

# Social Engineering: What If The User Opens Back Doors To Strangers?



**Christina Lekati**  
Social Engineering Security  
Trainer & Consultant  
Cyber Risk GmbH



# About Me

---



## Christina Lekati

- Psychologist & Social Engineer
- Trainer & Consultant for Cyber Risk GmbH on the Human Element of Security
- Social Engineering & Security Awareness Trainings to All Levels of Employees / Security Teams
- Corporate & High-Value Target Vulnerabilities Assessments
- Executive Board Member of the OSINT Curious project



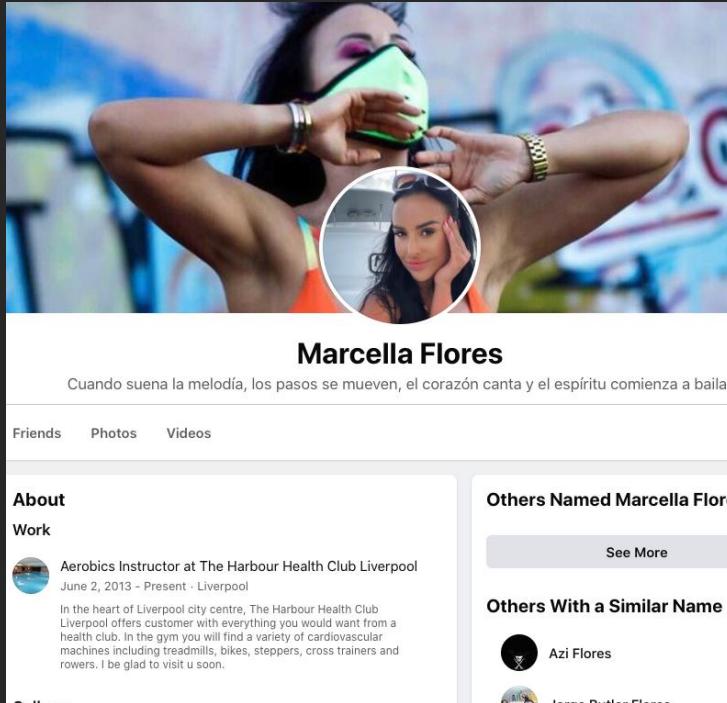
Christina Lekati



@ChristinaLekati



# Case Study: Marcella (Marcy) Flores



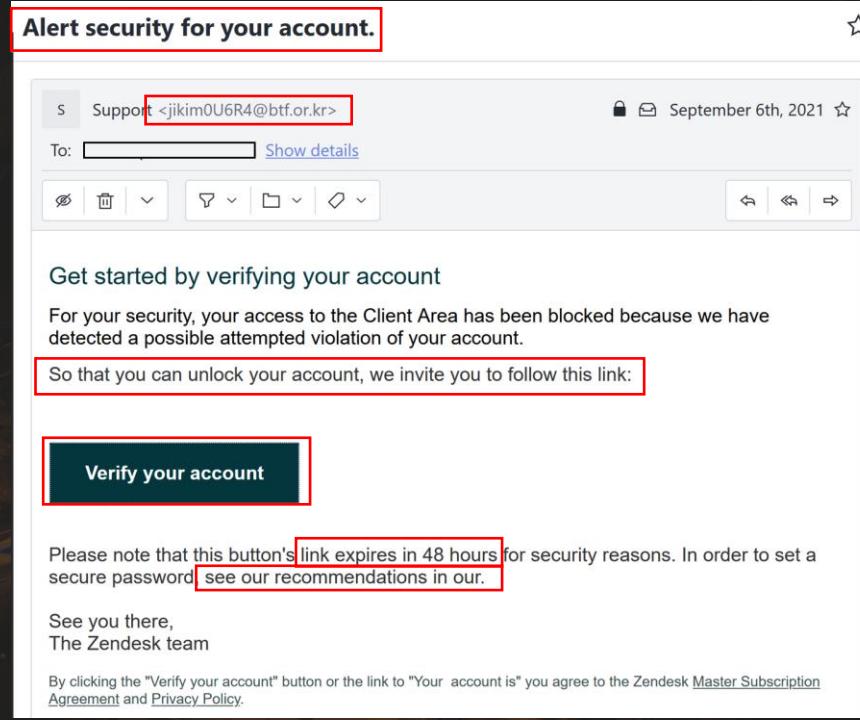
- Years-long Social Engineering operation targeting an employee of an aerospace defense contractor
  - “Marcella Flores” befriends the employee
  - First evidence of communication
  - “She” builds a relationship with him across corporate and personal communication platforms
  - Over 8 months, they exchange emails, messages, photographs – to establish credibility & rapport
  - Flirting was also added the mix
- 2019  
Nov. 2020  
June 2021

Source: <https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media>



# Social Engineering Attacks Have Evolved

## “Hit-and-Run”



VS

## More elaborate campaigns:

- Longer reconnaissance
- Tailored/ Personalized approach
- More elaborate mind-games
- Deep-fakes
- Often state-sponsored social engineering campaigns



# Case Study: Marcella (Marcy) Flores



From Marcella Flores<marcellaflores39@gmail.com>  
Sent on 6/1/2021, 4:01 AM  
To [REDACTED]  
Subject Diet Survey

My dear [REDACTED]  
This is a diet survey, u should fill out ur experiences esp during the pandemic period at home.  
Please press enable editing and then enable content to see full page.  
[https://1drv.ms/u/\[REDACTED\]](https://1drv.ms/u/[REDACTED])  
Send me soon, Thanks for kindness and ur participation  
Cheers  
Marcy😊

A	B	C	D	E	F	G					
	<b>Food habits</b>	<b>Your response</b>									
1	For privacy issues, this file is utterly confidential and anonymous. Therefore you are asked to click on "Enable Content" to have access throughout file.										
2	Eat plenty of fresh vegetables, legumes and fruits										
3	Eat plenty of cereals, preferably wholegrain, such as breads, rice, pasta and noodles										
4	Include lean meat, fish, poultry and/or alternatives										
5	Include milks, yogurts, cheeses and/or alternatives										
6	Batch cook large quantities of food to freeze										

2019  
Nov.  
2020  
June  
2021

- The threat actor sends the target malware via an ongoing email communication chain
- The “LEMPO” malware is designed to “establish persistence, perform reconnaissance, and exfiltrate sensitive information.”

