

# **Social Engineering: Targeting Key Individuals, Profiling And Weaponizing Psychology**



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



# About Me

---

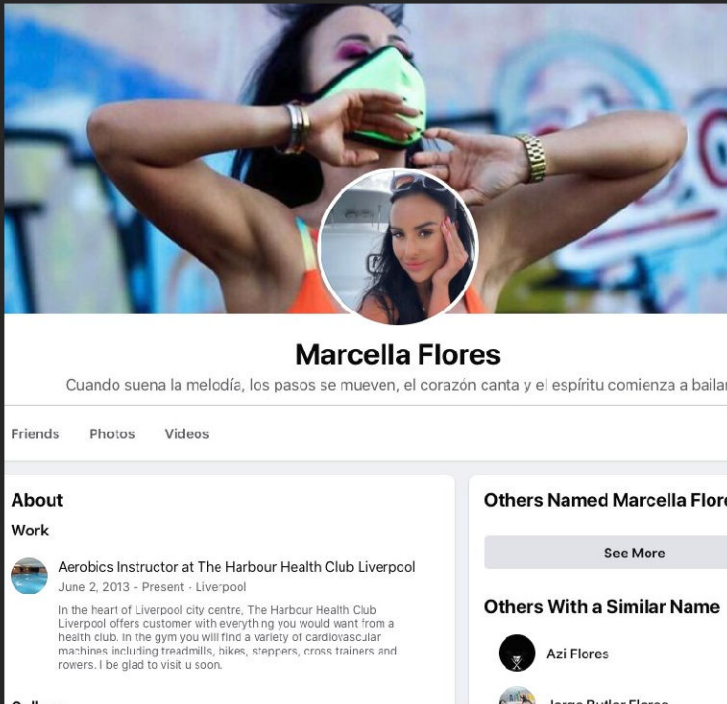


## Christina Lekati

- 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



# 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

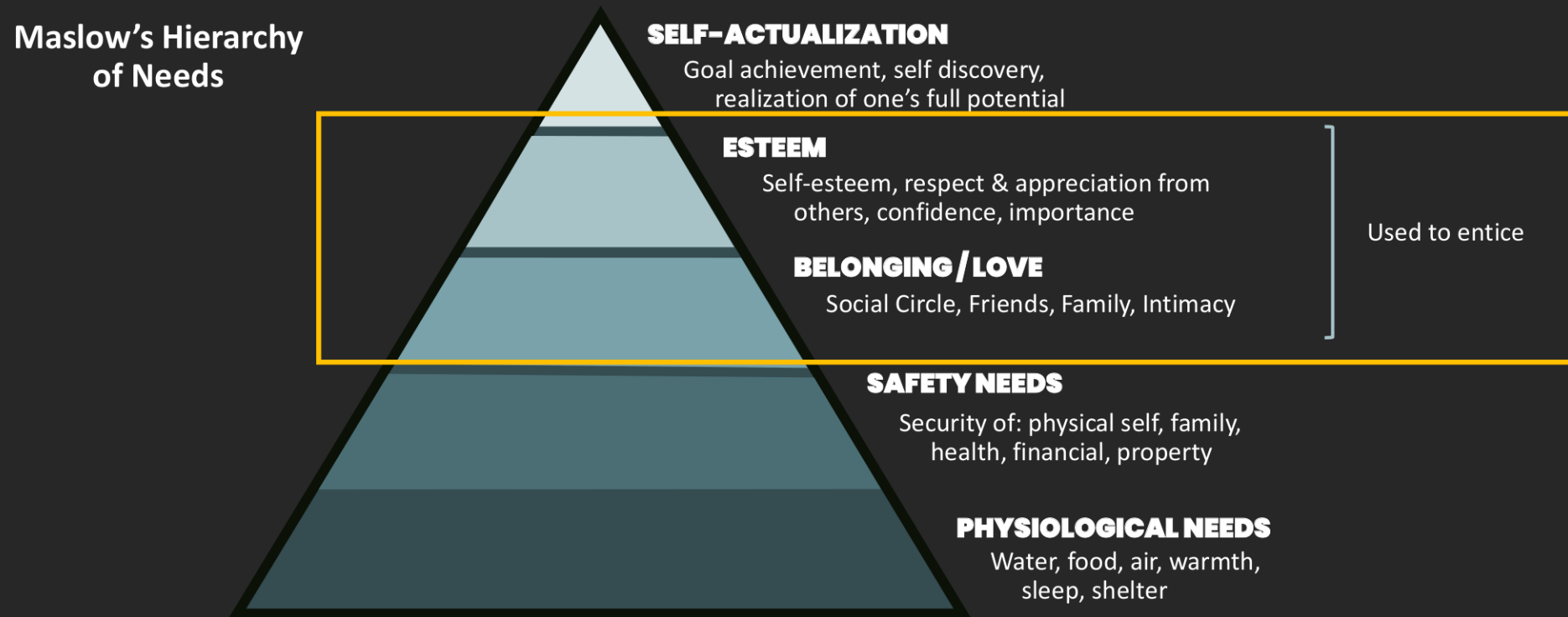
Nov.  
2020

June  
2021

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



# When Basic Human Needs Are Part Of The Kill-Chain



# Social Engineering Attacks Have Evolved

## “Hit-and-Run”



VS



### Alert security for your account.

Support <jikim0U6R4@btf.or.kr> September 6th, 2021

To:  [Show details](#)

Get started by verifying your account

For your security, your access to the Client Area has been blocked because we have detected a possible attempted violation of your account.

So that you can unlock your account, we invite you to follow this link:

[Verify your account](#)

