# SOCIAL ENGINEERING

## Lirili la lira

# WHAT IS SOCIAL ENGINEERING?

The art of manipulating people into giving up confidential information or performing certain actions - often without realizing they’re being tricked.

# 1 HOW IT WORKS

instead of hacking computers, attackers “hack” human psychology.

# 2 COMMON TACTICS

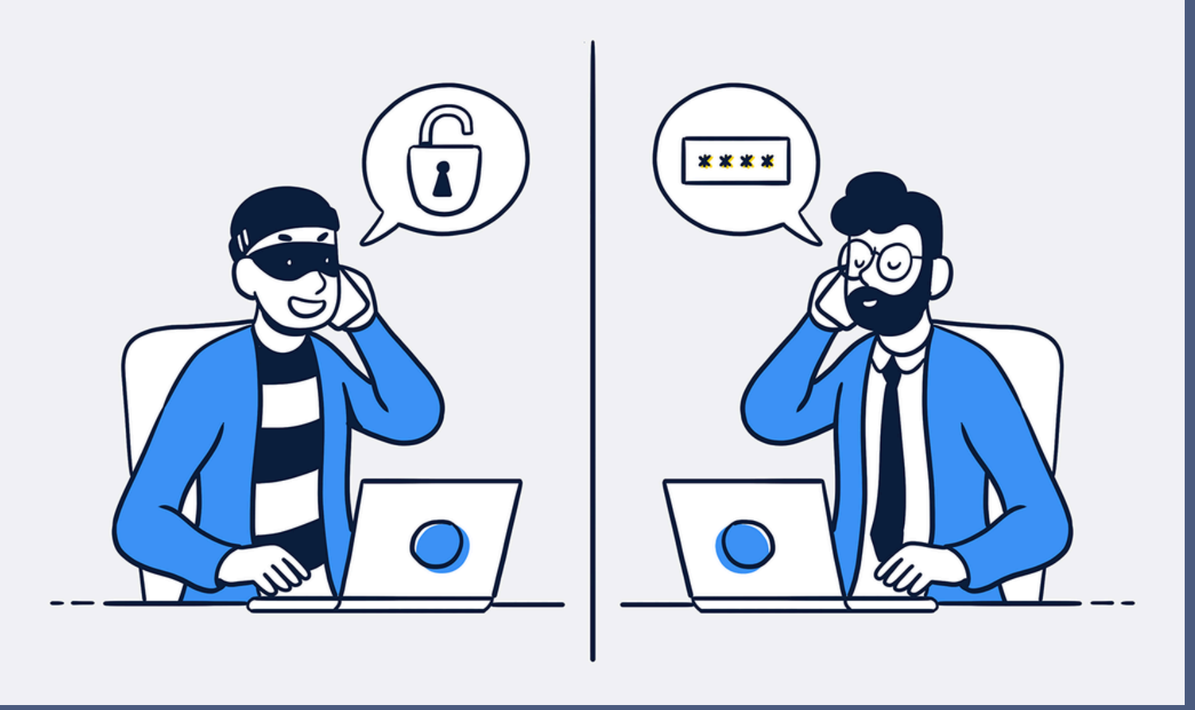
- phishing
- pretexting
- baiting
- tailgating

# 3 HOW TO PROTECT YOURSELF

- Think before you click
- Verify identities
- Use strong unique passwords and 2-factor authentication
- Stay sceptical of pressure tactics

# FINAL THOUGHTS 4

Technology isn’t always the weakest point - humans are. That’s why social engineering is so powerful and dangerous.


****


LOGIN
PASSWORD

# REAL-LIFE EXAMPLES

In 1988, Kevin Mitnick was convicted for breaking into DEC's network and copying their software, serving 12 months in prison and three years of supervised release. Near the end of his release, he hacked into Pacific Bell's voicemail systems. A warrant was issued, and he became a fugitive for two and a half years.


Kevin Mitnick
World's Most Famous Hacker
KnowBe4
CYBERCRIME MAGAZINE

# 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.