Source: <https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media>



# Do These Operations Really Happen?!

**FACEBOOK**

We identified the following tactics, techniques and procedures (TTPs) used by this threat actor across the internet:

**Social engineering:** In running its highly targeted campaign, Tortoiseshell deployed sophisticated fake online personas to contact its targets, build trust and trick them into clicking on malicious links.

**Secureworks®**

Products Services Partners Research

Research > The Curious Case of Mia Ash: Fake Persona Lures Middle Eastern Targets

THREAT ANALYSIS

## The Curious Case of Mia Ash: Fake Persona Lures Middle Eastern Targets

SecureWorks® Counter Threat Unit™ Threat Intelligence

THURSDAY, JULY 27, 2017  
BY: COUNTER THREAT UNIT RESEARCH TEAM

**proofpoint.**

LOGIN

[Home](#) / [Blog](#) / [Threat Insight](#) / Operation SpoofedScholars: A Conversation with TA453



## Operation SpoofedScholars: A Conversation with TA453

JULY 13, 2021 |

JOSHUA MILLER, CRISTA GIERING, & THE THREAT RESEARCH TEAM

**proofpoint.**

LOGIN

[Home](#) / [Blog](#) / [Threat Insight](#) / I Knew You Were Trouble: TA456 Targets Defense Contractor with Alluring Social Media Persona



## I Knew You Were Trouble: TA456 Targets Defense Contractor with Alluring Social Media Persona

JULY 28, 2021 |

JOSHUA MILLER, MICHAEL RAGGI, & CRISTA GIERING

### Sources:

- <https://about.fb.com/news/2021/07/taking-action-against-hackers-in-iran/>
- <https://www.secureworks.com/research/the-curious-case-of-mia-ash>
- <https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media>
- [https://www.proofpoint.com/us/blog/threat-insight/operation-spoofedscholars-conversation-ta453?utm\\_source=social\\_organic&utm\\_social\\_network=twitter&utm\\_campaign=21\\_July\\_Corporate\\_blog+&utm\\_post\\_id=ccf4c45f-a244-4163-8b61-f55737f869ff](https://www.proofpoint.com/us/blog/threat-insight/operation-spoofedscholars-conversation-ta453?utm_source=social_organic&utm_social_network=twitter&utm_campaign=21_July_Corporate_blog+&utm_post_id=ccf4c45f-a244-4163-8b61-f55737f869ff)



# Social Engineering Patterns

	“Mia Ash”	Operation “SpoofedScholars”	Facebook’s Fake Profiles	“Marcella Flores”
Target(s)	Specific individuals from specific countries & industries	Individuals “of intelligence interest” – highly selective targets.	Highly targeted personnel from: military, defence & aerospace industries	One target – defence aerospace contractor
Reconnaissance	Social Media	-	Social Media	Social Media
Communication Medium	Social Media, phone, email	Email	Social media , email, phone, other websites	Social media, email, other platforms
Pretext	Fake online persona	Fake persona/ Online conference invitation	Fake online personas	Fake online persona
Rapport/Trust Building Tactic(s)	Common interests – trust / relationship building	Use of legitimate (but compromised) infrastructure –lengthy communications	Casual contact and trust / relationship building	Long-term casual contact and trust / relationship building
Exploitation	Malicious email – Attachment - PupyRAT	Malicious email – Link - Credential Harvesting Website	Malware distribution, Credential Harvesting	Email - OneDrive URL - malicious files - LEMPO Malware
Goal	Espionage operations	Collection of Sensitive Information	Espionage operations	Reconnaissance, Exfiltration of Sensitive Information