Please note that this button's link expires in 48 hours for security reasons. In order to set a secure password [see our recommendations in our](#).

See you there,  
The Zendesk team

By clicking the "Verify your account" button or the link to "Your account is" you agree to the Zendesk [Master Subscription Agreement](#) and [Privacy Policy](#).

More elaborate campaigns:

- Longer reconnaissance
- Tailored/ Personalized approach
- More elaborate mind-games
- Deep-fakes & AI



# Case Study: Marcella (Marcy) Flores



**Marcella Flores**

Cuando suena la melodía, los pasos se mueven, el corazón canta y el espíritu comienza a bailar

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.

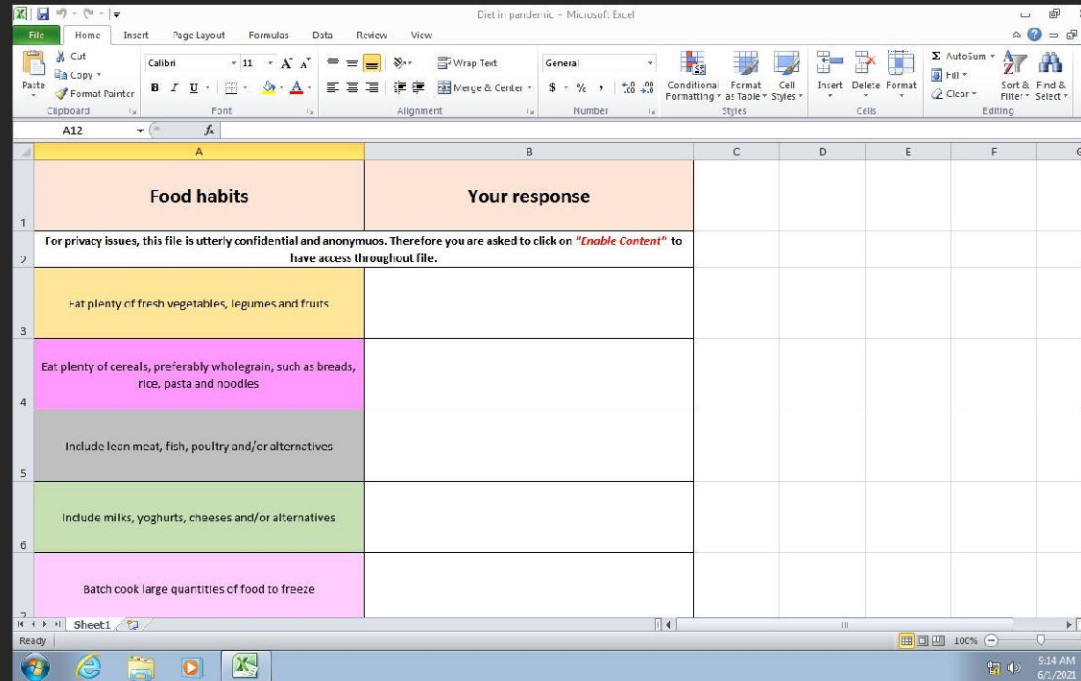
[https://1drv.ms/w/\[REDACTED\]](https://1drv.ms/w/[REDACTED])

Send me soon, Thanks for kindness and ur participation

Cheers

Marcy 😊

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



- 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.”

