Gianluca Stringhini

✉ gian (at) bu.edu

Associate Professor in the
Department of Electrical and Computer Engineering
at Boston University

Positions

5/2023-Present **Associate Professor**, *Boston University*, Boston, MA.
Department of Electrical and Computer Engineering

- Affiliated Faculty, Department of Computer Science (2018-Present)
- Affiliated Faculty, Faculty of Computing and Data Sciences (2021-Present)
- Affiliated Faculty, Center for Information Systems & Engineering (2023-Present)
- Affiliated Faculty, Hariri Institute for Computing (2020-Present)
- Affiliated Faculty, Center for Emerging and Infectious Diseases (2021-Present)
- Affiliated Faculty, Center for Antiracist Research (2020-Present)

9/2018-5/2023 **Assistant Professor**, *Boston University*, Boston, MA.
Department of Electrical and Computer Engineering

10/2017-8/2018 **Senior Lecturer (Associate Professor)**, *University College London*, London, United Kingdom.
Joint appointment in the Departments of Computer Science and Security and Crime Science

9/2014-9/2017 **Lecturer (Assistant Professor)**, *University College London*, London, United Kingdom.
Joint appointment in the Departments of Computer Science and Security and Crime Science

Education

2009-2014 **PhD in Computer Science**, *University of California Santa Barbara*, Santa Barbara, CA.
Dissertation title: "Stepping Up the Cybersecurity Game: Protecting Online Services from Malicious Activity" – Advisors Christopher Kruegel and Giovanni Vigna

2014 **MS in Computer Science**, *University of California Santa Barbara*, Santa Barbara, CA.

2006-2009 **Laurea Specialistica in Computer Engineering (MS equivalent)**, *Università degli Studi di Genova*, Genova, Italy.
Thesis title: "A Distributed System for Intrusion Prevention"

2003-2006 **Laurea Triennale in Computer Engineering (BS equivalent)**, *Università degli Studi di Genova*, Genova, Italy.
Thesis title: "Computer Security in a Linux System" (in Italian)

Awards

At Boston University

2024 **Honorable Mention**, *ACM CHI Conference on Human Factors in Computing Systems (CHI)*.
Award for the paper "Systemization of Knowledge (SoK): Creating a Research Agenda for Human-Centered Real-Time Risk Detection on Social Media Platforms"

2023 **Impact Recognition**, *ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW)*.
Award for the paper "Sliding into My DMs: Detecting Uncomfortable or Unsafe Sexual Risk Experiences within Instagram Direct Messages Grounded in the Perspective of Youth"

2023 **Finalist**, *CSAW Europe Best Applied Research Award*.
Nomination for the paper "Why So Toxic? Measuring and Triggering Toxic Behavior in Open-Domain Chatbots"

2023 **Senior Member**, *Association for Computing Machinery (ACM)*.

2022 **Honorable Mention**, *ACM SIGSAC Conference on Computer and Communications Security (CCS)*.
Award for the paper "Why So Toxic? Measuring and Triggering Toxic Behavior in Open-Domain Chatbots"

2022 **Honorable Mention**, *ACM CHI Conference on Human Factors in Computing Systems (CHI)*.
Award for the paper "Understanding the Digital Lives of Youth: Analyzing Media Shared within Safe Versus Unsafe Private Conversations on Instagram"

2022 **ECE Teaching Excellence Award**, *BU Department of Electrical and Computer Engineering*.

2022 **Early Career Excellence in Research**, *BU College of Engineering*.

2022 **Civic Tech Fellow**, *BU Faculty of Computing & Data Sciences*.

2021 **Honorable Mention**, *ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW)*.
Award for the paper "Does Platform Migration Compromise Content Moderation? Evidence from r/The_Donald and r/Incels"

2021 **Impact Recognition**, *ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW)*.
Award for the paper "I'm a Professor, which isn't usually a dangerous job: Internet-Facilitated Harassment and its Impact on Researchers"

2020 **NSF CAREER Award**, *National Science Foundation*.

2020 **Honorable Mention**, *AAAI International Conference on Web and Social Media*.
Award for the paper "Disturbed YouTube for Kids: Characterizing and Detecting Inappropriate Videos Targeting Young Children"

2019 **Junior Faculty Fellow**, *Hariri Institute for Computing and Computational Science & Engineering*.