# Kill-Chain Backbone



**Specific Target(s)**



**Reconnaissance**  
Mostly via Social Media & Public Presence



**Online Fake Persona**

Mostly using multiple social media platforms to appear legitimate



**Personalized Approach**



**Escalation from one platform**  
to other websites/phone and email



**Casual contact and trust / relationship building**

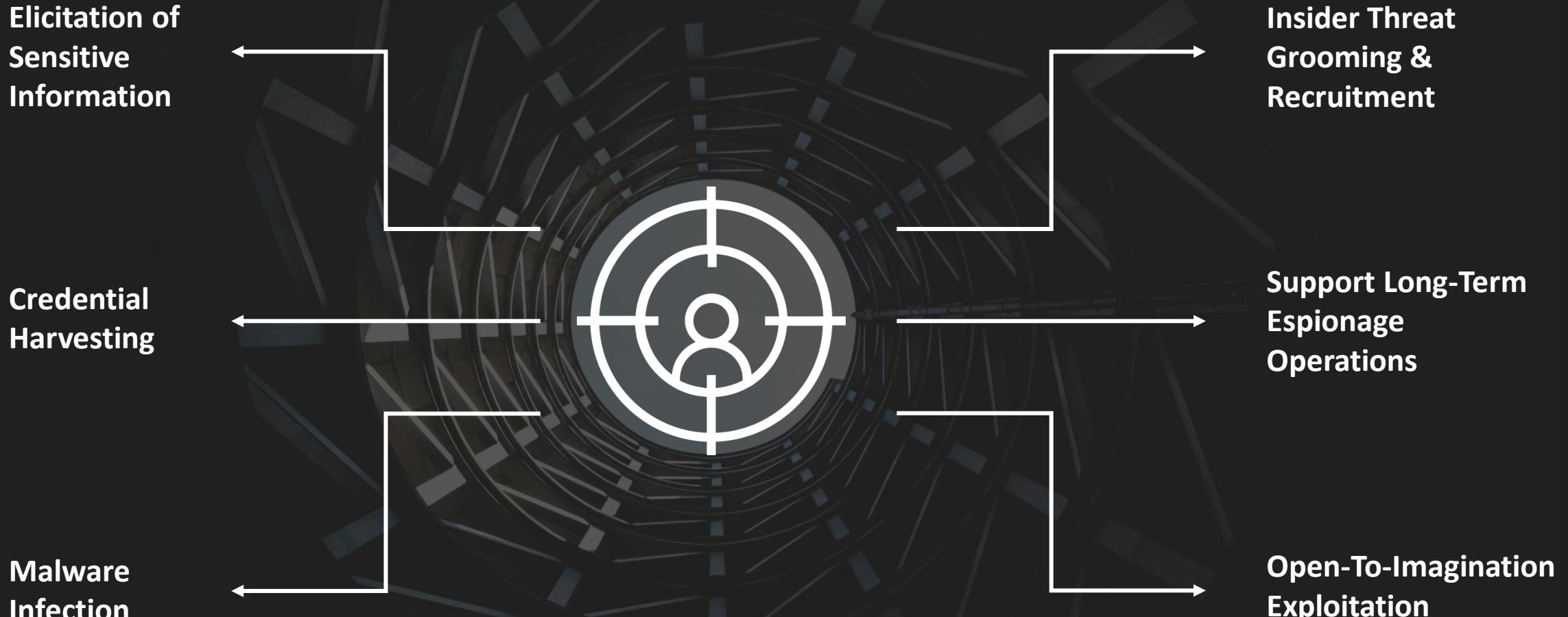


**(Casual)**

**Exploitation of Trust**  
Under A Pretext



# Return On Investment?



# Is This Happening A Lot?



ENISA THREAT LANDSCAPE 2022  
NOVEMBER 2022

## EXECUTIVE SUMMARY

This is the tenth edition of the ENISA Threat Landscape (ETL) report, an annual report on the status of the cybersecurity threat landscape. It identifies the top threats, major trends observed with respect to threats, threat actors and attack techniques, as well as impact and motivation analysis. It also describes relevant mitigation measures. This year's work has again been supported by ENISA's ad hoc Working Group on Cybersecurity Threat Landscapes (CTL).

During the reporting period of the ETL 2022, the prime threats identified include:

1. Ransomware
2. Malware
3. Social Engineering threats
4. Threats against data
5. Threats against availability: Denial of Service
6. Threats against availability: Internet threats
7. Disinformation – misinformation
8. Supply-chain attacks

The cover of the ENISA Threat Landscape 2022 report features a dark blue background with abstract white wave patterns. Overlaid on the waves are several blue icons: a person holding a sword, a shield, a skull, a thumbs-up, a soccer ball with an exclamation mark, and a book labeled "CVE". In the bottom right corner, the title "ENISA THREAT LANDSCAPE 2022" is written in large, white, sans-serif capital letters. The top right corner includes the European Union flag and the text "EUROPEAN UNION AGENCY FOR CYBERSECURITY".

## Social Engineering is a primary attack vector.

Source: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

Christina Lekati | Cyber Risk GmbH



# Weaponized Psychology

---

Cyber security is not only a technical challenge...

...it is also a behavioral one.

- As long as managers and employees can provide **access to systems** and **high-value information**, they become **targets**.
- Cybersecurity depends on them too.

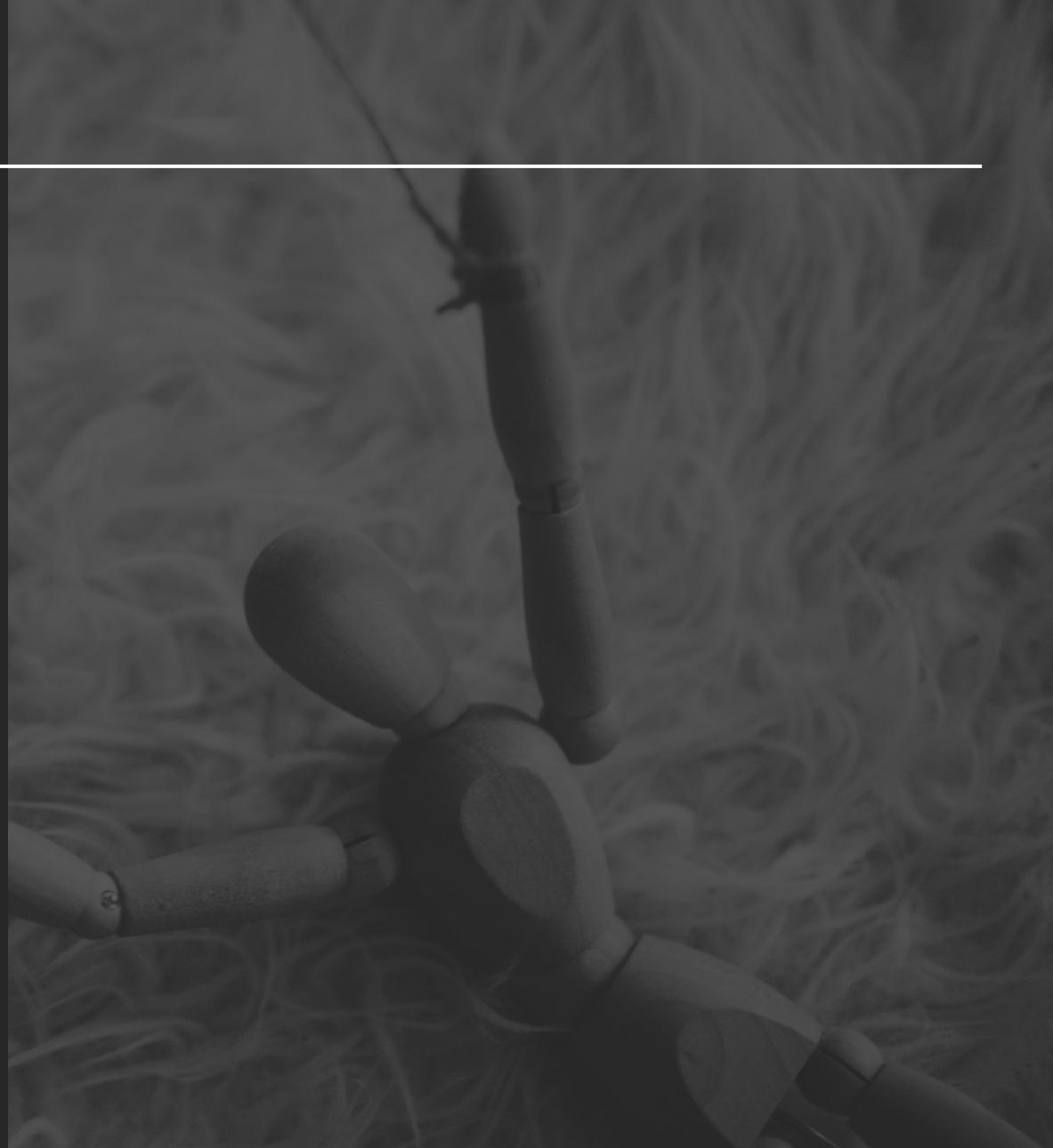


# Weaponized Psychology

---

- It is practical: low-cost, low risk, high-reward.
- Identifying and exploiting human vulnerabilities  
...or simply human needs.
- The basic human psychological wiring is universal  
...and it is universally exploitable.