2019

Nov.  
2020

June  
2021



# 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 Res

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 Q ☰

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

f t in e

proofpoint. LOGIN Q ☰

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

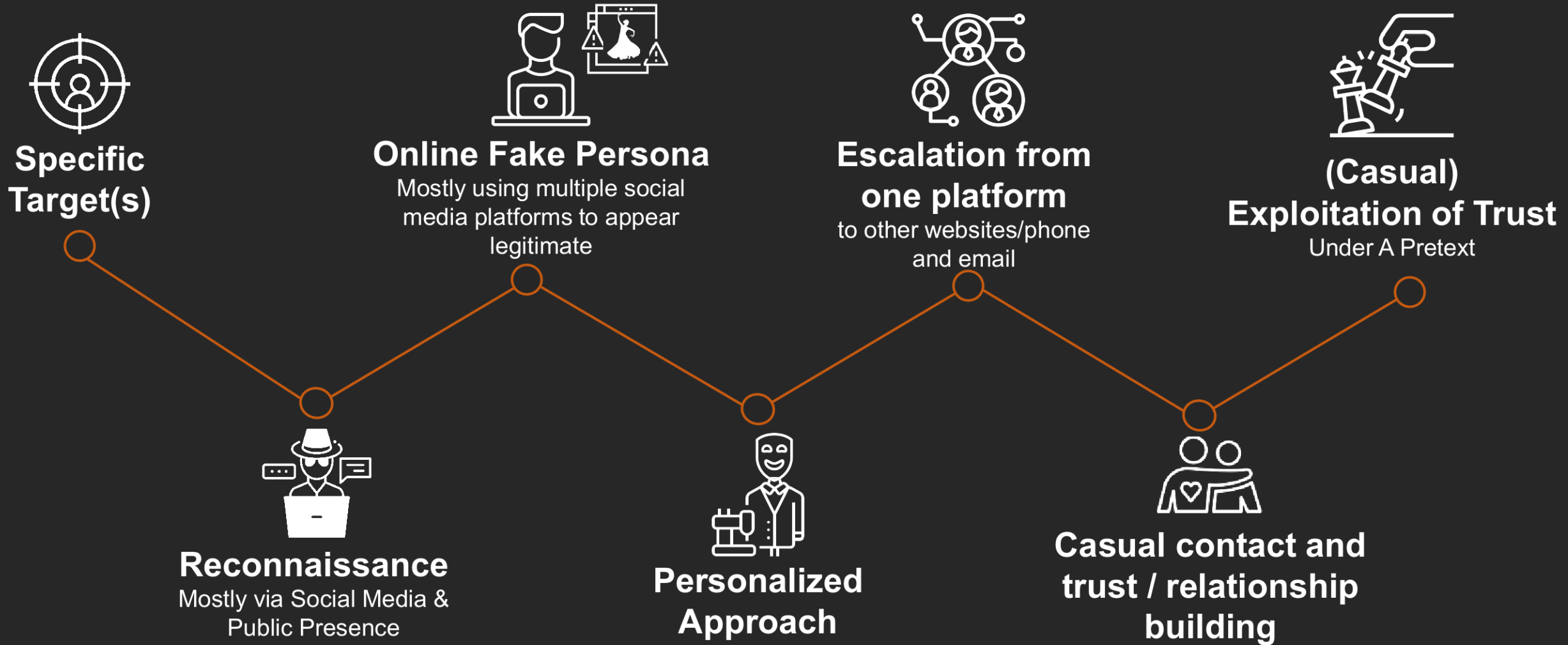
f t in e

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)



# Kill-Chain Backbone





# Return On Investment?

---

Elicitation of Sensitive Information

Insider Threat Grooming & Recruitment

Credential Harvesting

Support Long-Term Espionage Operations

Malware Infection

Open-To-Imagination Exploitation



# Target Behavior as a Cybersecurity Issue

---

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.

