

Steven M Furnell

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/7652633/publications.pdf>

Version: 2024-02-01

268
papers

5,814
citations

101384

36
h-index

110170

64
g-index

280
all docs

280
docs citations

280
times ranked

3289
citing authors

#	ARTICLE	IF	CITATIONS
1	Authenticating mobile phone users using keystroke analysis. <i>International Journal of Information Security</i> , 2006, 6, 1-14.	2.3	237
2	Information security policy compliance model in organizations. <i>Computers and Security</i> , 2016, 56, 70-82.	4.0	232
3	Information security conscious care behaviour formation in organizations. <i>Computers and Security</i> , 2015, 53, 65-78.	4.0	206
4	Surveying the Development of Biometric User Authentication on Mobile Phones. <i>IEEE Communications Surveys and Tutorials</i> , 2015, 17, 1268-1293.	24.8	202
5	AndroDialysis: Analysis of Android Intent Effectiveness in Malware Detection. <i>Computers and Security</i> , 2017, 65, 121-134.	4.0	182
6	Security implications of electronic commerce: a survey of consumers and businesses. <i>Internet Research</i> , 1999, 9, 372-382.	2.7	169
7	Authentication of users on mobile telephones – A survey of attitudes and practices. <i>Computers and Security</i> , 2005, 24, 519-527.	4.0	166
8	Assessing the security perceptions of personal Internet users. <i>Computers and Security</i> , 2007, 26, 410-417.	4.0	135
9	Advanced user authentication for mobile devices. <i>Computers and Security</i> , 2007, 26, 109-119.	4.0	112
10	Insider Threat Prediction Tool: Evaluating the probability of IT misuse. <i>Computers and Security</i> , 2001, 21, 62-73.	4.0	108
11	The challenges of understanding and using security: A survey of end-users. <i>Computers and Security</i> , 2006, 25, 27-35.	4.0	108
12	An integrated view of human, organizational, and technological challenges of IT security management. <i>Information Management and Computer Security</i> , 2009, 17, 4-19.	1.2	103
13	Power to the people? The evolving recognition of human aspects of security. <i>Computers and Security</i> , 2012, 31, 983-988.	4.0	96
14	D-FICCA: A density-based fuzzy imperialist competitive clustering algorithm for intrusion detection in wireless sensor networks. <i>Measurement: Journal of the International Measurement Confederation</i> , 2014, 55, 212-226.	2.5	94
15	A practical evaluation of Web analytics. <i>Internet Research</i> , 2004, 14, 284-293.	2.7	92
16	Towards Bayesian-Based Trust Management for Insider Attacks in Healthcare Software-Defined Networks. <i>IEEE Transactions on Network and Service Management</i> , 2018, 15, 761-773.	3.2	83
17	An assessment of website password practices. <i>Computers and Security</i> , 2007, 26, 445-451.	4.0	78
18	Continuous user authentication using multi-modal biometrics. <i>Computers and Security</i> , 2015, 53, 234-246.	4.0	78

#	ARTICLE	IF	CITATIONS
19	From culture to disobedience: Recognising the varying user acceptance of IT security. <i>Computer Fraud and Security</i> , 2009, 2009, 5-10.	1.3	75
20	Authentication and Supervision: A Survey of User Attitudes. <i>Computers and Security</i> , 2000, 19, 529-539.	4.0	74
21	Why users cannot use security. <i>Computers and Security</i> , 2005, 24, 274-279.	4.0	74
22	From desktop to mobile: Examining the security experience. <i>Computers and Security</i> , 2009, 28, 130-137.	4.0	72
23	A preliminary two-stage alarm correlation and filtering system using SOM neural network and K-means algorithm. <i>Computers and Security</i> , 2010, 29, 712-723.	4.0	69
24	Recognising and addressing "security fatigue"™. <i>Computer Fraud and Security</i> , 2009, 2009, 7-11.	1.3	63
25	Man-At-The-End attacks: Analysis, taxonomy, human aspects, motivation and future directions. <i>Journal of Network and Computer Applications</i> , 2015, 48, 44-57.	5.8	59
26	Beyond the PIN: Enhancing user authentication for mobile devices. <i>Computer Fraud and Security</i> , 2008, 2008, 12-17.	1.3	54
27	Computer hacking and cyber terrorism: the real threats in the new millennium?. <i>Computers and Security</i> , 1999, 18, 28-34.	4.0	53
28	A preliminary model of end user sophistication for insider threat prediction in IT systems. <i>Computers and Security</i> , 2005, 24, 371-380.	4.0	53
29	A systematic review of approaches to assessing cybersecurity awareness. <i>Kybernetes</i> , 2015, 44, 606-622.	1.2	53
30	Acceptance of Subscriber Authentication Methods For Mobile Telephony Devices. <i>Computers and Security</i> , 2002, 21, 220-228.	4.0	49
31	An Analysis of Information Security Awareness within Home and Work Environments. , 2010, , .		46
32	Enhancing security behaviour by supporting the user. <i>Computers and Security</i> , 2018, 75, 1-9.	4.0	45
33	Security beliefs and barriers for novice Internet users. <i>Computers and Security</i> , 2008, 27, 235-240.	4.0	44
34	Keystroke dynamics on a mobile handset: a feasibility study. <i>Information Management and Computer Security</i> , 2003, 11, 161-166.	1.2	43
35	A Long-Term Trial of Keystroke Profiling Using Digraph, Trigraph and Keyword Latencies. , 2004, , 275-289.		43
36	Friend-assisted intrusion detection and response mechanisms for mobile ad hoc networks. <i>Ad Hoc Networks</i> , 2008, 6, 1151-1167.	3.4	42