*The stimulus-response effect in human triggers is consistent, and exploiting these vulnerabilities is consistently successful.*



# Weaponized Psychology

Example:

Unmet Needs.

Difficult to identify?

 My **weakness** is **poker** and I am being offered a bonus to play again. I know where my free time (what is that) is going to go **for** a week or so

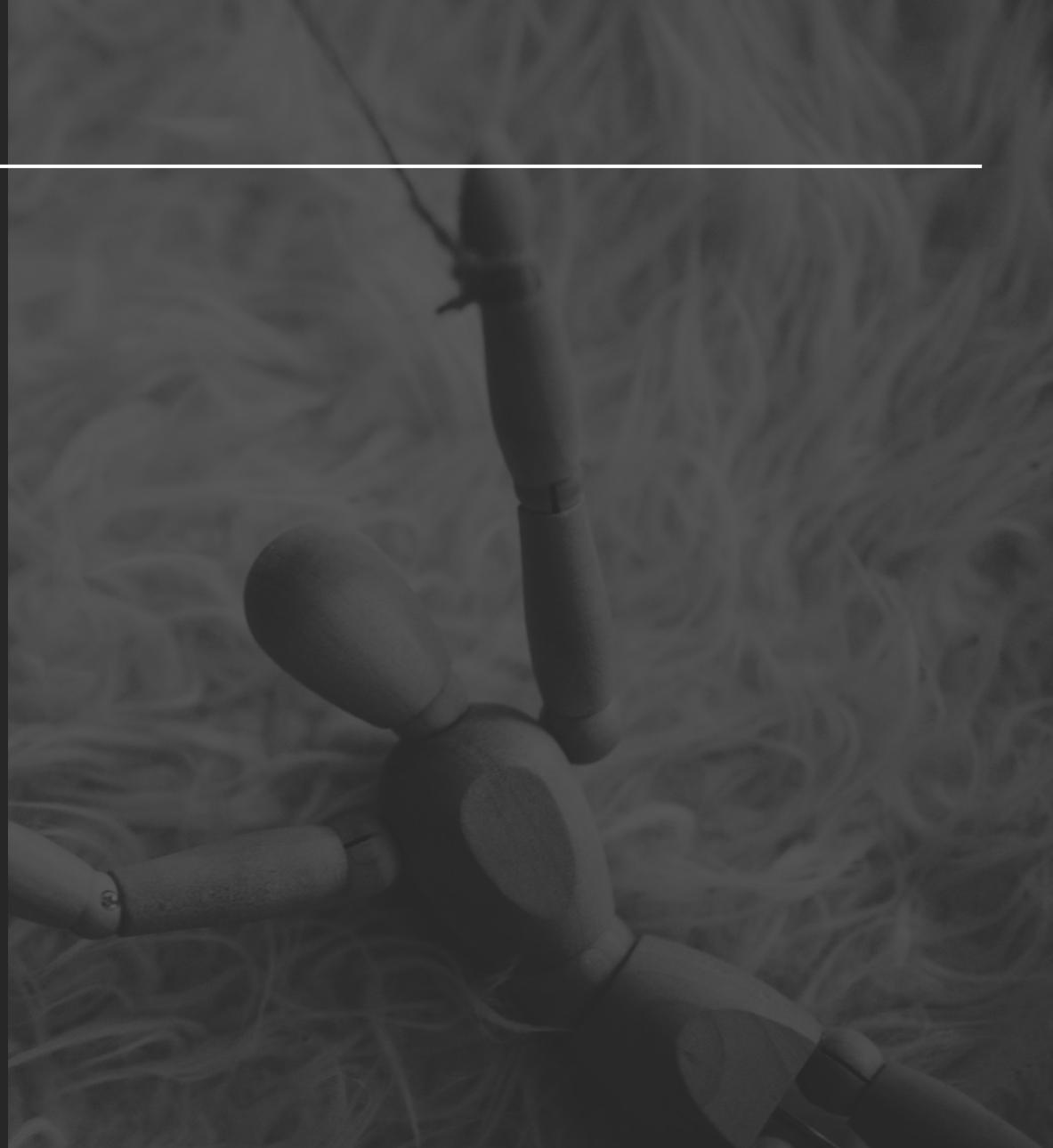
 29 November 2017 ·   
I am not alone because loneliness is always with me

 Beautiful **Women** is my **weakness** 😊 that's my only downfall 😞

 I work super hard. I **deserve Luxury**.



# Weaponized Psychology & OSINT

We pay more attention to what we prioritize. Other information may fade in the background.

I should be more concerned about my **job** but I'm really not .

[REDACTED] hate my job 😭😭😭

Ex Employee - [REDACTED]

Doesn't recommend      Negative forecast      Approves managing directors

I worked at [REDACTED] for more than a year - full time

**Pros**

Great team, lots of young people, good climate, great view, cafeteria, fitness facilities in the house, ongoing training, several events per year.

