SOCIAL ENGINEERING

The Art of Human Hacking

WHAT IS IT?

- A manipulation technique that exploits human error to gain private information, access, or valuables
- Attacks can happen online, in-person, and via other interactions.
- Often the first step in a larger cyberattack

THE Social Engineering ATTACK CYCLE

01
Information gathering

This is when a threat actor does research on the target to find what weakness and medium will work best for the attack.

02
Establish a relationship

This is when the threat actor lays out the plan of attack. It could involve choosing to target a specific department with a phishing email or impersonating an assistant to the CEO with a business email compromise (BEC) attack.

03
Exploitation

This is the attack itself. It's the threat actor calling MGM's IT help desk and launching the ploy.

04
Execution

This is when success is achieved.

COMMON TYPES

Phishing

Deceptive emails or messages.

Pretexting

Use of fabricated story to gain the victim’s trust and manipulate them into giving away personal information

Tailgating

Following someone into a restricted area.

Baiting

Offering something enticing to trick the victim.

PERSONALISED ADDS

THANK YOU FOR YOUR ATTENTION

Get In Touch With Us

+420 735 312 151

hasekjachym1@gmail.com

hoeskar_jahymecek

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Tempus Közalapítvány. Neither the European Union nor the funding authority can be held responsible for them.

Az Európai Unió finanszírozásával. Az itt szereplő információk és állítások a szerző(k) álláspontját képviselik, és nem feltétlenül tükrözik az Európai Unió vagy a(z) Tempus Közalapítvány hivatalos véleményét. Sem az Európai Unió, sem a támogatást nyújtó hatóság nem vonható felelősségre miattuk.