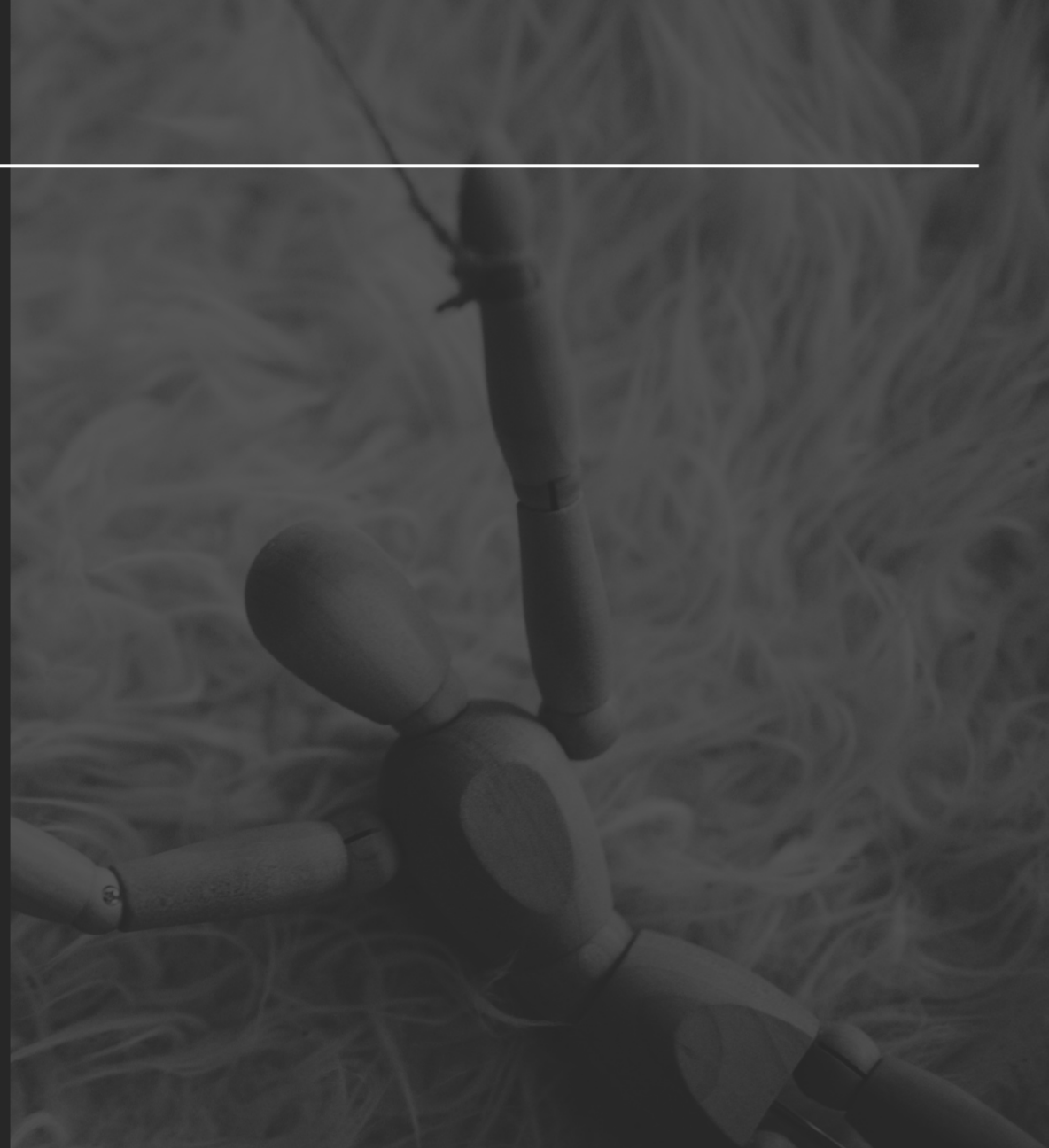


# Weaponized Psychology

---

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

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




# Weaponized Psychology





---



Example:

Unmet Needs. Strong Interests & Opinions.