2019 **Best Paper Award**, *Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*.
Award for the paper "On the Perils of Leaking Referrers in Online Collaboration Services"

2019 **Best Paper Award**, *Workshop on Computational Methods in Online Misbehavior (CYBERSAFETY)*.
Award for the paper "Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web"

2018 **Distinguished Paper Award**, *ACM SIGCOMM Internet Measurement Conference*.
Award for the paper "On the Origin of Memes by Means of Fringe Web Communities"

2018 **Secure the Internet Grant**, *Facebook Inc*.

At University College London

2018 **Finalist**, *CSAW Europe Best Applied Research Award*.
Nomination for the paper "Tiresias: Predicting Security Events Through Deep Learning"

| 2016-2018 | **UCLU Student Choice Teaching Awards (Nominee)**, *University College London Union*. |
| 2017 | **Second Place**, *CSAW Europe Best Applied Research Award*. |

Award for the paper "MaMaDroid: Detecting Android Malware by Building Markov Chains of Behavioral Models"

| 2017 | **Finalist**, *CSAW Europe Best Applied Research Award*. |

Nomination for the paper "What Happens After You Are Pwnd: Understanding The Use of Leaked Webmail Credentials In The Wild"

| 2017 | **Finalist**, *CSAW North America Best Applied Research Award*. |

Nomination for the paper "PayBreak: Defense against Cryptographic Ransomware"

| 2017 | **Best Paper Nominee**, *International Conference on Web and Social Media (ICWSM)*. |

Nomination for the paper "Kek, Cucks, and God Emperor Trump: A Measurement Study of 4chan's Politically Incorrect Forum and Its Effects on the Web"

| 2017 | **Best Paper Award**, *APWG eCrime Symposium*. |

Award for the paper "All Your Cards Are Belong To Us: Understanding Online Carding Forums"

| 2016 | **Future Leaders in Engineering and Physical Sciences**, *University College London*. |
| 2015 | **Google Research Award**, *Google Inc.*. |

At UC Santa Barbara

2014	**Outstanding Dissertation Award**, *Department of Computer Science, UC Santa Barbara*.
2012	**Symantec Research Labs Graduate Fellowship**, *Symantec Corp.*
2010	**Best Student Paper Award**, *Annual Computer Security Applications Conference (ACSAC)*.

Award for the paper "Detecting Spammers on Social Networks"

▬▬▬▬ Funding

Total amount of funding at BU: $5,265,762
Personal share of funding at BU: $3,225,344

At Boston University - PI

2024-2026	**NSF Secure and Trustworthy Cyberspace (SaTC)**, *Collaborative Research: SaTC: CORE: Small: Research on Concurrent Inauthentic Account and Narrative Detection (PI, $600,000, BU share $175,000)*, Co-PIs Jeremy Blackburn (Binghamton University), Jeremiah Onaolapo (University of Vermont).
2024-2027	**NSF Secure and Trustworthy Cyberspace (SaTC)**, *SaTC: CORE: Small: Enabling the Automated Delivery of Context-Aware Notifications (PI, $599,996)*.
2023-2027	**NSF Secure and Trustworthy Cyberspace (SaTC)**, *Collaborative Research: SaTC: TTP: Medium: iDRAMA.cloud: A Platform for Measuring and Understanding Information Manipulation (PI, $1,169,290, BU share $494,291)*, Lead PI Jeremy Blackburn (Binghamton University).
2022	**Google ASPIRE Fund Award**, *Measuring the Evolution and Migration of Android Malware (PI, $105,000, BU share $52,500)*, Co-PI Adam Aviv (George Washington University).
2021-2023	**NSF Secure and Trustworthy Cyberspace (SaTC)**, *Collaborative Research: SaTC: CORE: Small: Detecting Accounts Involved in Influence Campaigns on Social Media (PI, $500,000, BU share $280,000)*, Co-PI Jeremy Blackburn (SUNY Binghamton).

2021-2023 **NSF Secure and Trustworthy Cyberspace (SaTC)**, *Collaborative Research: SaTC: CORE: Small: Flanker: Automatically Detecting Lateral Movement in Organizations Using Heterogeneous Data and Graph Representation Learning (PI, $500,000, BU share $250,000)*, Lead PI Engin Kirda (Northeastern University).

2021 **Instagram Request for proposals on Safety and Community Health**, *Towards Proactive Moderation of Coordinated Harassment on Instagram (PI, $50,000 – Research Gift)*.

