Svitlana Samko

Decoding the Human Firewall: The Psychology Behind Social Engineering Attacks

Understanding and Mitigating Human Vulnerabilities in Cybersecurity

Svitlana Samko

18 years working experience in IT

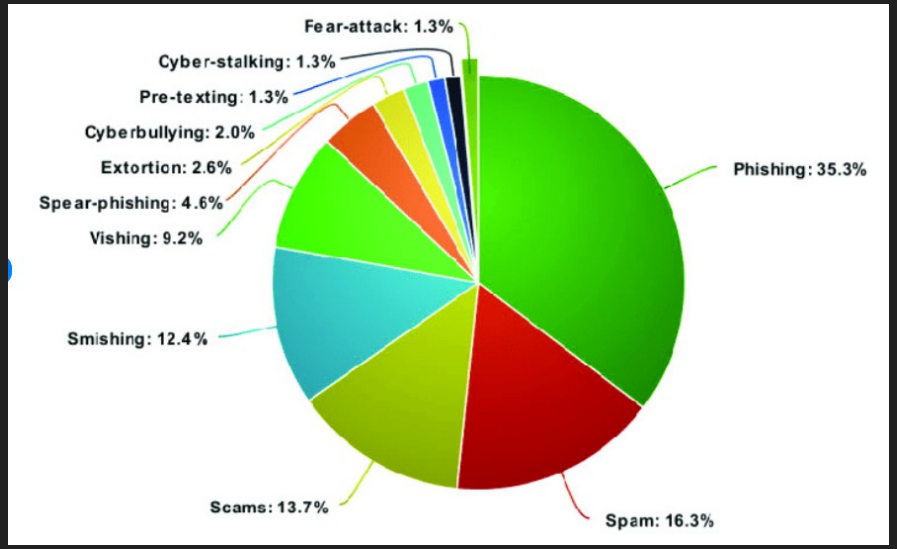
President of Toastmasters in EMEA
Verizon Online Club

Professional Mentor (>200 students,
90% are working)

https://www.linkedin.com/in/svitlana-samko/

The Prevalence of Social Engineering

Up to 98% of cyber attacks involve some form of social engineering.



Source

What is Social Engineering?

Manipulation of individuals into divulging confidential information or performing actions beneficial to the attacker.

Common Forms:

- **Phishing -** deceptive messages (usually emails) designed to trick you into revealing sensitive information or clicking malicious links.
- **Pretexting -** an attacker invents a false identity or scenario to manipulate you into sharing information or access.
- **Baiting -** luring victims with something enticing — like a free USB drive — that actually contains malware.
- **Tailgating -** a physical breach where someone sneaks into a secure area by following an authorized person.

The Human Brain: A Double-Edged Sword

Our cognitive shortcuts (heuristics) and biases can be exploited.

Authority Bias

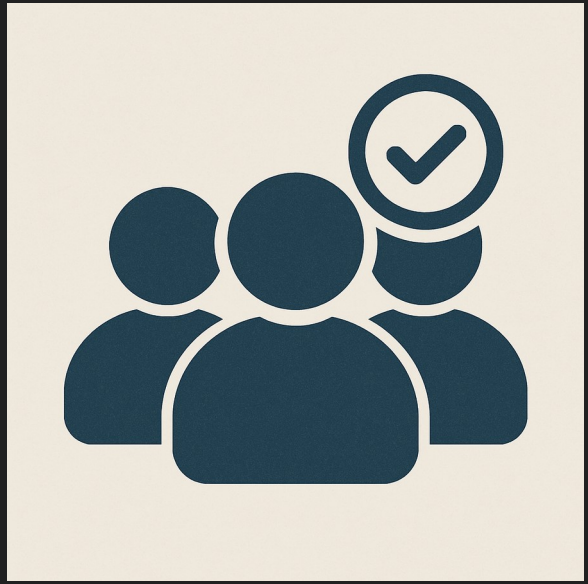
Tendency to comply with figures of authority.

Example: Employees might follow instructions from someone posing as a company executive without verification.

Social Proof Bias

Looking to others to determine correct behavior.

Example: Attackers use fake testimonials to legitimize scams.



Affect Heuristic

Making decisions based on emotions rather than logic.

Example: Clicking on a suspicious link due to excitement or fear.

Combating Psychological Manipulation

Strategies:

- Pause and Reflect: take a moment before responding to unexpected requests.
- Verify Sources: independently confirm the legitimacy of communications.
- Continuous Education: regular training on recognizing and resisting manipulation tactics.

Conclusion and Call to Action

Key Takeaway: Awareness of cognitive biases enhances our defense against social engineering.

Call to Action: Commit to questioning and verifying before acting on unsolicited requests.

The ABC of due diligence: assume nothing, believe nobody and check everything

By decoding our own minds, we fortify our defenses against manipulation.

Svitlana Samko

THANK YOU!

https://www.linkedin.com/in/svitlana-samko/