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 · 

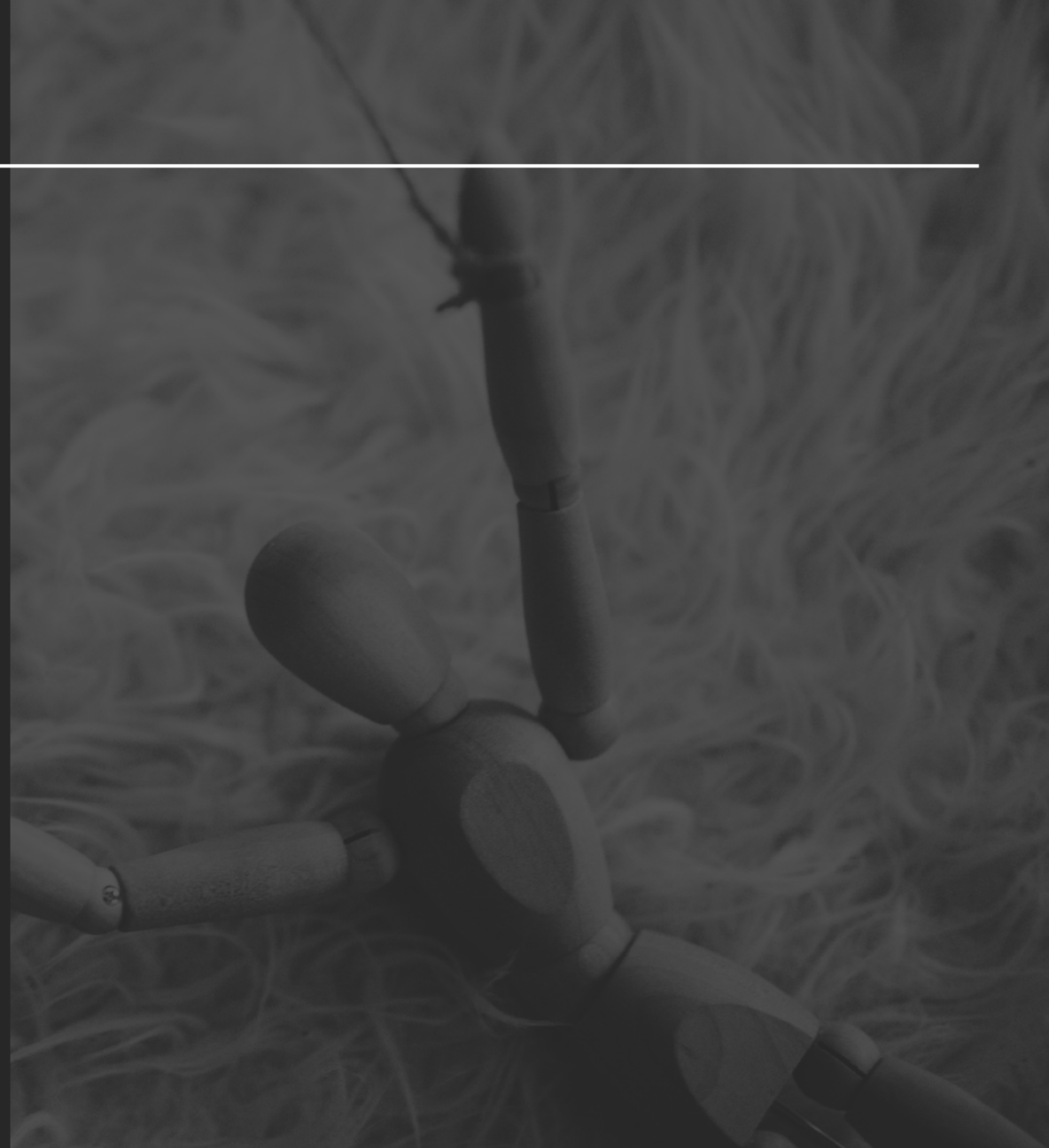
I am not **alone** because loneliness is **always** with me