2021 **Media Ecosystems Analysis Group**, *Tracking Fauxtography on Social Media (PI, $29,780)*.

2021 **BU CISE Seed Grant**, *EasyCSPeasy: Automatic XSS Prevention (PI, $25,000)*, Co-PI Manuel Egele (BU ECE).

2020-2025 **NSF Secure and Trustworthy Cyberspace (SaTC)**, *CAREER: Towards Data-Driven Methods to Counter Online Aggression (PI, $549,331)*.

2020-2021 **BU Engineering Dean's Catalyst Award**, *Real Time Monitoring of Disinformation Campaigns (PI, $42,000)*, Co-PI Chris Wells (BU COM).

2019-2022 **Hariri Institute Junior Fellowship**, *(PI, $10,000)*.

2020 **BU Institute for Health System Innovation & Policy Summer Research Project**, *Tracking COVID-19 Misinformation Campaigns across Social Media (PI, $4,800)*.

2018 **Facebook Secure the Internet Grant**, *Understanding the Use of Hijacked Facebook Accounts in the Wild, (PI, $92,000 – Research Gift)*.

At Boston University - Co-PI

2022-2023 **BU Hariri Institute Focused Research Program**, *Data and Misinformation in an Era of Sustainability and Climate Change Crises (Co-PI, $247,347, personal share $42,000)*, PIs Chris Wells, Sarah Finnie Robinson, Irena Vodenska, Co-PIs Michelle Amazeen, Hyunuk Kim, Arunima Krishna).

2022-2023 **Red Hat Collaboratory Research Incubation Award**, *AI for Cloud Ops (Co-PI, $836,994, personal share $216,056)*, PI Ayse Coskun, Co-PI Alan Liu.

2021-2022 **NSF Converegence Acccellerator**, *NSF Convergence Accelerator Track F: America's Fourth Estate at Risk: A System for Mapping the (Local) Journalism Life Cycle to Rebuild the Nation's News Trust (Co-PI, $750,000, BU share $186,977)*, PI Eduard Dragut (Temple), Co-PIs Cornelia Cagagea (UIC), Lei Guo (BU), Robert Holbert (Temple).

2021 **BU Hariri Institute Focused Research Program**, *Leveraging AI to Examine Disparities and Bias in Health Care (Co-PI, $209,205)*, Co-PI Iannis Paschalidis (BU ECE).

2020-2022 **NSF Partnership for Industry (PFI)**, *A Multi-Disciplinary Approach to Detecting Adolescent Online Risks (Senior Personnel, share $128,987)*, PI Pamela Wisniewski (UCF), Co-PI Munmun De Chowdhury (Georgia Tech).

2020-2021 **BU Hariri Institute Incubation Award**, *Towards Developing Computational Models to Predict the Spreading of Radicalizing Content on the Web (Co-PI, $54,950)*, PI Jessica Stern (BU Pardee School).

At University College London

2018 **GCHQ Small Grant**, *Understanding the Benefits and Drawbacks of Capture the Flag (CTF) exercises in an organisational context, (PI, £29,988)*.

2017 **EPSRC-Funded PETRAS Hub Grant**, *Botthings: Modelling The Potential Impact Of IoT Boosted Botnet Attacks, (PI, £118,525)*.

2017 **EPSRC Standard Research**, *EP/P011896/1 — ACCEPT: Addressing Cybersecurity and Cybercrime via a co-Evolutionary aPproach to reducing human-relaTed risks, (Co-PI, £1,101,225).*

2016 **EPSRC-funded BEAMS Future Leaders in Engineering and Physical Sciences**, *Measuring and countering malware delivery networks*, (PI, £29,054).

2016 **EPSRC Standard Research**, *EP/N028112/1 — DAPM: Detecting and Preventing Mass-Marketing Fraud (MMF), (Co-PI, £1,056,471 — UCL share £246,742).*

2016 **GCHQ Small Grant**, *Developing a Malware Analysis Infrastructure at UCL (PI, £14,244.84).*

2015 **Google Research Award**, *Understanding the Use of Stolen Accounts by Cybercriminals (PI, $66,500).*

2015 **Horizon 2020 MSCA Rise Scheme**, *H2020-MSCA-RISE ENCASE — EnhaNcing seCurity And privacy in the Social wEb: a user centered approach for the protection of minors (Co-PI, €2,160,000 — UCL share €324,000).*

2015 **EPSRC First Grant Scheme**, *EP/N008448/1 — Inferring the Purpose of Network Activities (PI, £122,803).*

Publications

The names of advised students/postdocs are underlined.