#	ARTICLE	IF	CITATIONS
37	Understanding the influences on information security behaviour. Computer Fraud and Security, 2012, 2012, 12-15.	1.3	37
38	Multi-modal Behavioural Biometric Authentication for Mobile Devices. International Federation for Information Processing, 2012, , 465-474.	0.4	37
39	Continuous and transparent multimodal authentication: reviewing the state of the art. Cluster Computing, 2016, 19, 455-474.	3.5	35
40	Public awareness and perceptions of biometrics. Computer Fraud and Security, 2007, 2007, 8-13.	1.3	34
41	Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions. , 2013, , .		34
42	Home working and cyber security – an outbreak of unpreparedness?. Computer Fraud and Security, 2020, 2020, 6-12.	1.3	34
43	Phishing: can we spot the signs?. Computer Fraud and Security, 2007, 2007, 10-15.	1.3	32
44	Securing the next generation: enhancing e-safety awareness among young people. Computer Fraud and Security, 2009, 2009, 13-19.	1.3	31
45	Investigating the problem of IDS false alarms: An experimental study using Snort. International Federation for Information Processing, 2008, , 253-267.	0.4	30
46	Can't get the staff? The growing need for cyber-security skills. Computer Fraud and Security, 2017, 2017, 5-10.	1.3	30
47	Identifying and predicting the factors affecting end-users' risk-taking behavior. Information and Computer Security, 2018, 26, 306-326.	1.5	30
48	Computer crime and abuse: A survey of public attitudes and awareness. Computers and Security, 1999, 18, 715-726.	4.0	29
49	End-user security culture: A lesson that will never be learnt?. Computer Fraud and Security, 2008, 2008, 6-9.	1.3	29
50	Assessing password guidance and enforcement on leading websites. Computer Fraud and Security, 2011, 2011, 10-18.	1.3	29
51	Human aspects of information security. Information Management and Computer Security, 2013, 21, 5-15.	1.2	29
52	Risk and restitution: Assessing how users establish online trust. Computers and Security, 2006, 25, 486-493.	4.0	28
53	Making security usable: Are things improving?. Computers and Security, 2007, 26, 434-443.	4.0	28
54	Selecting security champions. Computer Fraud and Security, 2011, 2011, 8-12.	1.3	28

