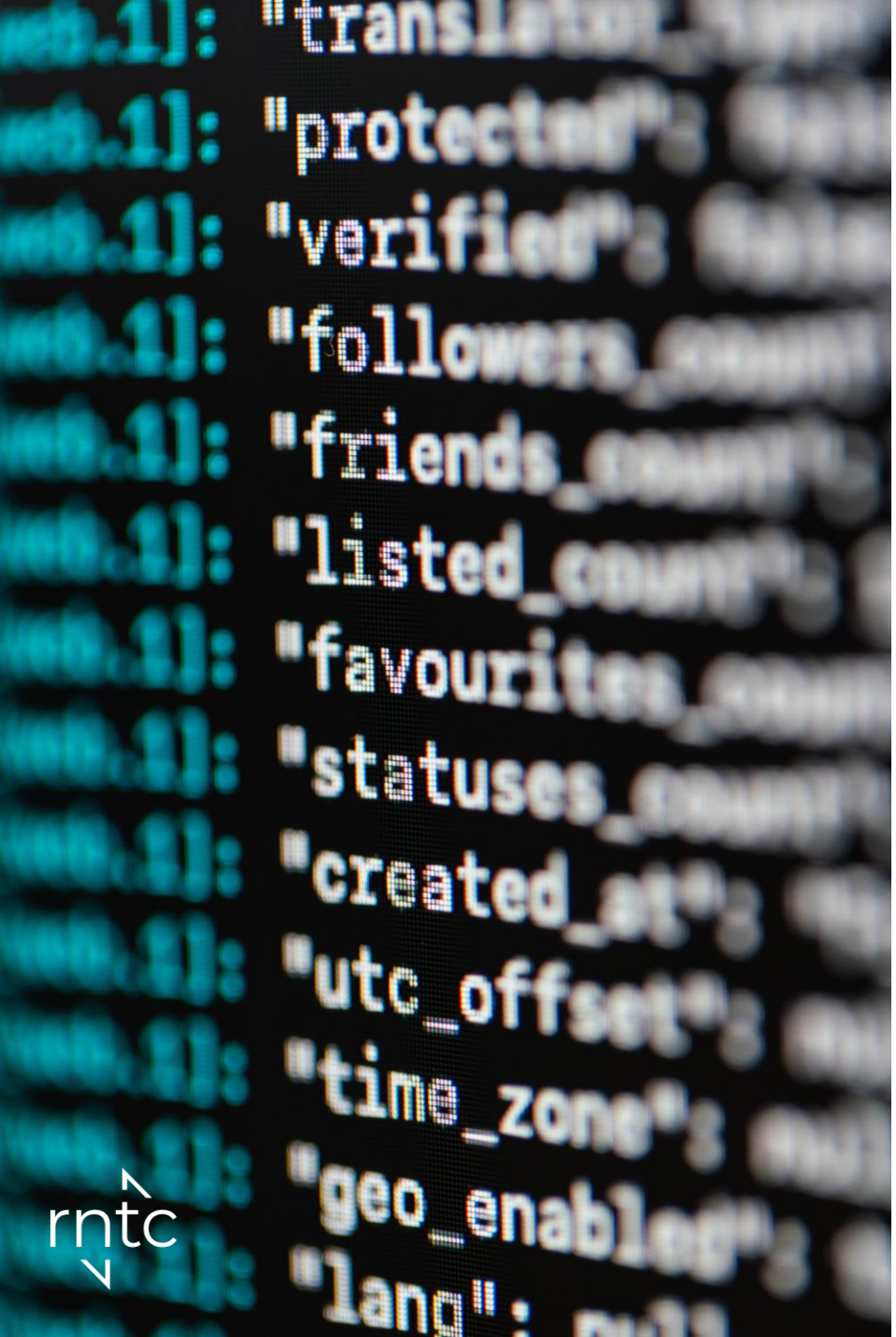
Perception Survey

rntc

# Information security Principles

## What cybersecurity principles did this training highlight?






# Information security Principles

- Prepare to be hacked
- Humans are the weakest link
- Choose privacy by design
- If you can't protect it, don't collect it!