Total number of peer-reviewed publications: 155
Total number of citations (Google Scholar, June 2024): 12,230
H-index (Google Scholar, June 2024): 58

Book Chapters

(B3) **G. Stringhini**, J. Blackburn. Understanding the Phases of Coordinated Online Aggression Attacks. In *Social Processes of Online Hate*, 2025 (in Print).

(B2) **G. Stringhini**. Adversarial Behaviours Knowledge Area. In *Cyber Security Body of Knowledge (CYBOK)*, 2019.

(B1) **G. Stringhini**. Fighting cybercrime once it switches from the online world to the real world. In *Routledge Handbook of Crime Science*, 2018.

Journal Papers

(J22) A. Alsoubai, A. Razi, Z. Agha, S. Ali, **G. Stringhini**, M. De Choudhury, P. Wisniewski. Profiling the Offline and Online Risk Experiences of Youth to Develop Targeted Interventions for Online Safety. In *Proceedings of the ACM on Human Computer Interaction (CSCW)*, 2024.

(J21) S. Ali, A. Razi, A. Alsoubai, S. Kim, C. Ling, M. De Choudhury, P. Wisniewski, **G. Stringhini**. Getting Meta: A Multimodal Approach for Detecting Unsafe Conversations within Instagram Direct Messages of Youth. In *Proceedings of the ACM on Human Computer Interaction (CSCW)*, 2023.

(J20) Y. Wang, C. Ling, **G. Stringhini**. Understanding the Use of Images to Spread COVID-19 Misinformation on Twitter. In *Proceedings of the ACM on Human Computer Interaction (CSCW)*, 2023.

(J19) A. Razi, S. Kim, A. Alsoubai, S. Ali, **G. Stringhini**, M. De Choudhury, P. Wisniewski. Sliding into My DMs: Detecting Uncomfortable or Unsafe Sexual Risk Experiences within Instagram Direct Messages Grounded in the Perspective of Youth. In *Proceedings of the ACM on Human Computer Interaction (CSCW)*, 2023.

(J18) C. Ling, U. Balci, J. Blackburn, **G. Stringhini**. A First Look at Zoombombing. In *IEEE Security & Privacy Magazine*, 2022.

(J17) A. Razi, S. Kim, **G. Stringhini**, T. Solorio, M. De Chowdhury, P. Wisniewski. A Human-Centered Systematic Literature Review of the Computational Approaches for Online Sexual Risk Detection. In *Proceedings of the ACM on Human Computer Interaction (CSCW)*, 2021.

(J16) K. Papadamou, S. Zannettou, J. Blackburn, E. De Cristofaro, **G. Stringhini**, M. Sirivianos. "How over is it?" Understanding the Incel Community on Youtube. In *Proceedings of the ACM on Human Computer Interaction (CSCW)*, 2021.

(J15) S. Kim, A. Razi, **G. Stringhini**, P. Wisniewski, M. De Choudhury. A Human-Centered Systematic Literature Review of Cyberbullying Detection Algorithms. In *Proceedings of the ACM on Human Computer Interaction (CSCW)*, 2021.

(J14) P. Doerfler, A. Forte, E. De Cristofaro, **G. Stringhini**, J. Blackburn, D. McCoy. "I'm a Professor, which isn't usually a dangerous job": Internet-Facilitated Harassment and its Impact on Researchers. In *Proceedings of the ACM on Human Computer Interaction (CSCW)*, 2021.

(J13) M. Ribeiro, S. Jhaver, S. Zannettou, J. Blackburn, E. De Cristofaro, **G. Stringhini**, R. West. Does Platform Migration Compromise Content Moderation? Evidence from r/The_Donald and r/Incels. In *Proceedings of the ACM on Human Computer Interaction (CSCW)*, 2021.

(J12) C. Ling, I. AbuHilal, J. Blackburn, E. De Cristofaro, S. Zannettou, **G. Stringhini**. Dissecting the Meme Magic: Understanding Indicators of Virality in Image Memes. In *Proceedings of the ACM on Human Computer Interaction (CSCW)*, 2021.