**Contra**

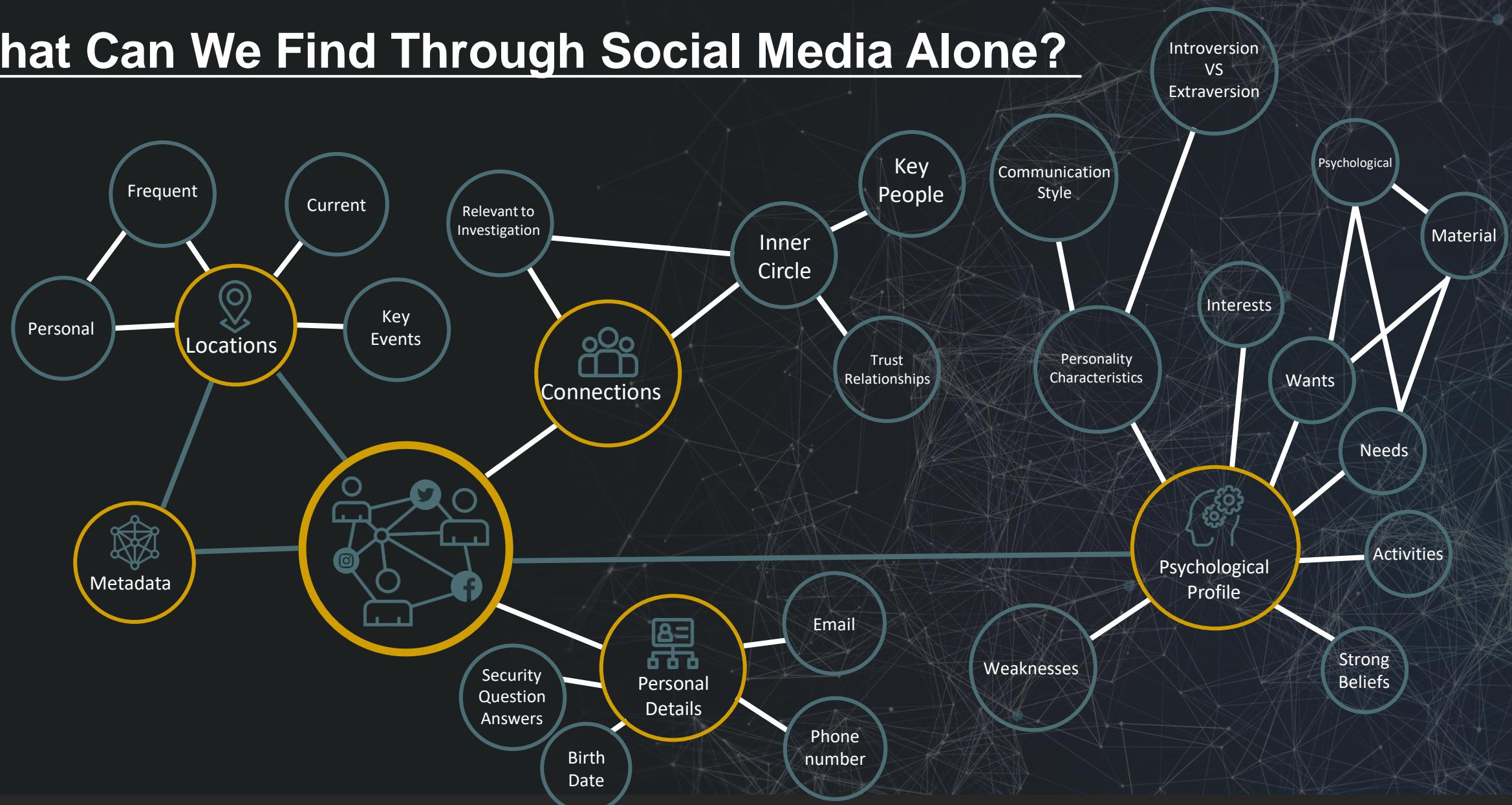
Insufficient extreme pressure, employees are treated like machines. if you are not strong enough, you will become mentally ill after some time. If there is constant monitoring, the best times have to come so you cannot really respond to customer requests. Customers are sometimes treated badly. (since there is no time to take a closer look at the problem) It is always extreme stress, can never recover briefly.

**Advice to management**

become more human.



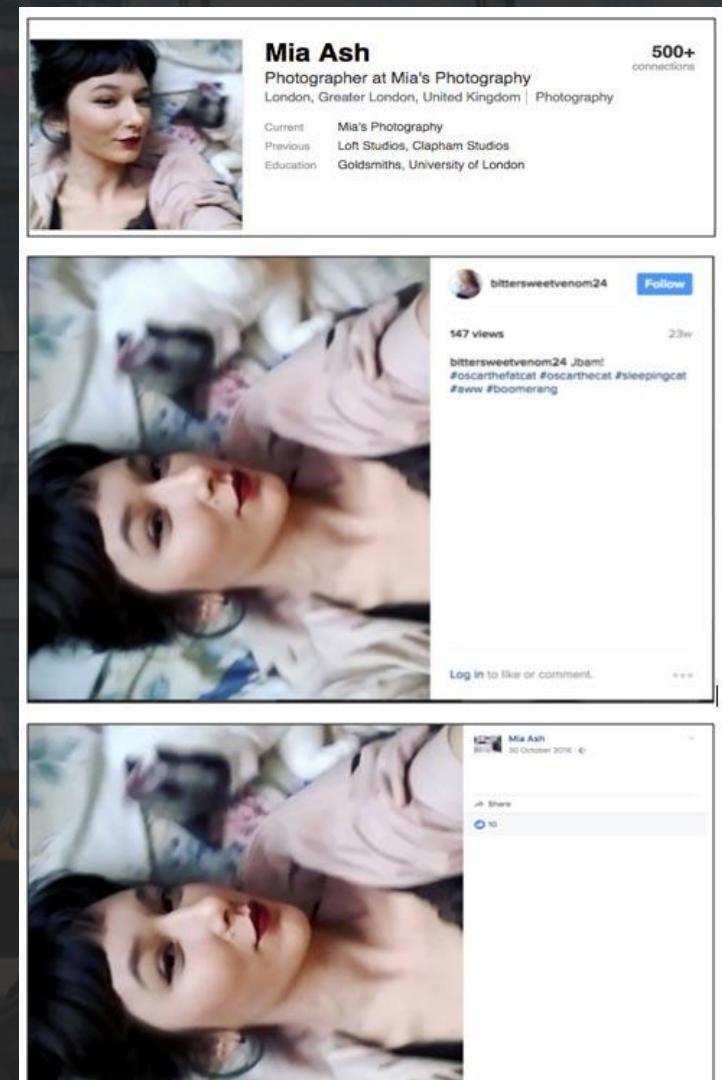
# What Can We Find Through Social Media Alone?



