

# IY5613: Human Aspects of Information Security and Privacy

View Online



[1]

N. S. Safa, 'Human Aspects of Information Security in Organisations', *Computer Fraud & Security*, vol. 2016, no. 2, pp. 15–18, 2016, doi: 10.1016/S1361-3723(16)30017-3.

[2]

G. M. Smith, 'Into Cerberus' Lair: Bringing the Idea of Security to Light', *The British Journal of Politics and International Relations*, vol. 7, no. 4, pp. 485–507, 2005, doi: 10.1111/j.1467-856x.2005.00204.x.

[3]

K. de Leeuw and J. A. Bergstra, *The History of Information Security: A Comprehensive Handbook*. Amsterdam: Elsevier, 2007.

[4]

K. de Leeuw and J. A. Bergstra, *The History of Information Security: A Comprehensive Handbook*. Amsterdam: Elsevier, 2007 [Online]. Available: <http://ezproxy01.rhul.ac.uk/login?url=http://www.dawsonera.com/depp/reader/protected/external/AbstractView/S9780080550589>

[5]

K. L.  
O

qvist, *Hands-On Guide to GDPR Compliance: Privacy by Design, Privacy by Default*. Portsmouth, NH: International Association for Privacy Professionals, 2018.

[6]

S. D. Warren and L. D. Brandeis, 'The Right to Privacy', *Harvard Law Review*, vol. 4, no. 5, 1890, doi: 10.2307/1321160.

[7]

T. Herath and H. R. Rao, 'Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations', *European Journal of Information Systems*, vol. 18, no. 2, pp. 106–125, 2009, doi: 10.1057/ejis.2009.6.

[8]

H. Cho, J.-S. Lee, and S. Chung, 'Optimistic Bias About Online Privacy Risks: Testing the Moderating Effects of Perceived Controllability and Prior Experience', *Computers in Human Behavior*, vol. 26, no. 5, pp. 987–995, 2010, doi: 10.1016/j.chb.2010.02.012.

[9]

B. Bulgurcu, H. Cavusoglu, and I. Benbasat, 'Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness', *MIS Quarterly*, vol. 34, no. 3, 2010, doi: 10.2307/25750690.

[10]

A. Hovav and J. D'Arcy, 'Applying an Extended Model of Deterrence Across Cultures: An Investigation of Information Systems Misuse in the U.S. and South Korea', *Information & Management*, vol. 49, no. 2, pp. 99–110, Mar. 2012, doi: 10.1016/j.im.2011.12.005.

[11]

T. Herath and H. R. Rao, 'Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness', *Decision Support Systems*, vol. 47, no. 2, pp. 154–165, 2009, doi: 10.1016/j.dss.2009.02.005. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167923609000530>

[12]

P. Ifinedo, 'Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory', *Computers & Security*, vol. 31, no. 1, pp. 83–95, 2012, doi: 10.1016/j.cose.2011.10.007. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404811001337>

[13]

M. D. Ciampa, *Security Awareness: Applying Practical Security in Your World*, Fifth edition. Australia: Cengage Learning, 2017.

[14]

M. Wilson and J. Hash, 'Building an Information Technology Security Awareness and Training Program'. [Online]. Available: [https://ws680.nist.gov/publication/get\\_pdf.cfm?pub\\_id=151287](https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=151287)

[15]

A. Adams and M. A. Sasse, 'Users Are Not the Enemy', *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999, doi: 10.1145/322796.322806.

[16]

O. T. Arıcak, Ş. Dünder, and M. Saldaña, 'Mediating Effect of Self-Acceptance Between Values and Offline/online Identity Expressions Among College Students', *Computers in Human Behavior*, vol. 49, pp. 362–374, 2015, doi: 10.1016/j.chb.2015.03.025.

