The Social Impact Of Cybercrime

AJ Guevara

What is Cybercrime?

- Crime using computers or networks
- Computer = tool OR target
- Examples: phishing, hacking, cyberbullying

Impact On Victims

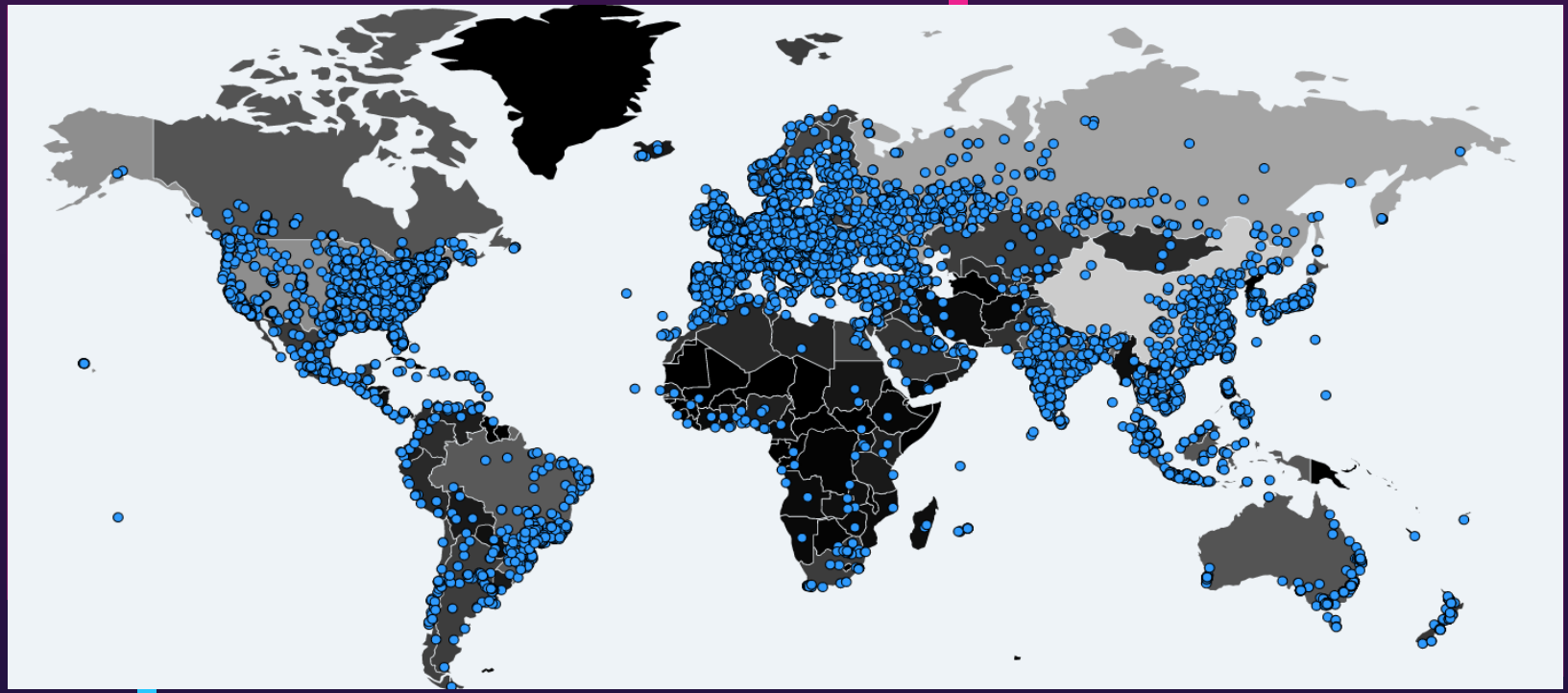
- Financial loss
- Emotional stress
- Loss of privacy
- Fear of technology

Impact on Society

- Loss of trust in technology
- Economic damage
- Spread of harmful content
- Targets vulnerable groups

Case Study

- WannaCry ransomware attack
- Affected 150+ countries
- Hospitals & businesses impacted
- Data locked for ransom



The Human Factor in Cybercrime

- Human behavior = biggest weakness
- Hackers trick people, not just systems
- Use fear, trust, and urgency
- Not knowing enough = more risk
- Being online more = more exposure

AI and the Future of Cybercrime

- AI automates attacks
- Smarter phishing emails
- Deepfakes & identity fraud
- Faster password cracking
- Harder to detect

AI References by Complaint Loss

Crime Type	Loss	Crime Type	Loss
Investment	$632,041,188	Extortion	$2,940,642
BEC	$30,256,592	Real Estate	$2,699,085
Tech/Customer Support	$19,457,078	Credit Card/Check Fraud	$1,836,105
Confidence/Romance	$19,041,653	Identity Theft	$1,643,308
Personal Data Breach	$18,767,964	Advanced Fee	$1,642,712
Employment	$12,550,185	Harassment/Stalking	$1,445,378
Other	$11,750,591	Malware	$1,248,199
Phishing/Spoofing	$10,283,732	Botnet	$697,226
IPR/Copyright and Counterfeit	$10,103,789	Charity	$531,455
Government Impersonation	$7,061,628	SIM Swap	$13,082
Lottery/Sweepstakes/ Inheritance	$4,486,965	Threats of Violence	$9,576
Data Breach	$4,319,380	Overpayment	$4,719
Non-Payment/ Non-Delivery	$3,726,777	Ransomware	$0
Descriptors			
Crimes Against Children	$9,866		
Cryptocurrency	$658,714,247		

Please see Appendix B and C for additional information related to IC3 complaint data, crime types, and descriptors.

Who is Most Vulnerable?

- Teens → cyberbullying & social pressure
- Adults → financial scams & identity theft
- Older adults → most targeted for fraud
- All groups face emotional and financial harm

Prevention Strategies

- Use strong passwords + MFA
- Don’t click suspicious links
- Don’t share personal info
- Stay aware of scams
- Practice safe online habits

Conclusion

- Cybercrime affects individuals & society
- Human behavior plays a key role
- AI increases risks
- Awareness = protection

References

- Federal Bureau of Investigation. (2025). Internet Crime Report 2025. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
- OpenLearn. (n.d.). The psychology of cybercrime. https://www.open.edu/openlearn/health-sports-psychology/psychology/the-psychology-cybercrime/content-section-3.1
- National Institute of Standards and Technology (NIST). (n.d.). Cybersecurity Framework. https://www.nist.gov/cyberframework
- Leukfeldt, R., & Holt, T. J. (2019). The human factor of cybercrime. Routledge. https://soclibrary.futa.edu.ng/books/THE%20HUMAN%20FACTOR%20OF%20CYBERCRIME%20by%20Rutger%20Leukfeldt%20and%20Thomas%20J.%20Holt%20(z-lib.org).pdf