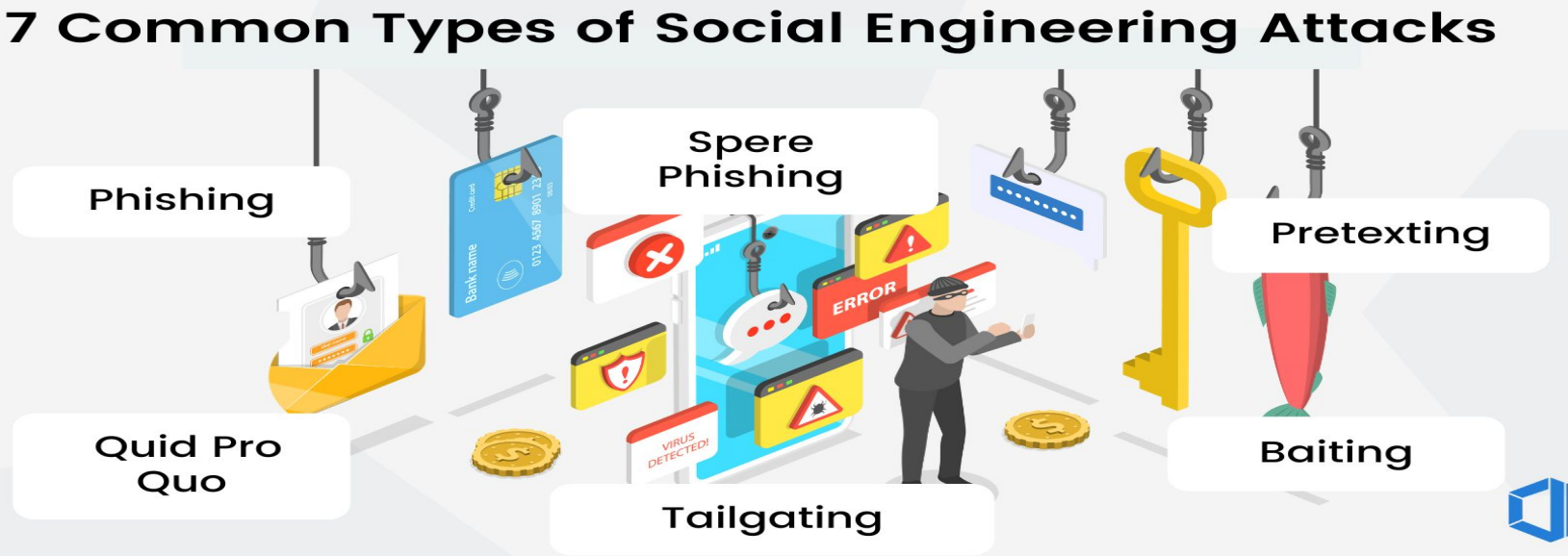
Cybersecurity and Social Engineering

Why Humans are the Weakest Link : The Psychology of social engineering

What is Social Engineering ?