# Case Study: Mia Ash

- Threat actor: likely COBALT GYPSY
- Target: telecommunications, government, defense, oil, and financial services organizations in Middle East and North Africa
- Plan A: Phishing attacks delivering PupyRAT
- Plan B: Mia Ash
- Fake identity used several social media accounts used to perform reconnaissance on and establish relationships with specific targets

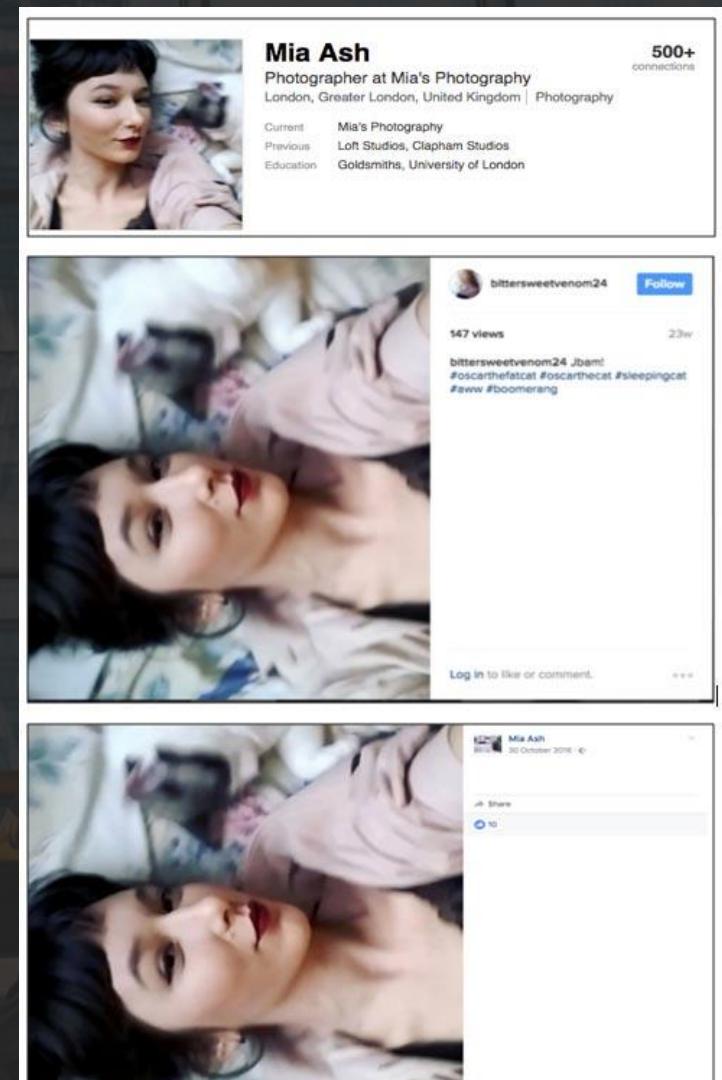
Source: <https://www.secureworks.com/research/the-curious-case-of-mia-ash>



# Case Study: Mia Ash

- Profiles that appear intended to **build trust and rapport** with potential victims.
- “She” initiated conversations based on “**common interests**” and moved on to profession-related, and personal discussions.
- **Escalated** target to other social media platforms & phone
- Once **work email** was provided – malicious Excel file was sent.
- The file would eventually deliver a PupyRAT

Source: <https://www.secureworks.com/research/the-curious-case-of-mia-ash>



*How do we defend against this threat?*



# Things We Know

---

As a general rule, there are **no rules**, and **no one** is exempt.



# Elicitation Techniques

---

*Oohhh...you are THE ONLY ONE who can help me with...*

*"Flattery"*

*From one IT pro to another, what is your take on XYZ technology....*

*"Familiarity & Tribe Instinct"*

*Terrible day at work? I had one too...what happened?*

*"Empathy & Tendency to Complain"*



**Elicitation:** An effort in which a seemingly normal conversation is contrived to extract (sensitive) information about individuals, their work, and their colleagues.



# Deflecting Elicitation Techniques

---

- Know what information should not be shared.
- Be suspicious of people who seek such information.
- Do not tell people any information they are not authorized to know.
- Do not click on links / download & enable attachments from online “strangers”.  
Avoid typing your credentials on a website you visited through an email link.



Source: [https://www.dcsa.mil/Portals/91/Documents/CI/DCSA-CI\\_Elicitation\\_2021.pdf](https://www.dcsa.mil/Portals/91/Documents/CI/DCSA-CI_Elicitation_2021.pdf)



# How Do We Protect HVTs?

What about the High Value Targets of the organization - the ones with increased levels of exposure and privileges?

The image displays two side-by-side screenshots from Trend Micro's website. The left screenshot shows the 'Executive Leadership' section under 'Corporate Executives', listing profiles for the Chief Executive Officer, Chief Financial Officer, Executive Vice President Japan and Global Consumer Business, Chief Operating Officer, Chief Marketing Officer, Executive Vice President Research & Development, and Executive Vice President Care Technology and CIO. Each profile includes a photo, title, and a 'View bio [+]' button. The right screenshot shows the 'Leading Security Experts' section, featuring profiles for the Chief Cybersecurity Officer and Vice President, Security Research. Both sections include a header image of a man in a suit, a brief bio, experience, specialties, education, and a 'Twitter' link.



# Target Vulnerability Assessments

---

## Criticality

Degree of importance, privileges, access to information and assets in an organization.



## Accessibility

Ease of approach, engagement & social escalation with the target.