#	ARTICLE	IF	CITATIONS
55	Information security policies: A review of challenges and influencing factors. , 2016, , .		28
56	Security education and awareness: just let them burn?. Network Security, 2017, 2017, 5-9.	0.6	28
57	Assessing the global accessibility of the Internet. Internet Research, 2002, 12, 329-338.	2.7	27
58	Security transparency: the next frontier for security research in the cloud. Journal of Cloud Computing: Advances, Systems and Applications, 2015, 4, .	2.1	27
59	Multi-dimensional personalisation for location and interest-based recommendation. Internet Research, 2004, 14, 379-385.	2.7	26
60	Information security burnout: Identification of sources and mitigating factors from security demands and resources. Journal of Information Security and Applications, 2019, 46, 96-107.	1.8	26
61	The cybersecurity workforce and skills. Computers and Security, 2021, 100, 102080.	4.0	26
62	Security literacy: the missing link in today's online society?. Computer Fraud and Security, 2014, 2014, 12-18.	1.3	25
63	Cloud Forensics: A Review of Challenges, Solutions and Open Problems. , 2015, , .		25
64	The challenge of measuring cyber-dependent crimes. Computer Fraud and Security, 2015, 2015, 5-12.	1.3	25
65	Towards an insider threat prediction specification language. Information Management and Computer Security, 2006, 14, 361-381.	1.2	24
66	A security framework for online distance learning and training. Internet Research, 1998, 8, 236-242.	2.7	23
67	A long-term trial of alternative user authentication technologies. Information Management and Computer Security, 2004, 12, 178-190.	1.2	23
68	A survey of cyber-security awareness in Saudi Arabia. , 2016, , .		23
69	Social engineering: assessing vulnerabilities in practice. Information Management and Computer Security, 2009, 17, 53-63.	1.2	22
70	E-commerce security: a question of trust. Computer Fraud and Security, 2004, 2004, 10-14.	1.3	21
71	A suspect-oriented intelligent and automated computer forensic analysis. Digital Investigation, 2016, 18, 65-76.	3.2	21
72	Enemies within: the problem of insider attacks. Computer Fraud and Security, 2004, 2004, 6-11.	1.3	20

#	ARTICLE	IF	CITATIONS
73	The Problem of False Alarms: Evaluation with Snort and DARPA 1999 Dataset. Lecture Notes in Computer Science, 2008, , 139-150.	1.0	20
74	Exploring touch-based behavioral authentication on smartphone email applications in IoT-enabled smart cities. Pattern Recognition Letters, 2021, 144, 35-41.	2.6	20
75	An investigation and survey of response options for Intrusion Response Systems (IRs). , 2010, , .		19
76	Incident prioritisation using analytic hierarchy process (AHP): Risk Index Model (RIM). Security and Communication Networks, 2013, 6, 1087-1116.	1.0	19
77	Text-Based Active Authentication for Mobile Devices. IFIP Advances in Information and Communication Technology, 2014, , 99-112.	0.5	19
78	Understanding the full cost of cyber security breaches. Computer Fraud and Security, 2020, 2020, 6-12.	1.3	19
79	A conceptual architecture for real-time intrusion monitoring. Information Management and Computer Security, 2000, 8, 65-75.	1.2	18
80	Comparing the Mobile Device Security Behavior of College Students and Information Technology Professionals. Journal of Information Privacy and Security, 2014, 10, 186-202.	0.4	18
81	A forensic acquisition and analysis system for IaaS. Cluster Computing, 2016, 19, 439-453.	3.5	18
82	Duplicitous social media and data surveillance: An evaluation of privacy risk. Computers and Security, 2020, 94, 101822.	4.0	18
83	Applications of keystroke analysis for improved login security and continuous user authentication. IFIP Advances in Information and Communication Technology, 1996, , 283-294.	0.5	18
84	Information security behavior: Recognizing the influencers. , 2017, , .		17
85	Understanding cybersecurity behavioral habits: Insights from situational support. Journal of Information Security and Applications, 2021, 57, 102710.	1.8	17
86	Biometrics – The promise versus the practice. Computer Fraud and Security, 2005, 2005, 12-16.	1.3	16
87	Authenticating ourselves: will we ever escape the password?. Network Security, 2005, 2005, 8-13.	0.6	16
88	From security policy to practice: Sending the right messages. Computer Fraud and Security, 2010, 2010, 13-19.	1.3	16
89	Improving Awareness of Social Engineering Attacks. IFIP Advances in Information and Communication Technology, 2013, , 249-256.	0.5	16
90	Transparent authentication systems for mobile device security: A review. , 2015, , .		16