- **And…**

# Digital security is a journey..... so enjoy the ride.

# Next Steps

Principles

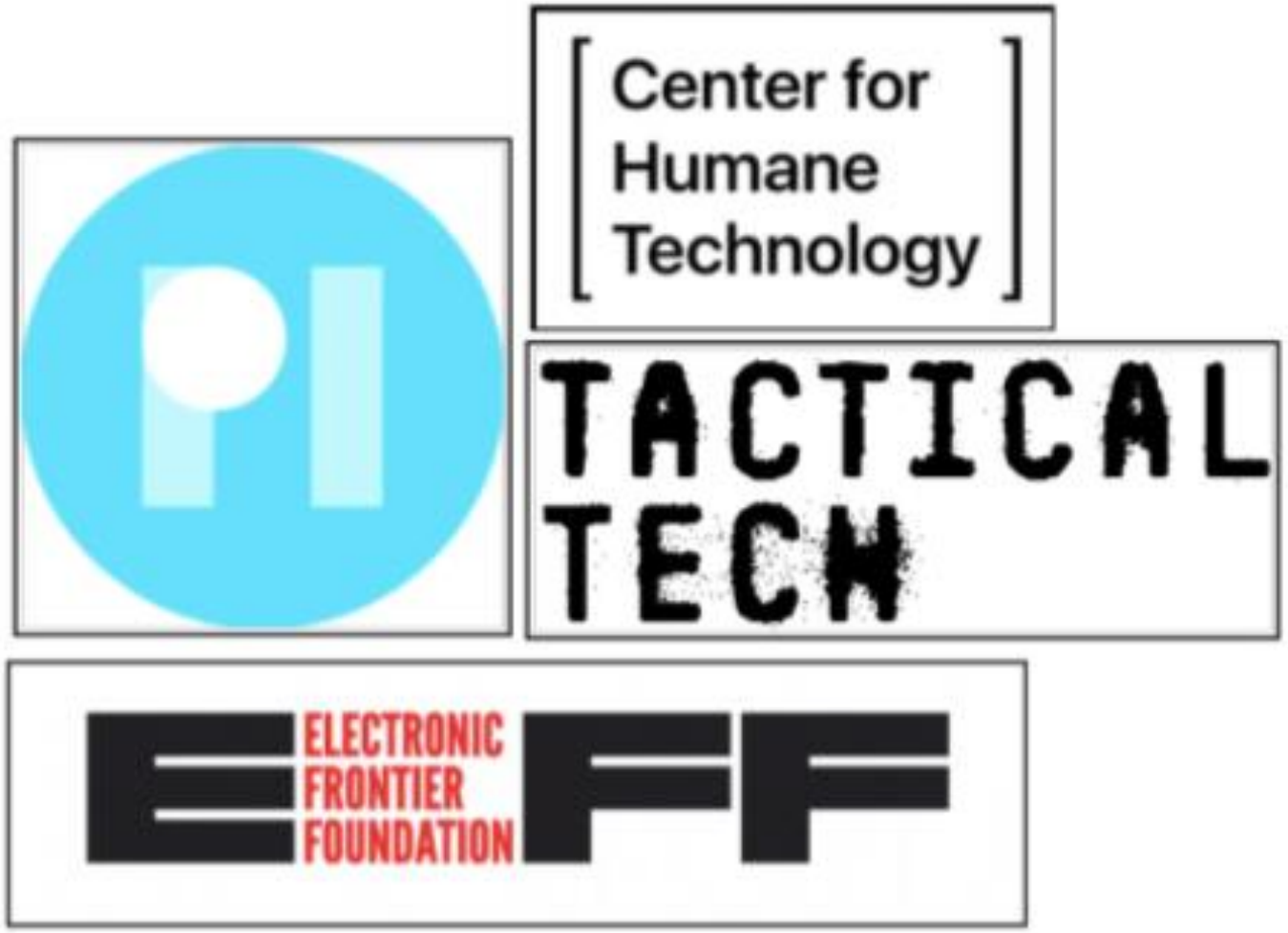
Useful Resources

Information Security Planning

Perception Survey

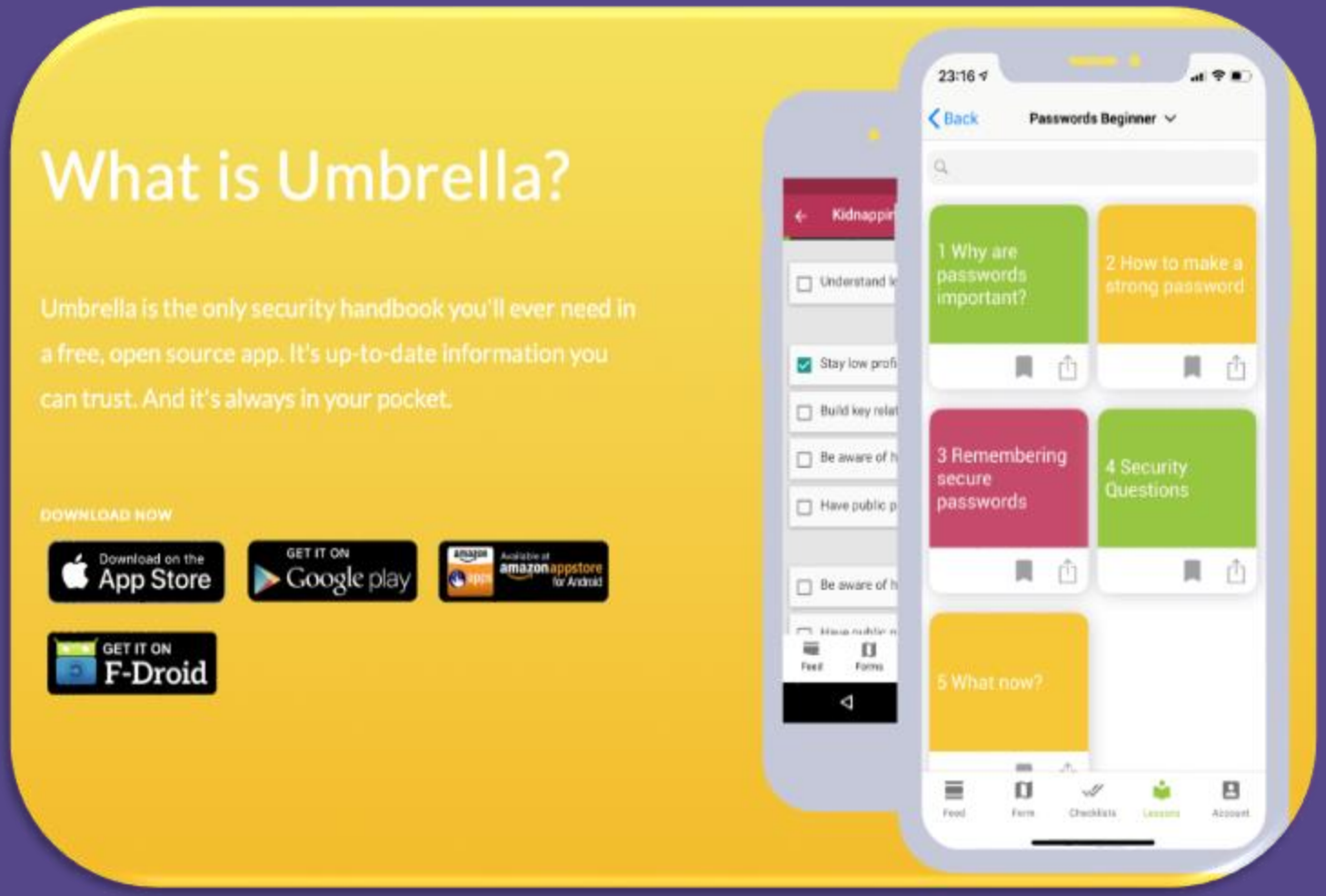
rntc

# Useful Resources




Digital Rights organisations

# Useful Resources




Link: https://secfirst.org/umbrella/

**“The best form of defense is attack.”**

- Carl von Clausewitz

# Next Steps

Principles

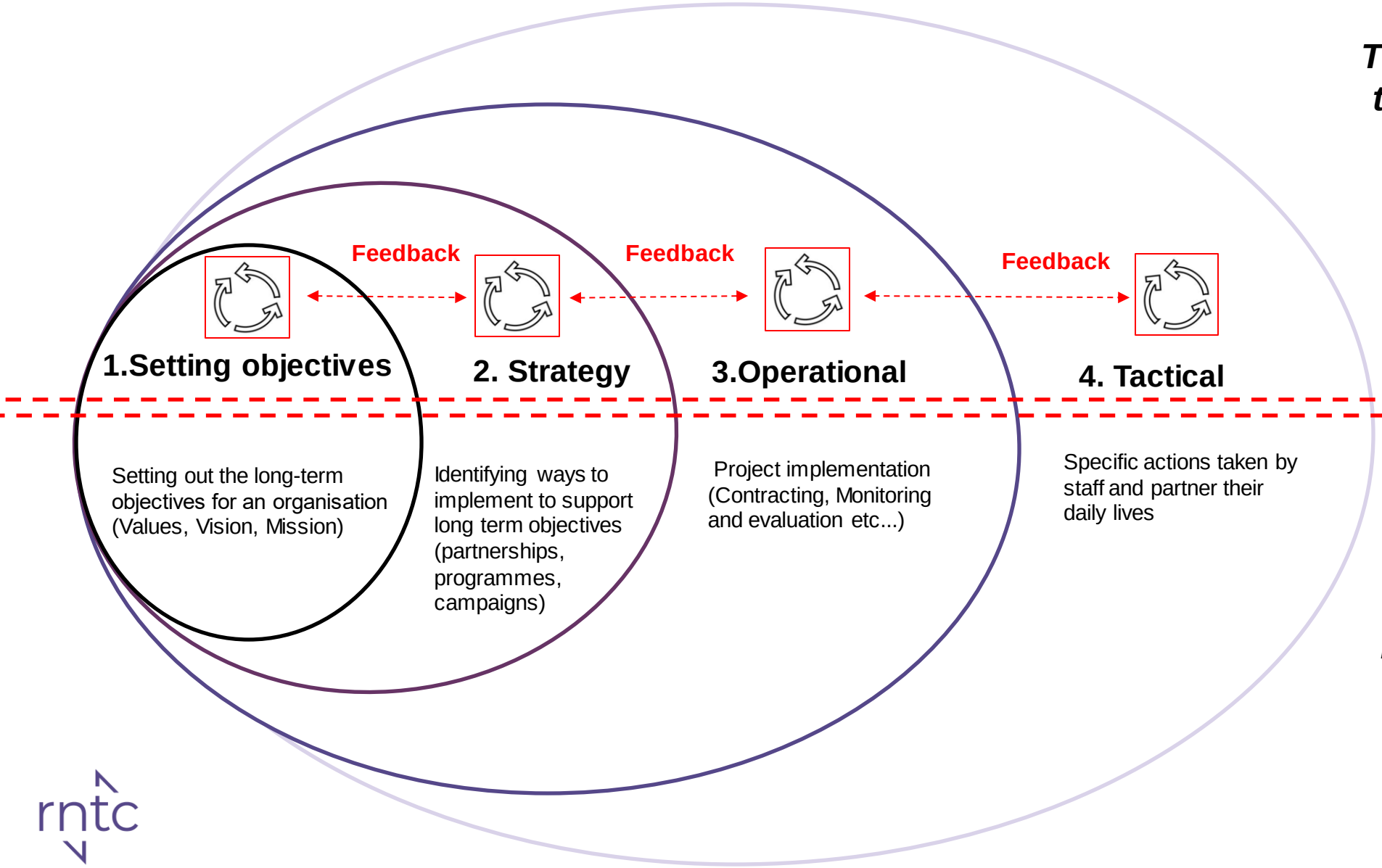
Useful Resources

Information Security Planning

Perception Survey

rntc

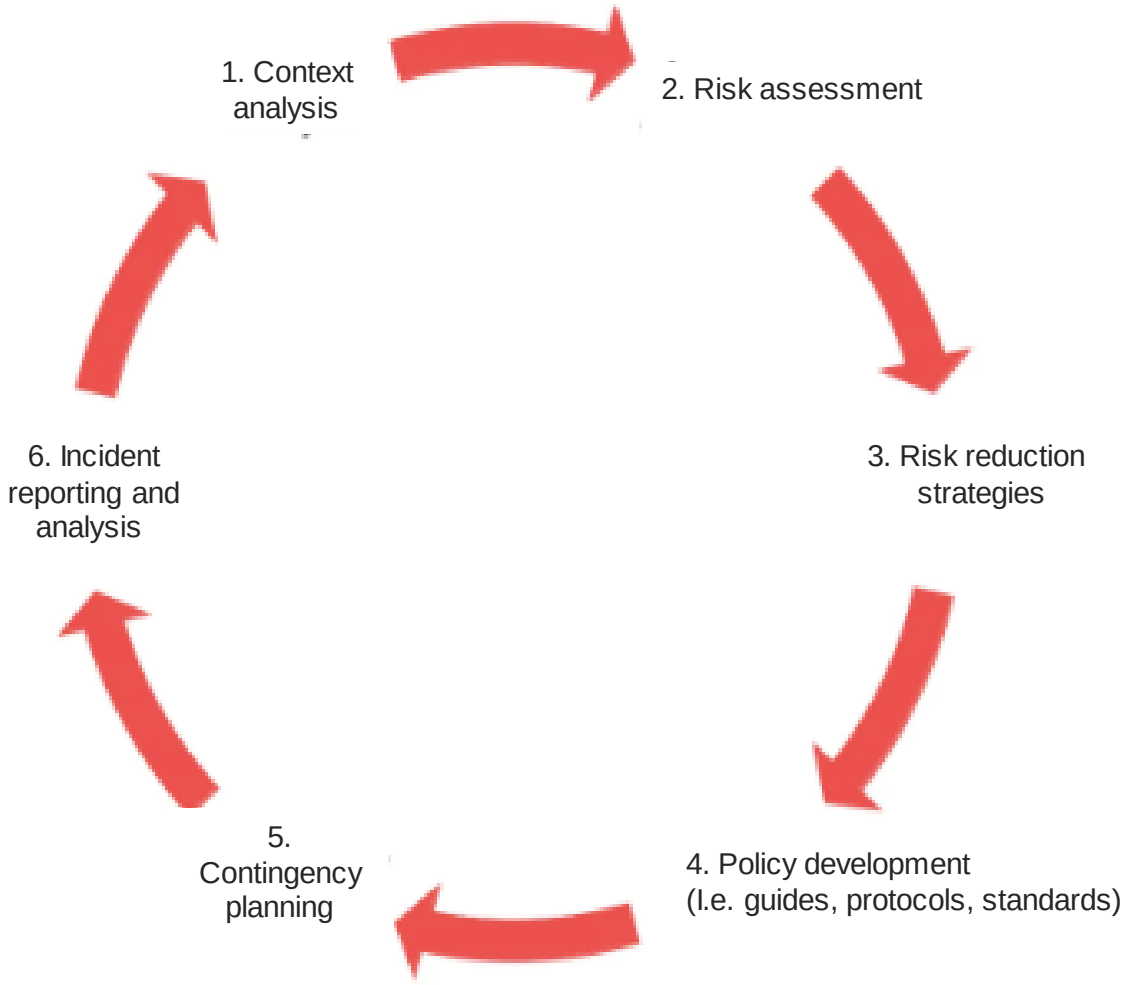