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

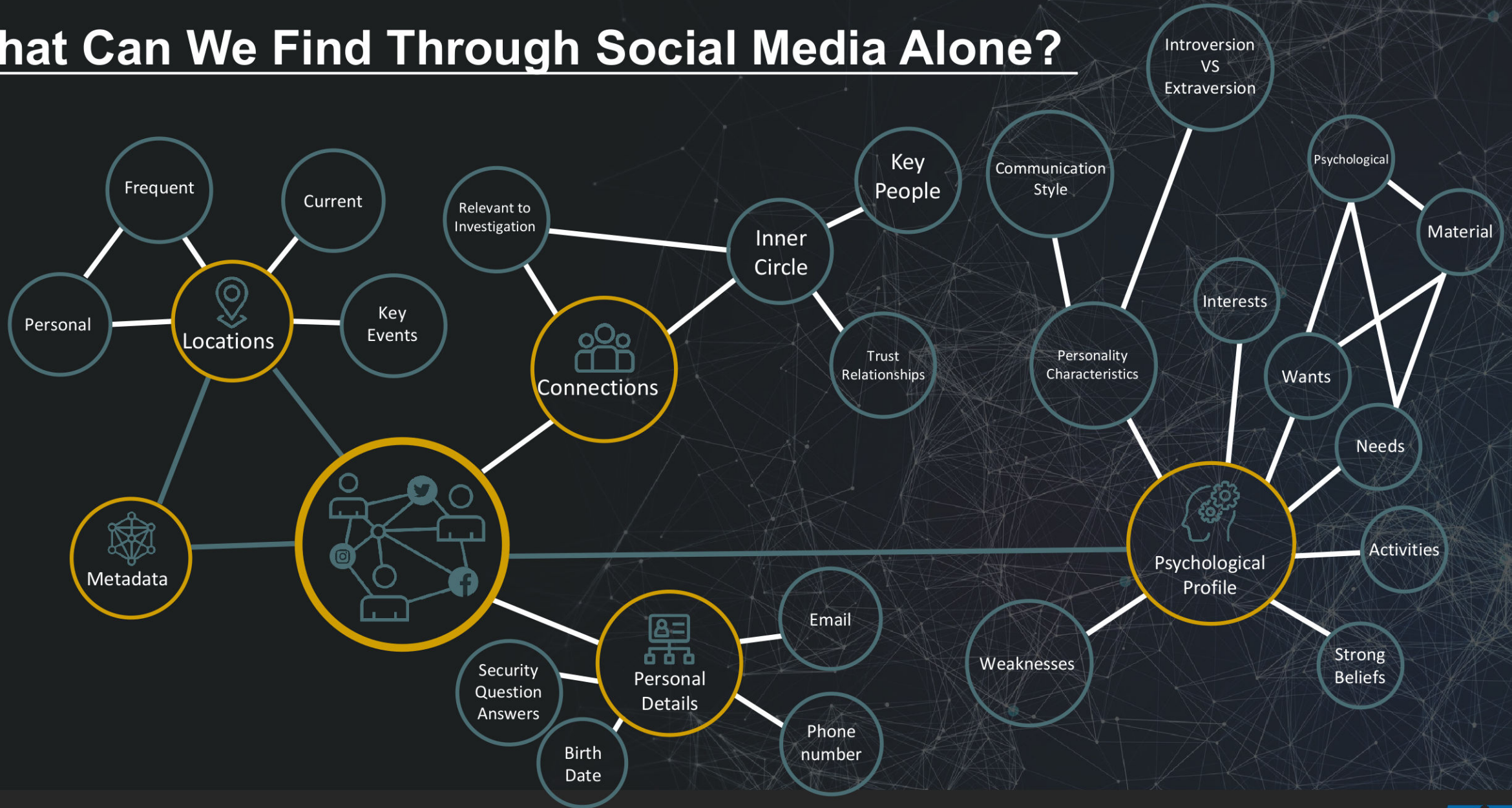
   

 I work super hard. I **deserve Luxury**.



# What Can We Find Through Social Media Alone?





**Threat &  
Vulnerability Profile**

# High Value Individuals / Targets

---

Business Leaders

CxO

Executives

People / Teams with :

- high-level clearance
- access to valuable information & assets



Public Figures:

- Politicians
- Celebrities
- Influencers
- Etc.



# What Do They Have?

---

Access to Sensitive Documents

They Are Valuable Insiders

Access to Privileged Accounts

Knowledge of Internal (Confidential) Details & Strategies

Authority Within the Organization

High Levels of Public Exposure





# Sensitive Information & Access

---

- Sensitive Information has a VERY high value.
- Classified Information or Controlled Unclassified Information (CUI)
- *“Unauthorized Disclosure is the communication or physical transfer of classified information or CUI to an unauthorized recipient”*
  - U.S. Department of Defense
- Unauthorized Disclosure:
  - Intentionally
  - Unintentionally



# Sensitive Information; Espionage Campaigns

## MI5 head warns of 'epic scale' of Chinese espionage

1 day ago



By Gordon Corera  
Security correspondent, BBC News

Source: <https://www.bbc.com/news/uk-67142161>

"If you're working today at the cutting edge of technology then geopolitics is interested in you, even if you're not interested in geopolitics," Mr McCallum said.

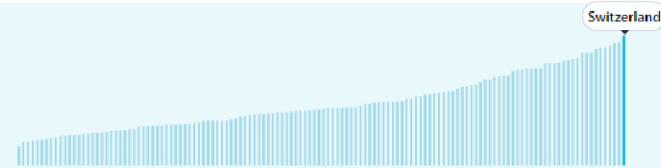
Mr McCallum said that MI5 had now seen suspected Chinese agents approach over 20,000 people in the UK over professional networking sites like LinkedIn, in order to try to cultivate them to provide sensitive information, double the previously reported figure.

The consequences of research being stolen in cutting-edge fields like Artificial Intelligence are not just for a company's profitability but also for the future of western countries, the head of MI5 warned.

*Which other country is at the "cutting edge of technology"?*

Switzerland ranking in the Global Innovation Index 2023

> Switzerland ranks **1st** among the 132 economies featured in the GII 2023.



Source: <https://www.wipo.int/gii-ranking/en/switzerland>

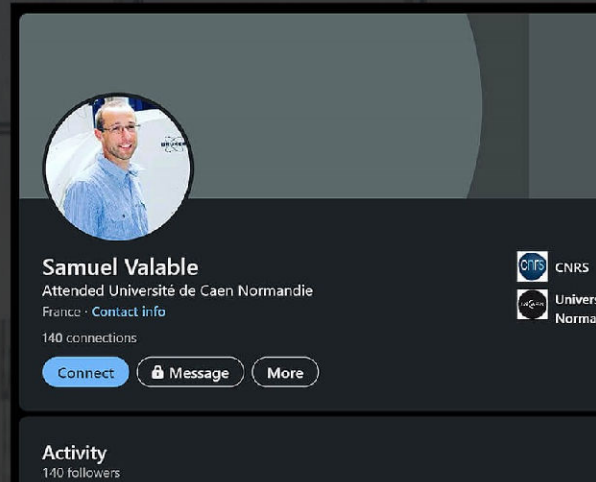


# Charming Kitten; Advanced Persistent Threat



Charming Kitten

Source: [www.crowdstrike.com/adversaries/](http://www.crowdstrike.com/adversaries/)



## Personally tailored attacks

The BfV writes that the group, which is considered a complex, targeted threat (Advanced Persistent Threat – APT), is using “sophisticated social engineering” for its current espionage attempts in this country. To do this, she develops “online identities tailored to the victims.” To do this, the attackers first researched the preferences and interests - including political ones - of their targets.