#	ARTICLE	IF	CITATIONS
91	A framework for reporting and dealing with end-user security policy compliance. Information and Computer Security, 2019, 27, 2-25.	1.5	16
92	Special issue on security of IoT-enabled infrastructures in smart cities. Ad Hoc Networks, 2019, 92, 101850.	3.4	16
93	Handheld hazards: The rise of malware on mobile devices. Computer Fraud and Security, 2005, 2005, 4-8.	1.3	15
94	Routes to security compliance: be good or be shamed?. Computer Fraud and Security, 2012, 2012, 12-20.	1.3	15
95	Awareness of Mobile Device Security. International Journal of Mobile Computing and Multimedia Communications, 2016, 7, 15-31.	0.4	15
96	Security issues in Online Distance Learning. VINE: the Journal of Information and Knowledge Management Systems, 2001, 31, 28-35.	1.0	14
97	Jumping security hurdles. Computer Fraud and Security, 2010, 2010, 10-14.	1.3	14
98	Comparing intentions to use university-provided vs vendor-provided multibiometric authentication in online exams. Campus Wide Information Systems, 2011, 28, 102-113.	1.1	14
99	An empirical analysis of the information security culture key factors framework. Computers and Security, 2021, 108, 102354.	4.0	14
100	Assessing the Usability of End-User Security Software. Lecture Notes in Computer Science, 2010, , 177-189.	1.0	14
101	Achieving automated intrusion response: a prototype implementation. Information Management and Computer Security, 2006, 14, 235-251.	1.2	13
102	A new taxonomy for comparing intrusion detection systems. Internet Research, 2007, 17, 88-98.	2.7	13
103	A non-intrusive biometric authentication mechanism utilising physiological characteristics of the human head. Computers and Security, 2007, 26, 468-478.	4.0	13
104	Considering the potential of criminal profiling to combat hacking. Journal in Computer Virology, 2007, 3, 135-141.	1.9	13
105	Usability versus complexity – striking the balance in end-user security. Network Security, 2010, 2010, 13-17.	0.6	13
106	SMS linguistic profiling authentication on mobile device. , 2011, , .		13
107	Online privacy: a matter of policy?. Computer Fraud and Security, 2012, 2012, 12-18.	1.3	13
108	Password practices on leading websites – revisited. Computer Fraud and Security, 2014, 2014, 5-11.	1.3	13

#	ARTICLE	IF	CITATIONS
109	Using security. Computer Fraud and Security, 2004, 2004, 6-10.	1.3	12
110	Malicious or misinformed? Exploring a contributor to the insider threat. Computer Fraud and Security, 2006, 2006, 8-12.	1.3	12
111	Evaluating the effect of guidance and feedback upon password compliance. Computer Fraud and Security, 2017, 2017, 5-10.	1.3	12
112	Assessing website password practices “ over a decade of progress?. Computer Fraud and Security, 2018, 2018, 6-13.	1.3	12
113	Motivating Information Security Policy Compliance: Insights from Perceived Organizational Formalization. Journal of Computer Information Systems, 2022, 62, 19-28.	2.0	12
114	Realising a Push Button Modality for Video-Based Forensics. Infrastructures, 2021, 6, 54.	1.4	12
115	IDS or IPS: what is best?. Network Security, 2004, 2004, 15-19.	0.6	11
116	An automated framework for managing security vulnerabilities. Information Management and Computer Security, 2005, 13, 156-166.	1.2	11
117	Biometrics: no silver bullets. Computer Fraud and Security, 2005, 2005, 9-14.	1.3	11
118	Essential Lessons Still Not Learned? Examining the Password Practices of End-Users and Service Providers. Lecture Notes in Computer Science, 2013, , 217-225.	1.0	11
119	Co-operative user identity verification using an Authentication Aura. Computers and Security, 2013, 39, 486-502.	4.0	11
120	Replacing passwords: in search of the secret remedy. Network Security, 2006, 2006, 4-8.	0.6	10
121	LUARM. International Journal of Digital Crime and Forensics, 2011, 3, 37-49.	0.5	10
122	Assessing staff attitudes towards information security in a European healthcare establishment. Medical Informatics = Medecine Et Informatique, 1996, 21, 105-112.	0.8	9
123	Security analysers: administrator assistants or hacker helpers?. Information Management and Computer Security, 2001, 9, 93-101.	1.2	9
124	Internet threats to end-users: Hunting easy prey. Network Security, 2005, 2005, 5-9.	0.6	9
125	Cyber crime: a portrait of the landscape. Journal of Criminological Research, Policy and Practice, 2019, 5, 13-26.	0.2	9
126	A generic methodology for health care data security. Medical Informatics = Medecine Et Informatique, 1994, 19, 229-245.	0.8	8