# Informational security planning at all layers of the organisation




***The security planning has to take place each level of the onion otherwise the differents parts of an organisation do not work coherently together to achieve strategic impact.***

***If there is regular feedback across each organisation layer about security threat / opportunity environment then the different layers are aligned, an organisation can generate strategic impact***

# The Information Security Planning Cycle



# Next Steps

Principles

Useful Resources

Information Security Planning

Perception Survey

rntc


# Perception Survey

Go to **menti.com**, enter the code [X] and answer the perception statements.

# Thank you!

rntc media training centre

مسارنا masarouna

RNW media

**The account management process discussed in session 3 should set out the different ways you will communicate with partners depending on nature of information you are exchanging and conditions in the partner's country.**

**This should normally take place in the pre-project security planning cycle. Here are three points which need to be at the core of communication choices.**

**1. Your choice of communication tools needs to be adapted to *local context*.**

- Some tools are red flags if the partner is forced to hand over or unlock phone. In Egypt for example, being caught with Signal in your phone at a checkpoint can be enough to warrant detention. In such cases, you need to make sure there are policies to ensure partners strive communicate on a devices which stays at home or use browser-based communication tools.
- Some tools will be blocked by the governments of your partner's country. You should have backup communication tools in case your primary choice goes down.
- Some communication tools may not work very well if internet speeds are not reliable.