## Detection & Response Capability

Target's level of knowledge & sophistication in recognizing & deterring attacks



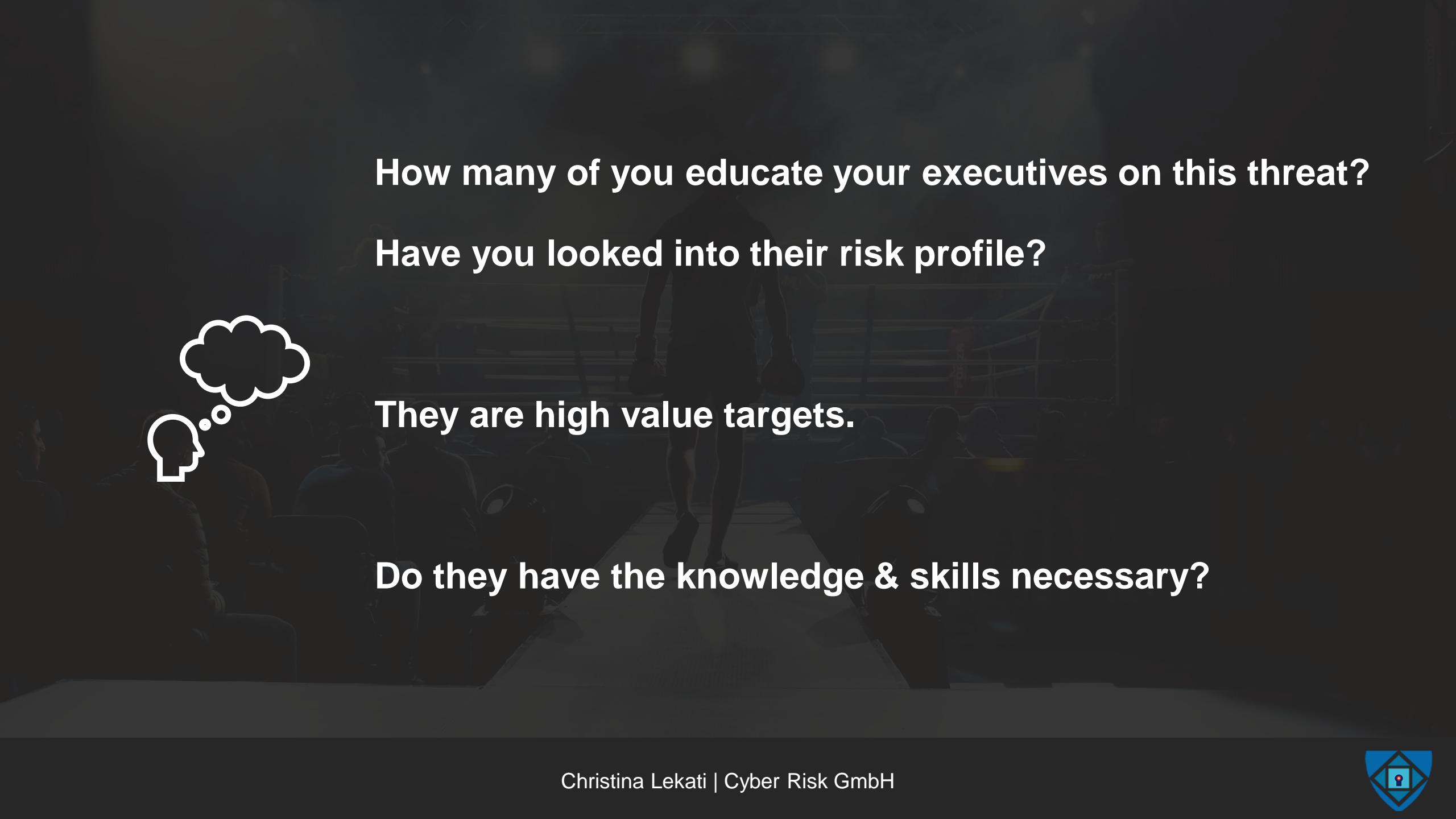
## Recognizability

Ability for an adversary to identify the target and collect information on them

## Vulnerability

Target: exposure, predictability, profiling accuracy  
Adversarial: capability, determination, resources





**How many of you educate your executives on this threat?**

**Have you looked into their risk profile?**



**They are high value targets.**

**Do they have the knowledge & skills necessary?**





**This is too advanced;**

**Our executives & employees still fall for the simple  
phishing emails!**



# Most Common Remarks From Victims:

---

*“I thought something was off.  
Wasn’t sure how to respond,  
so in the spur of the moment,  
I went with it.”*

*“...I didn’t report it  
because I felt I would also  
be implicated and actually  
I didn’t want to get fired.”*

*“I was under a lot of time  
pressure and my manager  
would not appreciate that  
verification call.”*

*“It did not even cross my  
mind that I could \*actually\*  
be a target.”*



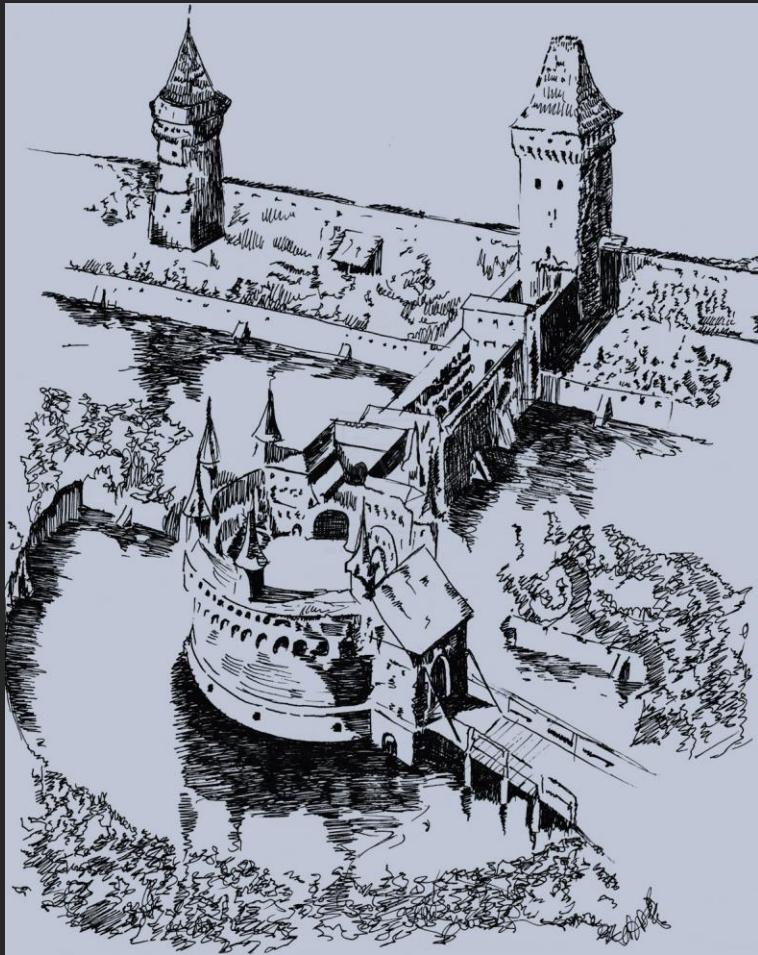
# Is This The Wild West?

---



# But...This is War

---



- Walls & Physical Security →
- Security technology “weapons” →
- Does the population open back doors to strangers?!
- Do they know who the enemy is?! Their tricks and tactics?
- Do they spread the word and are they prepared to defend?