#	ARTICLE	IF	CITATIONS
127	Computer abuse: vandalizing the information society. Internet Research, 1997, 7, 61-66.	2.7	8
128	Security Policy Enforcement in BPEL-Defined Collaborative Business Processes. , 2007, , .		8
129	A comparison of website user authentication mechanisms. Computer Fraud and Security, 2007, 2007, 5-9.	1.3	8
130	Online addiction. , 2010, , .		8
131	Establishing A Personalized Information Security Culture. International Journal of Mobile Computing and Multimedia Communications, 2011, 3, 63-79.	0.4	8
132	A study on improving security warnings. , 2014, , .		8
133	Secure Graphical One Time Password (GOTPass): An Empirical Study. Information Security Journal, 2015, 24, 207-220.	1.3	8
134	The usability of security “ revisited. Computer Fraud and Security, 2016, 2016, 5-11.	1.3	8
135	Addressing cyber security skills: the spectrum, not the silo. Computer Fraud and Security, 2020, 2020, 6-11.	1.3	8
136	A Novel Behaviour Profiling Approach to Continuous Authentication for Mobile Applications. , 2019, , .		8
137	Assessing website password practices “ Unchanged after fifteen years?. Computers and Security, 2022, 120, 102790.	4.0	8
138	Strategies for content migration on the World Wide Web. Internet Research, 1999, 9, 25-34.	2.7	7
139	Informing the decision process in an automated intrusion response system. Information Security Technical Report, 2005, 10, 150-161.	1.3	7
140	Gâ€ROME: semanticâ€driven capacity sharing among P2P networks. Internet Research, 2007, 17, 7-20.	2.7	7
141	The irreversible march of technology. Information Security Technical Report, 2009, 14, 176-180.	1.3	7
142	Factors for Measuring Password-Based Authentication Practices. Journal of Information Privacy and Security, 2014, 10, 71-94.	0.4	7
143	Awareness, behaviour and culture: The ABC in cultivating security compliance. , 2015, , .		7
144	An Identification of Variables Influencing the Establishment of Information Security Culture. Lecture Notes in Computer Science, 2015, , 436-448.	1.0	7

#	ARTICLE	IF	CITATIONS
145	Password meters: inaccurate advice offered inconsistently?. Computer Fraud and Security, 2019, 2019, 6-14.	1.3	7
146	Getting caught in the phishing net. Network Security, 2004, 2004, 14-18.	0.6	6
147	Securing the home worker. Network Security, 2006, 2006, 6-12.	0.6	6
148	It's a jungle out there: Predators, prey and protection in the online wilderness. Computer Fraud and Security, 2008, 2008, 3-6.	1.3	6
149	Assessing image-based authentication techniques in a web-based environment. Information Management and Computer Security, 2010, 18, 43-53.	1.2	6
150	Online identity: Giving it all away?. Information Security Technical Report, 2010, 15, 42-46.	1.3	6
151	Social networks " access all areas?. Computer Fraud and Security, 2011, 2011, 14-19.	1.3	6
152	Approach to the Evaluation of a Method for the Adoption of Information Technology Governance, Risk Management and Compliance in the Swiss Hospital Environment. , 2012, , .		6
153	User profiling from network traffic via novel application-level interactions. , 2016, , .		6
154	Privacy risk and the use of Facebook Apps: A gender-focused vulnerability assessment. Computers and Security, 2020, 96, 101866.	4.0	6
155	Biometrically Linking Document Leakage to the Individuals Responsible. Lecture Notes in Computer Science, 2018, , 135-149.	1.0	6
156	Evaluation of Contextual and Game-Based Training for Phishing Detection. Future Internet, 2022, 14, 104.	2.4	6
157	The Resource Locator Service: fixing a flaw in the web. Computer Networks, 2001, 37, 307-330.	3.2	5
158	Securing mobile devices: technology and attitude. Network Security, 2006, 2006, 9-13.	0.6	5
159	Considering the Usability of End-User Security Software. International Federation for Information Processing, 2006, , 307-316.	0.4	5
160	Vulnerability management: an attitude of mind?. Network Security, 2010, 2010, 4-8.	0.6	5
161	Still on the hook: the persistent problem of phishing. Computer Fraud and Security, 2013, 2013, 7-12.	1.3	5
162	Biometrics: making the mainstream. Biometric Technology Today, 2014, 2014, 5-9.	0.7	5