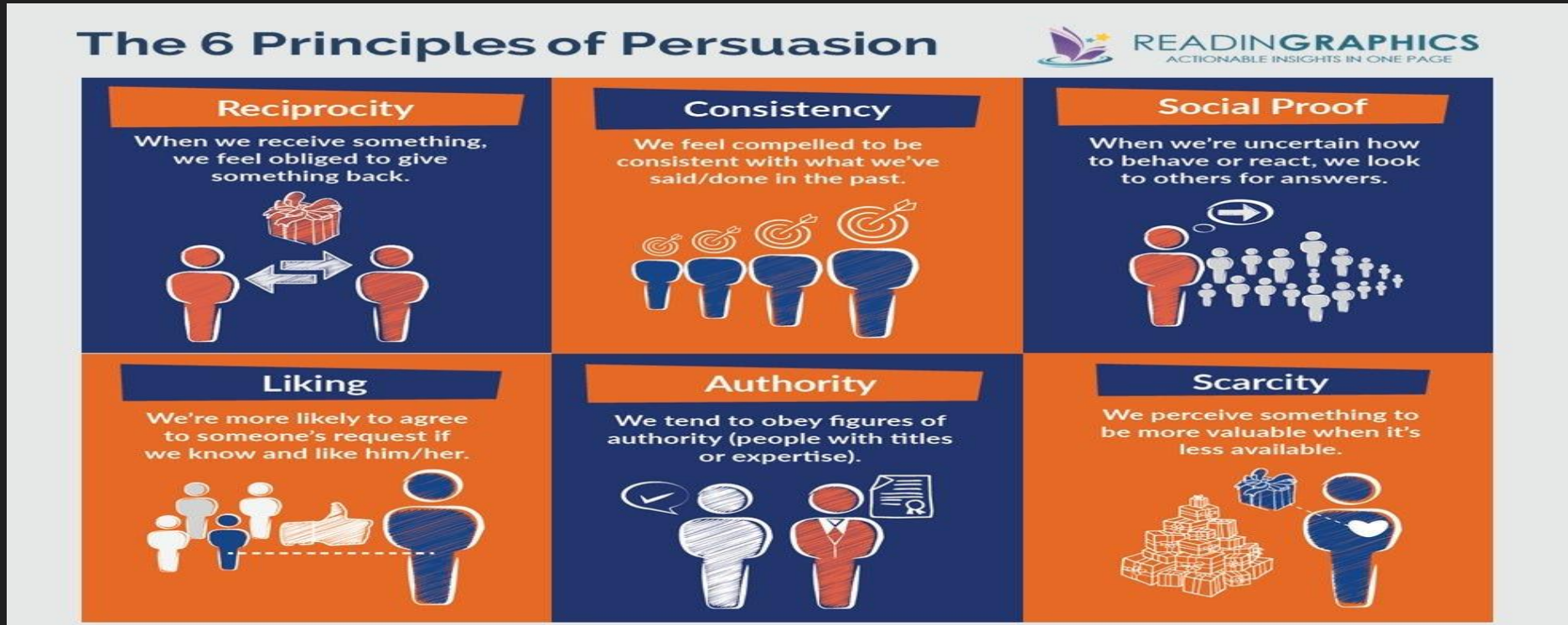
Social engineering are attacks that exploits humans rather than technology.

Common types of social engineering:



The Psychology Behind it :Why it works

Social engineers weaponize six core principles of persuasion:



Real World Examples

Twitter hack: US and UK teens arrested over breach of celebrity accounts

Three men charged in hack that saw accounts of Barack Obama, Joe Biden and Elon Musk compromised in bitcoin scam

Tech Firm Ubiquiti Suffers $46M Cyberheist

Stu Sjouwerman | Aug 7, 2015

Post Share

Brian Krebs just reported on a massive $46M Cyberheist.

Networking firm **Ubiquiti Networks Inc.** disclosed this week that cyber thieves recently stole $46.7 million using an increasingly common scam in which crooks spoof communications from executives at the victim firm in a bid to initiate unauthorized international wire transfers.

Ubiquity, a San Jose based maker of networking technology for service providers and enterprises, disclosed the attack in a quarterly financial report filed this week with the **U.S. Securities and Exchange Commission (SEC)**. The company said it discovered the fraud on June 5, 2015, and that the incident involved employee impersonation and fraudulent requests from an outside entity targeting the company's finance department.

Cyber Attack Shuts Down MGM Casinos And Resorts Across The U.S.

Vulnerability by age group

Vulnerability to social engineering scams by age group

A vulnerability heatmap offers a clear visualization of how different age groups are exposed to different social engineering attack vectors.

Age group	Tech support scams	Online shopping scams	Social media scams	Impersonation and phishing scams
18–29	Low	High	High	High
30–49	Low	High	Medium	High
50–64	Medium	Medium	Low	High
65+	High	Low	Low	High

How to Defend

Tips for avoiding a Social Engineering Attack

- **LIMIT PUBLIC INFORMATION:**
  Limit the amount of personal information that you share online.
- **BE SKEPTICAL:**
  Always question requests for sensitive information.
- **TRUST BUT VERIFY:**
  Don't share information with people you don't know unless you can verify their identity.
- **CALL THEM BACK:**
  Through the main switchboard if possible.
- **NO PASSWORDS OVER THE PHONE:**
  Never share your password with anyone over the phone.

Wordfence™

wordfence.com/learn

In conclusion

The future of cybersecurity is Humans and technology. We will never eliminate human error, but by understanding how human behaviour influence vulnerabilities, we can reduce the impact of human error and improve security.