Cybersecurity and Cyber Offending

Diane Gilzow, Michaela Payne, Dymphine Ngabonziza, Kerina Drummond

April 15th, 2025

Motives for Cyber Offending

- Financial
  - According to an article, “Money is the number one motivation for the majority of hackers.”
  - Hackers are on the lookout for valuable data to sell on the dark web or companies that are willing to pay a ransom to get their data back. (upguard.com)
- How Does this Influence Cybersecurity?
  - Increase in ransomware attacks and data breaches (Data can make a lot of money)
  - Increase in scams, cyber fraud, or phishing scams to deceive people into giving away data or money.
- Because data is valuable and easy to obtain, it’s important for organizations to enhance their security measures.

Motives for Cyber Offending Contd.

- Recognition
  - “Some hackers are motivated by the sense of achievement that comes with cracking open a major system. Some may work in groups or independently, but, on some scale, they would like to be recognized” (6 motivations of Cyber Criminals).
- Insider Threats
  - “Individuals who have access to critical information or systems can easily choose to misuse that access—to the detriment of their organization” (6 motivations of Cyber Criminals).
    - “These threats can come from internal employees, vendors, a contractor or a partner—and are viewed as some of the greatest cyber security threats to organizations” (6 motivations of Cyber Criminals).
      - “However, not all insider threats are intentional, according to an Insider Threat Report from Crowd Research Partners. Most (51%) are due to carelessness, negligence, or compromised credentials, but the potential impact is still present even in an unintentional scenario” (6 motivations of Cyber Criminals).

.

Psychological Theories for Cyber Offending

- Neutralization Theory
  - Trying to justify criminal behavior in any shape or form to neutralize guilt.
- Victims can be blamed for any kind of cyberattack, such as having weak security or an inability to avoid victimization.
- Social Impact: This increases the justification for cybercrime, especially for gray hat hackers or amateurs.
  - Helps normalize cybercrime (especially in online communities)
  - Promotes a culture centered around cybercrime

Psychological Theories for Cyber Offending Contd.

Psychodynamic Theory

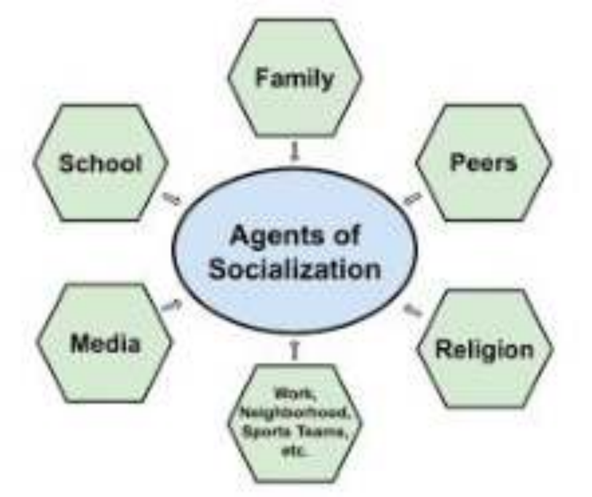
- This theory suggests that early experiences in life influence behavior
- This theory was developed by Sigmund Freud
- His theory is used to explain some types of cybercrime, including:
    - Cyberbullying
    - Child Porn
- In latent terms: What happens as a child can affect our future

Psychological Theories for Cyber Offending Contd.

Behavioral Theory

- This theory suggests behavior is learned
- These behaviors are often learned from:

1. The family
2. Schools
3. Peers
4. Mass Media
5. Environment

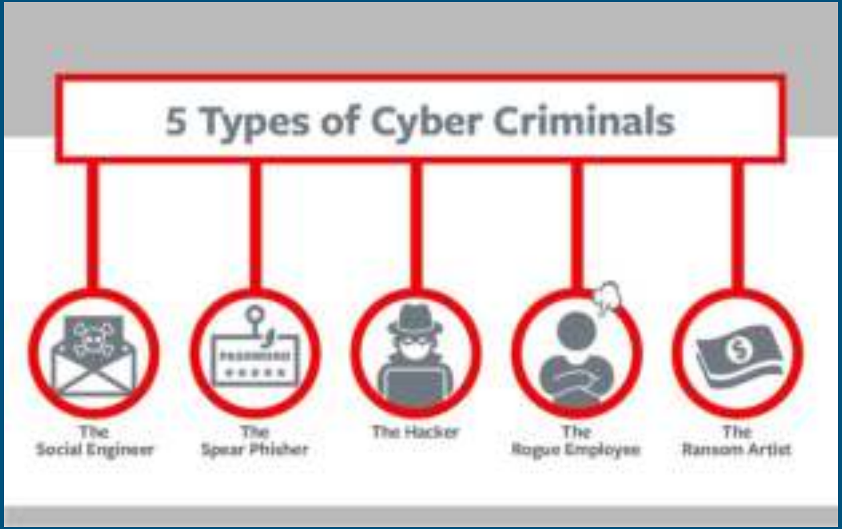


Research shows cyber criminals often weigh risk vs reward

Actions such as hacking and cyberbullying support this idea that cyber offending is learned

Cyber Victimization

- What is cyber victimization?
- Examples of cyber victimization:
  - Cyberbullying
  - Phishing scams
  - Social engineering
  - Ransomware



Cyber Victimization Contd.

- Psychological factors tend to increase one’s risk of cyber victimization
- A few psychological risks include:
  - Optimism Bias
  - Hyperbolic Discounting
  - Depression and Stress

Consequences of Cyber Victimization

- Cyber victimization can cause psychological and physical harm to the victims
  - Depression, fear, anger, embarrassment, and lack of trust are just a few psychological consequences of cyber victimization
  - Loss of money, loss of computer files/data leaks, and even cyber interference in critical infrastructure like factories and hospitals, can be a result of cyber victimization

Conclusion

Take Away: There are many reasons offenders commit cybercrimes, but no matter the reason, in order to prevent being victimized, we must stay informed and take our security into our own hands.

- Putting tools in place and being aware of what we release online are two major steps.

Tools such as firewalls, MFA, and anti-virus software can be vital to technical security, employing strong passwords, keeping SPII offline, and keeping devices updated.

References

- https://www.upguard.com/blog/finance-sector-cyber-attacks#:~:text=prevent%20cyber%20attacks%20%3E-,Why%20Do%20Cybercriminals%20Target%20the%20Financial%20Sector?,information%20and%20sending%20them%20money.
- https://www.orangecyberdefense.com/global/blog/research/we-are-not-responsible-for-that-neutralization-through-denials-of-responsibility
- https://docmckee.com/cj/docs-criminal-justice-glossary/cyber-victimization-definition/
- https://www.coretech.us/blog/6-motivations-of-cyber-criminals
- Module 5 presentation
- https://www.google.com/url?sa=i&url=https%3A%2F%2Friskandinsurance.com%2Fcyber-attacks-top-cause-of-it-downtime-for-uk-businesses%2F&psig=AOvVaw2eC6U4ZFhqm1tosYb0NND1&ust=1744320118875000&source=images&cd=vfe&opi=89978449&ved=0CBQQjRxqFwoTCPiSmo_xy4wDFQAAAAAdAAAAABAE
- https://www.google.com/url?sa=i&url=https%3A%2F%2Fdeeleyinsurance.com%2F5-types-of-cyber-criminals%2F&psig=AOvVaw1vMRGsb_oO_jUA-xXZgbrx&ust=1744321600366000&source=images&cd=vfe&opi=89978449&ved=0CBQQjRxqFwoTCOibw7z2y4wDFQAAAAAdAAAAABAE
- https://www.google.com/url?sa=i&url=https%3A%2F%2Fhsespot.com%2Fsocial-and-psychological%2F&psig=AOvVaw1yv78Q0xpCz_FQFE6KSFaf&ust=1744728884791000&source=images&cd=vfe&opi=89978449&ved=0CBQQjRxqFwoTCMD-2d7j14wDFQAAAAAdAAAAABAJ
- https://www.google.com/search?q=do+feelings+such+as+fear+and+embarassment+make+it+hard+to+report+cyber+vucitmization&oq=do+feelings+such+as+fear+and+embarassment+make+it+hard+to+report+cyber+vucitmization&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIGCAEQIRgK0gEJMTYwNDZqMGo3qAIAsAIA&sourceid=chrome&ie=UTF-8