#	ARTICLE	IF	CITATIONS
163	The Current Use of Authentication Technologies: An Investigative Review. , 2015, , .		5
164	Graphical One-Time Password (GOTPass): A usability evaluation. Information Security Journal, 2016, 25, 94-108.	1.3	5
165	A novel transparent user authentication approach for mobile applications. Information Security Journal, 2018, 27, 292-305.	1.3	5
166	A heuristics for HTTP traffic identification in measuring user dissimilarity. Human-Intelligent Systems Integration, 2020, 2, 17-28.	1.2	5
167	A National Certification Programme for Academic Degrees in Cyber Security. IFIP Advances in Information and Communication Technology, 2018, , 133-145.	0.5	5
168	Personalising Security Education: Factors Influencing Individual Awareness and Compliance. Communications in Computer and Information Science, 2019, , 189-200.	0.4	5
169	Poster: The Need for a Collaborative Approach to Cyber Security Education. , 2021, , .		5
170	Hacking begins at home. Computer Fraud and Security, 2004, 2004, 4-7.	1.3	4
171	Qualified to help: In search of the skills to ensure security. Computer Fraud and Security, 2004, 2004, 10-14.	1.3	4
172	Considering the security challenges in consumer-oriented ecommerce. , 0, , .		4
173	Taking responsibility for online protection â€“ why citizens have their part to play. Computer Fraud and Security, 2007, 2007, 8-13.	1.3	4
174	Testing our defences or defending our tests: the obstacles to performing security assessment references. Computer Fraud and Security, 2008, 2008, 8-12.	1.3	4
175	The security and privacy impact of criminalising the distribution of hacking tools. Computer Fraud and Security, 2008, 2008, 9-16.	1.3	4
176	Who guides the little guy? Exploring security advice and guidance from retailers and ISPs. Computer Fraud and Security, 2008, 2008, 6-10.	1.3	4
177	Scare tactics â€“ A viable weapon in the security war?. Computer Fraud and Security, 2009, 2009, 6-10.	1.3	4
178	The price of patching. Computer Fraud and Security, 2014, 2014, 8-13.	1.3	4
179	Security, Privacy and Usability â€“ A Survey of Usersâ€™ Perceptions and Attitudes. Lecture Notes in Computer Science, 2015, , 153-168.	1.0	4
180	A Forensic Acquisition and Analysis System for IaaS: Architectural Model and Experiment. , 2016, , .		4

#	ARTICLE	IF	CITATIONS
181	Insider Misuse Attribution using Biometrics. , 2017, , .		4
182	Multi-Platform Authorship Verification. , 2019, , .		4
183	Insider Threat Specification as a Threat Mitigation Technique. Advances in Information Security, 2010, , 219-244.	0.9	4
184	A Response Strategy Model for Intrusion Response Systems. International Federation for Information Processing, 2012, , 573-578.	0.4	4
185	Collaborative Cybersecurity Learning: Establishing Educator and Learner Expectations and Requirements. IFIP Advances in Information and Communication Technology, 2022, , 46-59.	0.5	4
186	The Importance of the Job Role in Social Media Cybersecurity Training. , 2022, , .		4
187	A web-based resource migration protocol using WebDAV. , 2002, , .		3
188	Vulnerability exploitation: the problem of protecting our weakest links. Computer Fraud and Security, 2003, 2003, 12-15.	1.3	3
189	The effects of audio and video correlation and lip synchronization. Campus Wide Information Systems, 2003, 20, 159-166.	1.1	3
190	Helping us to help ourselves. Network Security, 2004, 2004, 7-12.	0.6	3
191	Malware comes of age: The arrival of the true computer parasite. Network Security, 2004, 2004, 11-15.	0.6	3
192	IT Governance and Its Impact on the Swiss Healthcare. , 2010, , .		3
193	Managing privacy settings: lots of options, but beyond control?. Computer Fraud and Security, 2015, 2015, 8-13.	1.3	3
194	An analysis of home user security awareness & education. , 2017, , .		3
195	Identity-as-a-Service: An Adaptive Security Infrastructure and Privacy-Preserving User Identity for the Cloud Environment. Future Internet, 2019, 11, 116.	2.4	3
196	Organizational formalization and employee information security behavioral intentions based on an extended TPB model. , 2019, , .		3
197	A novel approach for improving information security management and awareness for home environments. Information and Computer Security, 2021, 29, 25-48.	1.5	3
198	Pandemic Parallels: What Can Cybersecurity Learn From COVID-19?. Computer, 2021, 54, 68-72.	1.2	3