[17]

S. L. Pfleeger, M. A. Sasse, and A. Furnham, 'From Weakest Link to Security Hero: Transforming Staff Security Behavior', *Journal of Homeland Security and Emergency Management*, vol. 11, no. 4, 2014, doi: 10.1515/jhsem-2014-0035. [Online]. Available: <https://discovery.ucl.ac.uk/id/eprint/1460572/2/jhsem-2014-0035.pdf>

[18]

C. Colwill, 'Human Factors in Information Security: The Insider Threat – Who Can You Trust These Days?', *Information Security Technical Report*, vol. 14, no. 4, pp. 186–196, 2009, doi: 10.1016/j.istr.2010.04.004.

[19]

K. L.  
O  
..

qvist, Hands-On Guide to GDPR Compliance: Privacy by Design, Privacy by Default. Portsmouth, NH: International Association for Privacy Professionals, 2018.

[20]

M. F. Denny, J. Fox, and T. R. Finneran, The Privacy Engineer's Manifesto: Getting From Policy to Code to QA to Value. [Place of publication not identified]: Apress Open, 2014.

[21]

D. Wright and P. de Hert, Eds., Privacy Impact Assessment, vol. volume 6. Dordrecht: Springer, 2012.

[22]

R. Clarke, 'Privacy Impact Assessment: Its Origins and Development', Computer Law & Security Review, vol. 25, no. 2, pp. 123-135, 2009, doi: 10.1016/j.clsr.2009.02.002. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0267364909000302>

[23]

A. Acquisti and J. Grossklags, 'Privacy and Rationality in Individual Decision Making', IEEE Security and Privacy Magazine, vol. 3, no. 1, pp. 26-33, 2005, doi: 10.1109/MSP.2005.22.

[24]

Johnston and Warkentin, 'Fear Appeals and Information Security Behaviors: An Empirical Study', MIS Quarterly, vol. 34, no. 3, 2010, doi: 10.2307/25750691.

[25]

R. Sharman and M. Gupta, *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*. Hershey, Pa: Information Science Reference, 2008.

[26]

M. Gupta and R. Sharman, *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*. Hershey, PA: Information Science Reference, 2009 [Online]. Available:  
<http://ezproxy01.rhul.ac.uk/login?url=http://www.dawsonera.com/depp/reader/protected/external/AbstractView/S9781605660370>

[27]

J. Magnusson, 'Intentional Decentralization and Instinctive Centralization', *Information Resources Management Journal*, vol. 26, no. 4, pp. 1-17, 2013, doi: 10.4018/irmj.2013100101. [Online]. Available:  
<https://www.igi-global.com/gateway/article/99710>

[28]

R. B. Cialdini, *Influence: The Psychology of Persuasion*, Revised edition. New York: Collins, 2007.

[29]

R. B. Cialdini, *Influence: The Psychology of Persuasion*, EPub edition. New York: Collins, 2009 [Online]. Available:  
<https://www.safaribooksonline.com/library/view/-/9780061899874/?ar>

[30]

P. O. Okenyi and T. J. Owens, 'On the Anatomy of Human Hacking', *Information Systems Security*, vol. 16, no. 6, pp. 302-314, 2007, doi: 10.1080/10658980701747237.

[31]

C. Hadnagy, *Social Engineering: The Art of Human Hacking*. John Wiley & Sons, 2010.

[32]

C. Hadnagy, *Social Engineering: The Art of Human Hacking*. Indianapolis, Ind: Wiley, 2011 [Online]. Available: <http://ezproxy01.rhul.ac.uk/login?url=http://www.dawsonera.com/depp/reader/protected/external/AbstractView/S9781118028018>

[33]

K. D. Mitnick and W. L. Simon, *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*. New York: Little, Brown, 2011.

[34]

A. Da Veiga and J. H. P. Eloff, 'A Framework and Assessment Instrument for Information Security Culture', *Computers & Security*, vol. 29, no. 2, pp. 196–207, 2010, doi: 10.1016/j.cose.2009.09.002.

[35]

P. Dourish and K. Anderson, 'Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena', *Human-Computer Interaction*, vol. 21, no. 3, pp. 319–342, 2006, doi: 10.1207/s15327051hci2103\_2.