Money Trail
Digital safety & security
Welcome!
Training overview

Risk Assessment
- What to protect?
- Protect from what?
- How to protect?

Security Measures
- Information Safety
- Communication channels
- Standard Operating Procedures
- Security Measures

Security Tools
- Passwords & Encryption
- Operational & Mobile Security
- Analysing measures
Risk assessment

Time slot indication

..:.. h - ..:.. h
Training overview

**Risk Assessment**
- What to protect?
- Protect from what?
- How to protect?

**Security Measures**
- Information Safety
- Communication channels
- Standard Operating Procedures
- Security Measures

**Security Tools**
- Passwords & Encryption
- Operational & Mobile Security
- Analysing measures
Why carry out a risk assessment?
Why carry out a risk assessment?
Risk assessment training

The goal
To assess digital security on a personal and professional level

The method
Based on a case you will work together to understand possible dangers during an investigation
Welcome to Deltora Magazine

Roile River Delta Case
Life in Petronia
Your aim
Your team

• An experienced journalist
• A foreign journalist
• An ambitious newbie
• A consulting expert
• An activist
• The editor-in-chief
Investigative proposal
What to protect?
Example of Actor Network with possible adversaries/ capabilities

*Not representative for Petronia case
• Who is involved in the investigation?
• Which data and information is processed by actors as part of the investigation?
• What devices are being used?
• How sensitive is this data or information?
**Actors**: Who is involved in the investigation?

*Everybody that you work with and need to successfully conduct your investigation.*

**Assets**: Which data and information is processed by actors as part of the investigation; how sensitive is this data or information; what devices are you using?

*Everything that you work with and need to successfully conduct your investigation.*

**Activities**: How is this data and/or information obtained, communicated, processed, published, etc?

*All you journalistic or investigative workflows and processes*
Protect from what?
Example of Actor Network with possible adversaries/ capabilities

*Not representative for Petronia case

Private investigators: Observations

Face to Face

Cyber Criminals: Phishing

Email

Private investigators: Hacking

Face to Face

Cyber Criminals: Hacking

Executive B

Executive A

Executive A

Activist Group B

Activist A

Government Officials: Targeted surveillance

Chat

Private investigators: Wire tapping

Calls

Government Officials: Wiretapping

Text

Government Officials: Mass surveillance

Email

Messaging app
**Adversaries:**
People or organisations that have an interest to influence or stop your investigation.

**Capabilities:**
Activities your adversaries can undertake to uncover your investigation, its actors, assets and activities.

**Threats:**
Activities your adversaries can carry out to influence your investigation, its actors and activities.
Risk assessment
Call with executive

Texting with source
How to protect?
Present your protection plan!
Recap and feedback
Questions
Security measures

Part 1

Time slot indication

..... h - .... h
Training overview

Risk Assessment
- What to protect?
- Protect from what?
- How to protect?

Security Measures
- Information Safety
- Communication channels
- Standard Operating Procedures
- Security Measures

Security Tools
- Passwords & Encryption
- Operational & Mobile Security
- Analysing measures
Do you feel secure?
How does the internet work?
Security
Security
Privacy
Anonymity
What can you learn from a message?
So, I think you should take a look at these recent development, as I am pretty sure Mister Z and Miss Y are involved in some shady business.

Kind Regards,

Received: from [computername]
(sad231sdc.adsl.wanadoo.com [127.0.0.1])
(using TLSv1 with cipher AES128-SHA (128/128 bits)) (No client certificate requested)
What can metadata tell?
The experienced expert
What about your communication?
Assess your communication

Somebody sends you a public tweet offering sensitive information about a minister. He/she asks for your email address to continue communication.
Assess your communication

You want to discuss something sensitive with the foreign journalist in your team. He is not answering you on Whatsapp, so you pick up the phone.
Assess your communication

Practice with your team

Study your case
Your communication tools
Check the used tools
Standard Operating Procedures
Share your Standard Operating Procedures
Security checklist
Questions & feedback
Money Trail

Digital safety & security
Today’s programme

1. Security measures
2. OpSec plan
3. Passwords
4. Encryption
5. Tools

Q&A
Security Measures

Part 2

Time slot indication

..... h - ..... h
Training overview

Risk Assessment
- What to protect?
- Protect from what?
- How to protect?

Security Measures
- Information Safety
- Communication channels
- Standard Operating Procedures
- Security Measures

Security Tools
- Passwords & Encryption
- Operational & Mobile Security
- Analysing measures
Rebel radio
What’s the risk?
What's the risk?
S.O.P. II

1. Create a plan
2. Gather feedback
3. Adjust
Strategies

- Mitigating confiscation of assets
- Full disk encryption
- Account security and OTP
- Identity management
- VPNs/ obfuscation technologies
- Remote storage
- Compartmentalisation
Security tools

Time slot indication

\[ \ldots h - \ldots h \]
Training overview

Risk Assessment
- What to protect?
- Protect from what?
- How to protect?

Security Measures
- Information Safety
- Communication channels
- Standard Operating Procedures
- Security Measures

Security Tools
- Passwords & Encryption
- Operational & Mobile Security
- Analysing measures
How secure are your passwords?
Let’s check
Just!c3 !8

correct horse battery staple
Just!c3!8

correct horse battery staple
28 bits of entropy

Just!c3!8

2^28

Non-gibberish word +16
Unknown order +1

Cap +1
Common permutations +3

Punctuation +4

Numeral +3

Correct horse battery staple +11

Four random common words +11
28 bits of entropy

$2^{28}$

Non gibberish word

$2^{16}$

Common permutations

$2^{3}$

Unknown order

$2^{1}$

Cap

$2^{1}$

Numeral

$2^{3}$

Punctuation

$2^{4}$

1000 guesses / s

44 bits of entropy

$2^{44}$

correct horse battery staple

$2^{11}$

Four random common words

$2^{11}$

1000 guesses / s
28 bits of entropy

\[ 2^{28} \]

Just!c3 !8

1000 guesses / s

CRACKED IN 3 DAYS

44 bits of entropy

\[ 2^{44} \]

correct horse battery staple

1000 guesses / s

CRACKED IN 550 YEARS
Sentence-long
Unique
Random
Extra characters
Justice 18

HARD TO REMEMBER

EASY TO CRACK

HARD TO CRACK
EASY TO REMEMBER

The Great Dictator is a great movie to watch
$M0v!e 9r@nd c@t z@nd@m !c3#
Let’s create
Dice-generated passphrases

1. Roll five dices at once.
2. Write all numbers down.
3. Look at the wordlist and find the word which corresponds with the numbers.
4. Write the word down that corresponds with the numbers.
5. Repeat step 1-4 five more times to come up with a total of six words.
6. Come up with a short story or phrase to remember the six words by.

e.g.: Anger – Cage – Echo – Royal – Smog – Truck

e.g.: I felt anger when locked in a cage I heard my own echo, which sounded royal through the smog all formed by the truck carrying my confinement.

https://www.eff.org/files/2016/07/18/eff_large_wordlist.txt
Let’s try!
How to communicate in a safe way?
Encryption: the basics

What you just did

Asymmetric encryption

(or should have done)

How this works
Hackathon
Analyse your measures

1. What is it?
2. When is it useful?
3. When is it not useful / what are its limitations?
4. What does it do to your content, data, metadata?
5. Where to get started / what best solutions out there?
6. Can it be dangerous to use?

Prepare an informative - but fun - presentation
Practice with your team
Security checklist
Security checklist

https://security.money-trail.org/
Questions & feedback
Money Trail
Digital safety & security

https://security.money-trail.org/