#	ARTICLE	IF	CITATIONS
199	From Passwords to Biometrics: In Pursuit of a Panacea. Communications in Computer and Information Science, 2015, , 3-15.	0.4	3
200	Malware. , 2006, , 27-54.		3
201	E-Commerce Security. , 2006, , 131-149.		3
202	Improving Security Awareness through Computer-Based Training. IFIP Advances in Information and Communication Technology, 2003, , 287-301.	0.5	3
203	A Holistic View of Cybersecurity Education Requirements. , 2022, , 289-307.		3
204	The ISHTAR guidelines for healthcare security. Health Informatics Journal, 1998, 4, 179-183.	1.1	2
205	Endpoint study of Internet paths and Web pages transfers. Campus Wide Information Systems, 2003, 20, 90-97.	1.1	2
206	A model for monitoring and migrating Web resources. Campus Wide Information Systems, 2003, 20, 67-74.	1.1	2
207	Usability pitfalls in Wireless LAN security. Network Security, 2006, 2006, 4-8.	0.6	2
208	Safety in numbers? Early experiences in the age of chip and PIN. Computer Fraud and Security, 2006, 2006, 4-7.	1.3	2
209	Identity impairment: The problems facing victims of identity fraud. Computer Fraud and Security, 2007, 2007, 6-11.	1.3	2
210	The Research on a Patch Management System for Enterprise Vulnerability Update. , 2009, , .		2
211	A distributed and cooperative user authentication framework. , 2010, , .		2
212	Getting past passwords. Computer Fraud and Security, 2013, 2013, 8-13.	1.3	2
213	A response selection model for intrusion response systems: Response Strategy Model (RSM). Security and Communication Networks, 2014, 7, 1831-1848.	1.0	2
214	A Comprehensive Framework for Understanding Security Culture in Organizations. IFIP Advances in Information and Communication Technology, 2019, , 143-156.	0.5	2
215	Comparing the protection and use of online personal information in South Africa and the United Kingdom in line with data protection requirements. Information and Computer Security, 2019, 28, 399-422.	1.5	2
216	Passwords a Lesson in Cyber Security Failure?. Itnow, 2020, 62, 26-27.	0.1	2

#	ARTICLE	IF	CITATIONS
217	Security Fatigue. , 2021, , 1-5.		2
218	Disadvantaged by Disability: Examining the Accessibility of Cyber Security. Lecture Notes in Computer Science, 2021, , 197-212.	1.0	2
219	Operational Characteristics of an Automated Intrusion Response System. Lecture Notes in Computer Science, 2003, , 65-75.	1.0	2
220	Exploring Trust, Security and Privacy in Digital Business. Lecture Notes in Computer Science, 2009, , 191-210.	1.0	2
221	A Novel Security Architecture for a Space-Data DTN. Lecture Notes in Computer Science, 2012, , 342-349.	1.0	2
222	The Design and Evaluation of a User-Centric Information Security Risk Assessment and Response Framework. International Journal of Advanced Computer Science and Applications, 2018, 9, .	0.5	2
223	Establishing a Personalized Information Security Culture. , 0, , 53-69.		2
224	Preventative Actions for Enhancing Online Protection and Privacy. International Journal of Information Technologies and Systems Approach, 2011, 4, 1-11.	0.8	2
225	Toward an Automatic Classification of Negotiation Styles Using Natural Language Processing. Lecture Notes in Computer Science, 2017, , 339-342.	1.0	2
226	A Framework for Role-Based Monitoring of Insider Misuse. , 2004, , 51-65.		1
227	Cybercrime: The Transformation of Crime in the Information Age “ By D.S. Wall. British Journal of Sociology, 2008, 59, 177-179.	0.8	1
228	Mac security: An Apple that can't be bitten?. Network Security, 2010, 2010, 7-11.	0.6	1
229	Multifactor graphical passwords: An assessment of end-user performance. , 2011, , .		1
230	Disguising the dangers: hiding attacks behind modern masks. Computer Fraud and Security, 2012, 2012, 9-13.	1.3	1
231	A Technology Independent Security Gateway for Real-Time Multimedia Communication. Lecture Notes in Computer Science, 2013, , 14-25.	1.0	1
232	A forensic acquisition based upon a cluster analysis of non-volatile memory in IaaS. , 2017, , .		1
233	A novel multimedia-forensic analysis tool (M-FAT). , 2017, , .		1
234	What Parts of Usable Security Are Most Important to Users?. IFIP Advances in Information and Communication Technology, 2021, , 126-139.	0.5	1