# BONUS SLIDES

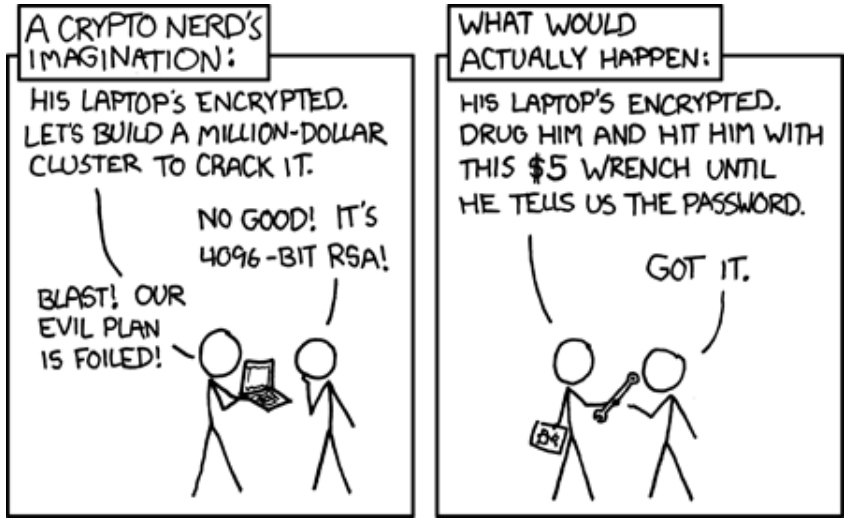
## Communicating with partners (1)

# BONUS SLIDES

## Communicating with partners (2)

- Not all partners, even if they are in the same country, are dealing with the same threat model. You should therefore spend time understanding the different threat models and have different communication protocols for each partner to address different threats.. Here are some measures you might use with high-risk partners:
  - Using end-to-end encryption with Perfect Forward Secrecy at all times.
  - Being metadata sensitive by. not choosing tools which generate sensitive metadata (location, IP address, contacts, call logs etc..)
  - Remove any non-essential application/ software from devices.
  - Using auto-delete or temporary messages functionality.
  - Verifying key fingerprints / safety numbers of out band when you start communicating.
  - Using linux distributions on devices to minimise risk of backdoors.
  - Using virtualisation software to create virtual machines (see Virtualbox)
  - Using 'amnesic' operating systems such as Tails OS
  - Using hidden volumes using Veracrypt or 'accountless' tools couple with or TOR such as: Jitsi or Onionshare.
  - Create ways in which people can anonymously send you information without you already being in contact with them..
    - https://securedrop.org,
    - Globaleaks,
    - Onionshare

- In high-risk cases, you should encourage partners not to store anything sensitive on laptop as this will expose them to forensic analysis of adversary.
  - Using virtual machines, Tails OS and Veracrypt can certainly reduce risk of exposing sensitive data but they will not work when adversary is highly skilled, and determined. As mentioned during the training, learning when not to generate or collect data which cannot be protected and leveraging radically transparency will work better in many the situations where the adversary's technical resources are unlimited or brute force can be used to extract passwords.




# BONUS SLIDES

## Communicating with partners (3)

**2. Your choice of communication tools needs to be adapted to *human psychology and realistic behaviour change*:**

- In an ideal world, you will be able to choose communication tools which already exist. You are more likely to find resistance from partners if they have to install a completely new tool and if you are their only contact who uses that tool, they might not be very motivated to use the tool.
- Harden as much as possible security settings of the communication tools you already use before adopting a new tools. For example, many people use WhatsApp and there are multiple changes to settings which can upgrade security of using WhatsApp https://freedom.press/training/upgrading-whatsapp-security/.
- Focus on user friendly experience which will not create a lot of friction unless circumstances really justify tightening of security measures. For example, for many people Signal is great WhatsApp alternative simply because they work in very similar ways. By choosing path of least friction, you will increase likelihood of the new communication tool being adopted. https://www.wired.co.uk/article/signal-vs-whatsapp.
- If possible, use communication tools which already If there is a need to protect sensitive information, then, where possible design a project communication architecture which always uses end to end encryption to avoid people making mistakes. This is why it can be advisable in some to move email communication to one encrypted provider such as ProtonMail or Tutanota.
- In certain places, you cannot expect partners to pay for communication tools, so if you want them adopt a new communication tool then you need to make sure the free version of the tool you are using has sufficient features.
- Bear in mind, that in some cases, adopting a stronger security posture can justify foregoing these recommendations.