Source: <https://www.heise.de/news/Verfassungsschutz-Iranische-Hacker-wollen-Regimekritiker-hierzulande-ausspaehen-9240674.html>

“In the second step, personal contact takes place, during which the victim is manipulated through social engineering and misled with false promises to behave in a way that is critical to security. As a third step, once the conversation has established itself, the attacker sends an invitation to an online video chat. In order to participate in the video chat, the victim must click on the link sent by the attacker. In the login mask, the victims enter their login data and allow the attacker to access the online services they use.” continues the report. “Through the social engineering carried out in advance, Charming Kitten can establish a seemingly harmless contact in a targeted manner, in that the group refers to people who are known to the victims or addresses topics that seem logical to the victims.”

Source: <https://securityaffairs.com/149400/breaking-news/charming-kitten-targets-iranian-dissidents.html>



# Published Threat Intelligence & Unpublished Stories

We know of State-Sponsored APTs & Cyber Crime/  
Ransomware groups that rely on this Modus Operandi:

But there are also 100 untold stories  
from victims that will remain unnamed.



Charming Kitten



Source: <https://www.crowdstrike.com/adversaries/>



# Who is the attacker?

---

- State-sponsored threat actors
- Cyber Criminal Organizations
- Competitors
- Hacktivists & hacktivist groups



*Be very careful of this attack vector if your organization belongs to, or supports the critical infrastructure, if handles important technology and/or research (& supply chain) or if APTs are targeting you - you an exceptionally attractive target.*



# Target Vulnerability Assessment

---

## 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 do we defend against this threat?*



# Defense – Overarching Measures

---

- Reinforce a “security mindset” within your organization.  
Utilize the group influence dynamics, start from the Executive Team / C-Suite!
- Good quality training that actively engages employees. Training that is personal, intrigues and interests them.
- Implement social engineering protocols; e.g. caller identification verification processes.
- Run exercises / attack simulations to reinforce good practices, learning & memory.
- Minimize employee decision-making and use the principle of least privilege where possible.





# Defense – High Value Targets

---

- HVT tailored training (for them & their assistants) that includes deflecting elicitation techniques.
- They understand why and learn how to implement appropriate safety measures in their private, public, & corporate lives.
- Extensive public image? Educate them on how criminals use OSINT & how they can curate the information they post.
- Conduct vulnerability assessments through open-source intelligence (OSINT). Eliminate-minimize-manage risks.



# Elicitation Techniques

---

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

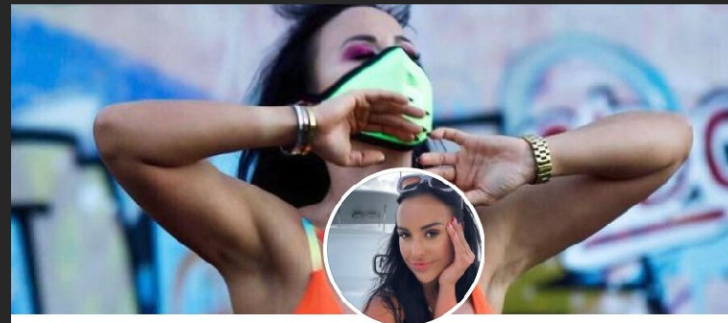
*"Flattery"*

*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.



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 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 in trouble.”*

*“I was under a lot of time  
pressure and my higher-up  
would not appreciate that  
verification call”*