#	ARTICLE	IF	CITATIONS
235	Information Security and Privacy â€œ Challenges and Outlook. IFIP Advances in Information and Communication Technology, 2021, , 383-401.	0.5	1
236	Facing up to security and privacy in online meetings. Network Security, 2021, 2021, 7-13.	0.6	1
237	The 4th International Network Conference (INC 2004). Internet Research, 2004, 14, .	2.7	1
238	Investigating and Evaluating Behavioural Profiling and Intrusion Detection Using Data Mining. Lecture Notes in Computer Science, 2001, , 153-158.	1.0	1
239	A Practical Usability Evaluation of Security Features in End-User Applications. International Federation for Information Processing, 2007, , 205-216.	0.4	1
240	Assessing the Feasibility of Security Metrics. Lecture Notes in Computer Science, 2013, , 149-160.	1.0	1
241	A Holistic View of Cybersecurity Education Requirements. Advances in Information Security, Privacy, and Ethics Book Series, 2019, , 1-18.	0.4	1
242	Security Usability Challenges for End-Users. , 0, , 196-219.		1
243	Benchmarking Consumer Data and Privacy Knowledge in Connected and Autonomous Vehicles. , 2022, , .		1
244	Development of security guidelines for existing healthcare systems. Medical Informatics = Medecine Et Informatique, 1995, 20, 139-148.	0.8	0
245	When vulnerability reports can work against us. Network Security, 2004, 2004, 11-15.	0.6	0
246	Analysis of securityâ€™relevant semantics of BPEL in crossâ€™domain defined business processes. Information Management and Computer Security, 2007, 15, 116-127.	1.2	0
247	Self-preservation among online prey. Computer Fraud and Security, 2008, 2008, 9-12.	1.3	0
248	Neural Network Estimation of TCP Performance. , 2008, , .		0
249	Automated Precautionary Measures for Managing System Security Vulnerabilities. , 2009, , .		0
250	Editorial for Security and Privacy in Wireless Networks Special Issue. Mobile Networks and Applications, 2013, 18, 664-665.	2.2	0
251	Performance evaluation of a Technology Independent Security Gateway for Next Generation Networks. , 2014, , .		0
252	Investigating the Viability of Multifactor Graphical Passwords for User Authentication. Information Security Journal, 2014, 23, 10-21.	1.3	0

#	ARTICLE	IF	CITATIONS
253	Proactive biometric-enabled forensic imprinting. , 2016, , .		0
254	The Current Situation of Insider Threats Detection: An Investigative Review. , 2018, , .		0
255	Automated Trust Negotiation for Cloud Applications in Identity-as-a-Service. , 2019, , .		0
256	Efficient Privacy-preserving User Identity with Purpose-based Encryption. , 2019, , .		0
257	Information Security Risk Communication: A User-Centric Approach. , 2019, , .		0
258	Malware. , 2008, , 147-169.		0
259	Preventative Actions for Enhancing Online Protection and Privacy. , 2012, , 226-236.		0
260	An Expert Panel Approach on Developing a Unified System Authentication Benchmarking Index. International Journal of Interdisciplinary Telecommunications and Networking, 2013, 5, 32-42.	0.2	0
261	Assessing the provision of public-facing cybersecurity guidance for end-users. , 2020, , .		0
262	Network Security Intelligence Centres for Information Security Incident Management. Advances in Intelligent Systems and Computing, 2021, , 270-282.	0.5	0
263	Education for the Multifaith Community of Cybersecurity. IFIP Advances in Information and Communication Technology, 2020, , 32-45.	0.5	0
264	Preventative Actions for Enhancing Online Protection and Privacy. , 0, , 1397-1407.		0
265	Pre-execution Security Policy Assessment of Remotely Defined BPEL-Based Grid Processes. Lecture Notes in Computer Science, 2007, , 178-189.	1.0	0
266	Building a Trusted Community for Mobile Ad Hoc Networks Using Friend Recommendation. , 2007, , 129-141.		0
267	Assessing cyber security consumer support from technology retailers. Computer Fraud and Security, 2022, 2022, .	1.3	0
268	From Cybersecurity Hygiene to Cyber Well-Being. Lecture Notes in Computer Science, 2022, , 124-134.	1.0	0