# BONUS SLIDES

## Communicating with partners (5)

**3. You should plan for worst case scenario. This helps you be prepared and not be on back foot when crisis occurs. Here are some elements of contingency planning you should consider:**

- Compartmentalising accounts (I.e. unique emails and passwords) using aliases and email forwarding services (see Simplelogin or Anonaddy).
- Preparing an emergency plan for when your partner:
    - Loses access to accounts
    - Does not communicate with you for prolonged period unexpectedly (radio silence).
    - Communicates with you but while held under duress.
- Review the digital tools you are currently and those you are thinking using.
- Ask yourself – can I trust the companies behind them? You can use the privacytools.io tool selection criteria to answer this question.
    - Spend some time doing research about the companies and how they handled privacy and security of their clients in past. If you feel that your trust is misplaced and thatt the impact on a project or partners would be too significant if a breach were to occur then it is time to make a change.
    - There are no perfect tools. In most countries, a government can force for example an email provider to log IP addresses linked to a particular account. Hostile governments can recruit spies from the company's staff. The main red flags you need to identify are those which indicate a company has a structural problem (I.e. privacy invasion is part of business model, company leadership heavily linked to leadership of hostile government, poor security practices).

# BONUS SLIDES

## Communicating with partners (6)

# BONUS SLIDES

## Where does all of this fit within the security plan? (7)

As you know, I love security plans ;).

Decisions about how to protect information exchanged between you and your partners should take place during the first three steps of the security planning cycle (see slide 72)

The following table shows the result from an information asset mapping exercise (part of step 2 risk assessment) which identifies the degree to which information (or data) which will result from a collaboration with the partner in question is exposed to threats. This kind of analysis should be carrying out before considering a collaboration with a partner but during projects is better than nothing.

| Partner Information asset | Risk score | Impact score | Threat Score (Risk + Impact) |
|---|---|---|---|
| Social media posts | 4 | 5 | 9 |
| Email correspondence | 4 | 3 | 7 |
| etc.. | 3 | 5 | 8 |

# BONUS SLIDES

## Where does all of this fit within the security plan? (7)

Once you have completed the context analysis and  risk assessment) of your collaboration with partner, you should understand the threat exposure of information assets you want to protect, and you can begin identifying risk reduction measures.

The table below provides an example of how you might expand on the risk assessment table provided in previous slide by adding a new column for your chosen risk reduction measures.

| Information asset | Threat Score (Risk + Impact) | Risk reduction |
|---|---|---|
| Email | 7 | Set up Two-factor Authentication on all accounts<br>Use encrypted email provider |
| Social media posts | 9 | No social media<br>Set up alerts for any potential mentions about our collaboration |
| etc.. | .... | ..... |

# BONUS SLIDES

## Where does all of this fit within the security plan? (8)

Once you have completed the previous steps, you can move on to step 4 of the security planning cycle: policy development. At this stage, you need to integrate your analysis for steps 1,2 and 3 to create communication protocols and guidelines.

Ideally, you would develop various protocols which are tailored to the assessed threat level a partner is facing and the assessed potential for behaviour change of your partner. The table below provides of example of how different partners could be assigned to different protocols depending on where they fall on the matrix.

| | Low potential for behaviour change | Medium potential for behaviour change | High potential for behaviour change |
|---|---|---|---|
| Low threat level | Apply protocol 1 | Apply protocol 1 | Apply protocol 2 |
| Medium threat level | Apply protocol 2 | Apply protocol 2 | Apply protocol 3 |
| High threat level | Apply protocol 2 | Apply protocol 3 | Apply protocol 3 |

# QUESTIONS