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



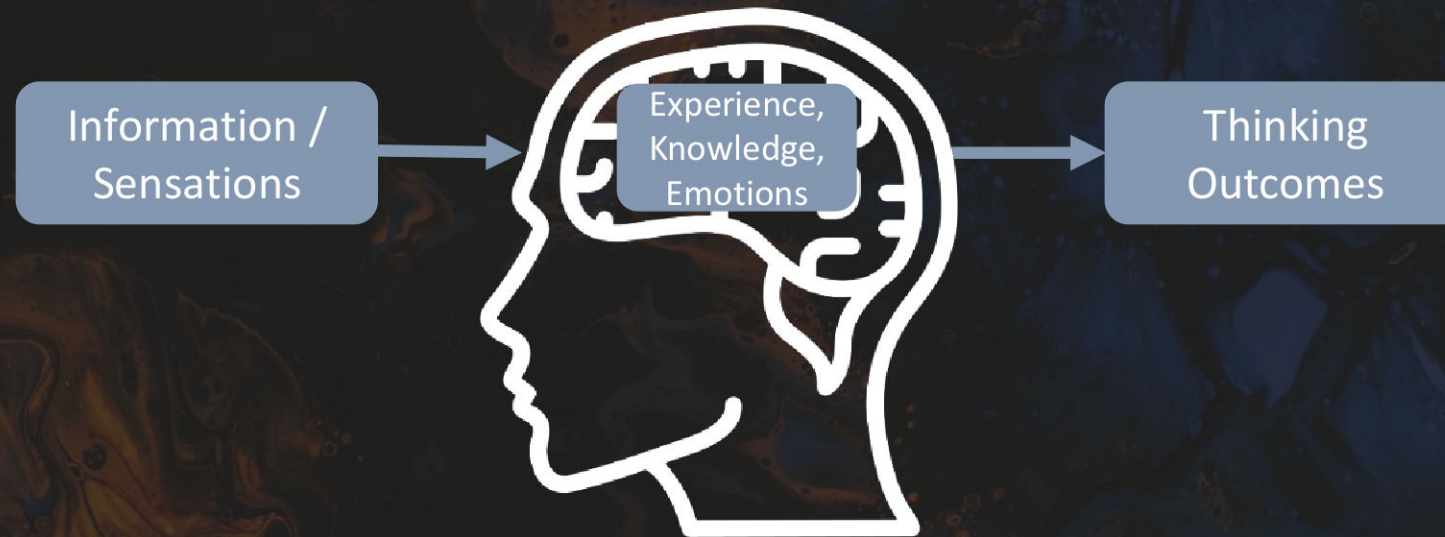
# The Good News: Neuroplasticity

---

All the above knowledge can be utilized in a defensive capacity.

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.



# Where Does Your Responsibility End?

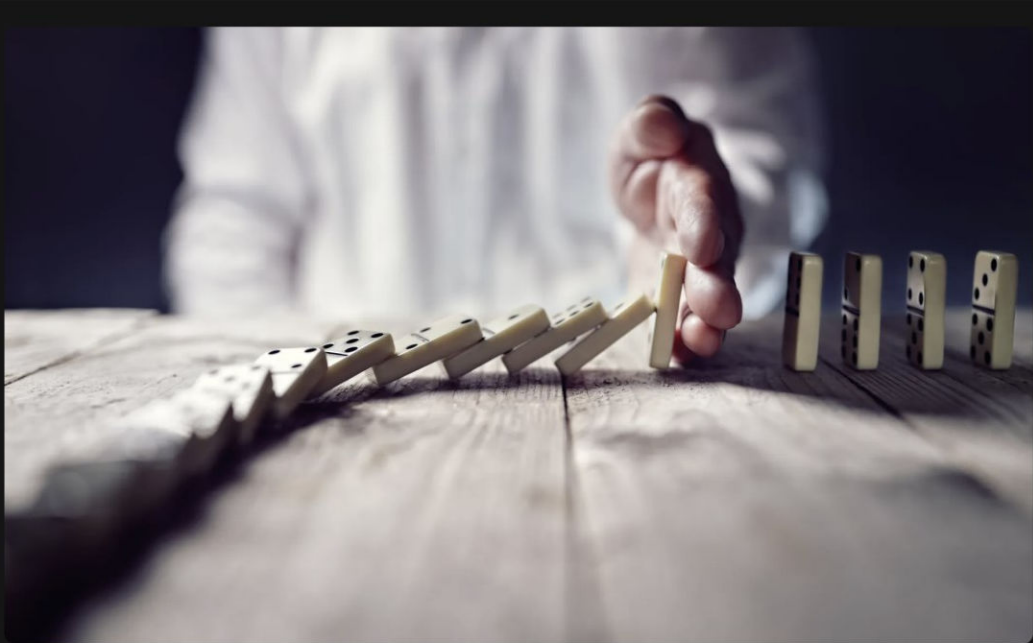
---

- People are still responsible for their own actions
- Your High Value Individual will at some point be called to respond to an attack
- BUT, do they know who the attacker is? Their tricks & tactics? Can they identify & respond to a suspicious approach? Keep their secrets, secret?
- We cannot defend against something we know almost nothing about.





# Complementary Reading



## 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>

DCSA  
<https://www.dcsa.mil>

DCSA, Counterintelligence Directorate  
<https://www.dcsa.mil/mc/ci>

Center for Development of Security Excellence  
<https://www.cdse.edu>

## ELICITATION

**BE ALERT! BE AWARE!**  
Report suspicious activities to your facility security officer

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

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