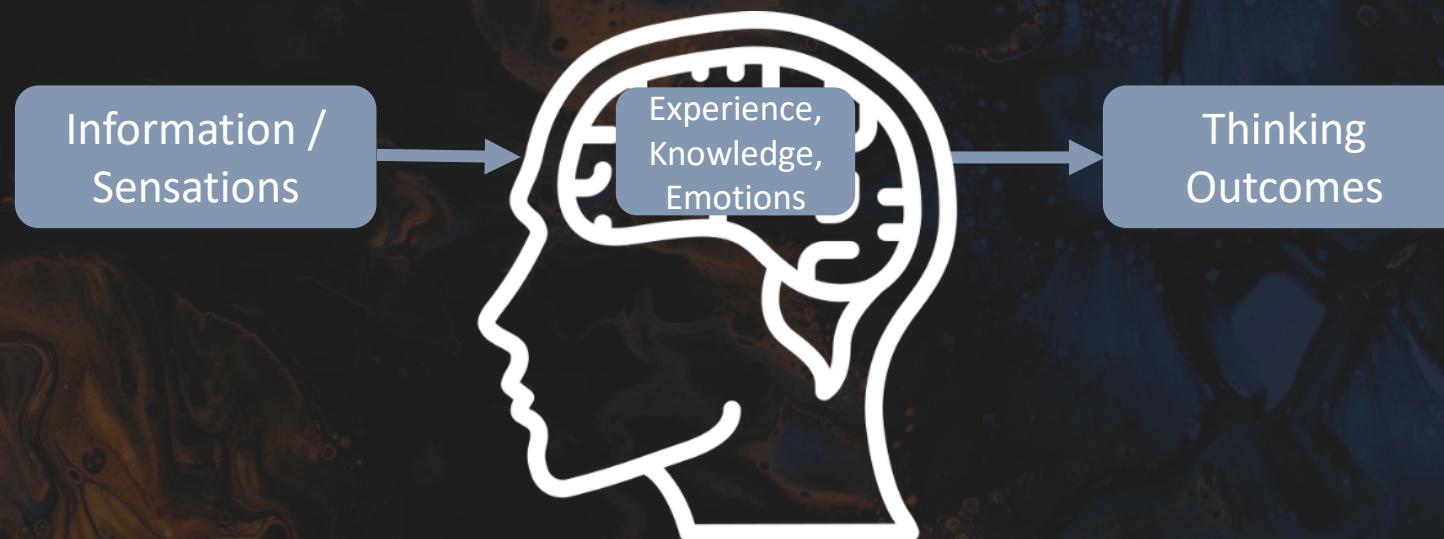
# The Good News: Neuroplasticity

---

The User can “make” or break almost any technical security measure.

Our brains ARE capable of creating new behavioral pathways that can become automatic.

Red flags act like cognitive triggers when employees have been trained well.



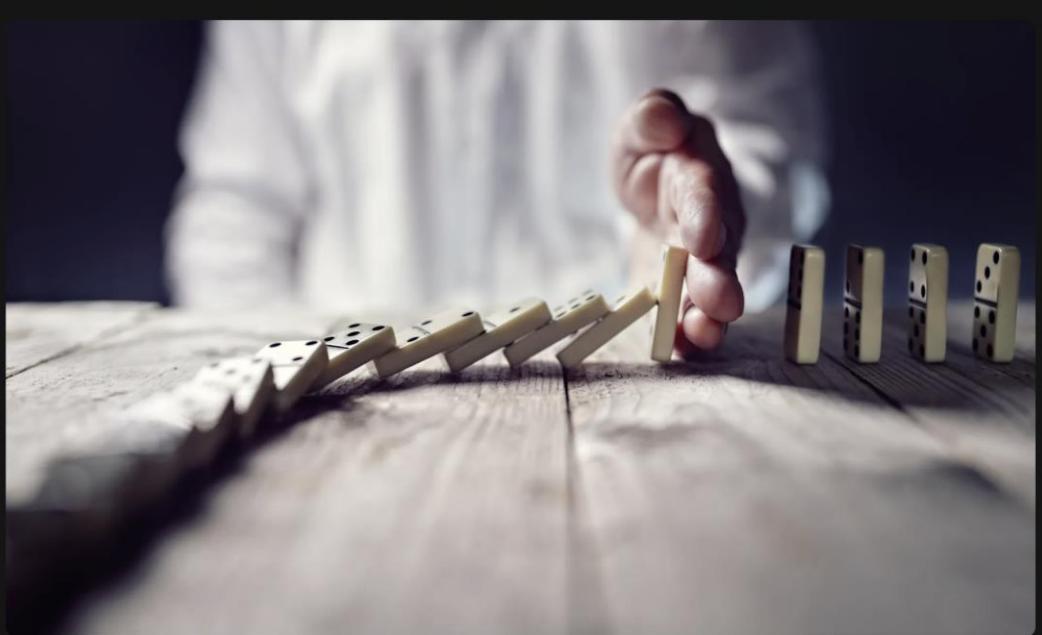
# Defense

---

- Minimize employee decision-making and use the principle of least privilege where possible
- Good quality training that actively engages employees. Training that is personal, intrigues and interests them
- Reinforce a “security mindset” within your organization – utilize group influence tactics
- Run exercises / attack simulations to reinforce good practices, learning & memory
- Conduct vulnerability assessments through open-source intelligence (OSINT)



# Additional Resources



## Social Engineering Kill–Chain: Predicting, Minimizing & Disrupting Attack Verticals



Christina Lekati on Jun 02, 2022

Source: <https://ahead.feedly.com/posts/social-engineering-kill-chain-predicting-minimizing-and-disrupting-attack-verticals>

Christina Lekati | Cyber Risk GmbH

The cover of a brochure titled "ELICITATION". It features the Defense Counterintelligence and Security Agency (DCSA) logo at the top left. The main title "ELICITATION" is in large, bold, blue capital letters on the right side. Below the title, there is contact information: "DCSA", "https://www.dcsa.mil", "DCSA, Counterintelligence Directorate", "https://www.dcsa.mil/mc/ci", and "Center for Development of Security Excellence", "https://www.cdse.edu". At the bottom, there is a "BE ALERT! BE AWARE!" section with the instruction "Report suspicious activities to your facility security officer". The DCSA logo is also present at the bottom right.

Source: [https://www.dcsa.mil/Portals/91/Documents/CI/DCSA-CI\\_Elicitation\\_2021.pdf](https://www.dcsa.mil/Portals/91/Documents/CI/DCSA-CI_Elicitation_2021.pdf)



***“Knowledge is a weapon.  
I intend to be formidably armed.”***

*- Terry Goodkind*



## **Christina Lekati**

Social Engineering Security  
Trainer & Consultant  
Cyber Risk GmbH

### Contact Details:



Christina Lekati



@ChristinaLekati