(J11) G. Suarez-Tangil, **G. Stringhini**. Eight Years of Rider Measurement in the Android Malware Ecosystem: Evolution and Lessons Learned. In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2020.

(J10) G. Suarez-Tangil, M. Edwards, C. Peersman, **G. Stringhini**, A. Rashid, M. Whitty. Automatically Dismantling Online Dating Fraud. In *IEEE Transactions on Information Forensics and Security (TIFS)*, 2020.

(J9) E. Mariconti, G. Suarez-Tangil, J. Blackburn, E. De Cristofaro, N. Kourtellis, I. Leontiadis, J. Luque Serrano, **G. Stringhini**. "You Know What to Do": Proactive Detection of YouTube Videos Targeted by Coordinated Hate Attacks. In *Proceedings of the ACM on Human Computer Interaction (CSCW)*, 2019.

(J8) D. Chatzakou, N. Kourtellis, J. Blackburn, E. De Cristofaro, **G. Stringhini**, A. Vakali. etecting Cyberbullying and Cyberaggression in Social Media. In *ACM Transactions on the Web (TWEB)*, 2019.

(J7) E. Mariconti, L. Onwuzurike, P. Andriotis, E. De Cristofaro, G. Ross, **G. Stringhini**. MaMaDroid: Detecting Android Malware by Building Markov Chains of Behavioral Models (Extended Version). In *ACM Transactions on Privacy and Security (TOPS)*, 2019.

(J6) A. Bermudez-Villalva, J. Onaolapo, M. Musolesi, **G. Stringhini**. Under and Over the Surface: A Comparison Of The Use Of Leaked Account Credentials in the Dark and Surface Web. In *Journal of Crime Science*, 2018.

(J5) A. Ioannou, J. Blackburn, **G. Stringhini**, E. De Cristofaro, N. Kourtellis, M. Sirivianos. From risk factors to detection and intervention: a practical proposal for future work on cyberbullying. In *Behaviour and Information Technology*, 2018.

(J4) P. Andriotis, M.A. Sasse, **G. Stringhini**. Studying Users' Adaptation to Android's Runtime Fine-grained Access Control System. In *Journal of Information Security and Applications*, 2018.

(J3) I. Becker, A. Hutchings, R. Abu-Salma, R. Anderson, N. Bohm, S. Murdoch, M.A. Sasse, **G. Stringhini**. International Comparison of Bank Fraud Reimbursement: Customer Perceptions and Contractual Terms. In *Journal of Cybersecurity*, 2018.

(J2) M. Egele, **G. Stringhini**, C. Kruegel, G. Vigna. Towards Detecting Compromised Accounts on Social Networks. In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2016.

(J1) **G. Stringhini**, M. Egele, C. Kruegel, and G. Vigna. Poultry Markets: On the Underground Economy of Twitter Followers. In *ACM SIGCOMM Computer Communication Review - Volume 42 Issue 4*, 2012.

Conference Proceedings

(C97) Z. Sun, F. B. Kokulu, P. Zhang, A. Oest, **G. Stringhini**, T. Bao, R. Wang, Y. Shoshitaishvili, A. Doupè, G.J. Ahn. From Victims to Defenders: An Exploration of the Phishing Attack Reporting Ecosystem. In *International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, 2024.

(C96) Z. Zhang, R. Kumar, J. Li, L. Korver, A. Byrne, **G. Stringhini**, A. Matta, A. Coskun. PraxiPaaS: A Decomposable Machine Learning System for Efficient Container Package Discovery. In *IEEE International Conference on Cloud Engineering (IC2E)*, 2024.

(C95) M. Toslali, S. M. Qasim, S. Parthasarathy, F. Oliveira, H. Huang, **G. Stringhini**, Z. Liu, A. Coskun. Astraea: An Online, Probabilistic Distributed Tracing System. In *IEEE International Conference on Cloud Engineering (IC2E)*, 2024.

(C94) I. Angelakopoulos, **G. Stringhini**, M. Egele. Pandawan: Quantifying Progress in Linux-based Firmware Rehosting. In *USENIX Security Symposium*, 2024.

(C93) J. Patel, P. Paudel, E. De Cristofaro, **G. Stringhini**, J. Blackburn. iDRAMA-scored-2024: A Dataset of the Scored-co platform Spanning 2020 to 2023. In *AAAI International Conference on Web and Social Media (ICWSM)*, 2024.

(C92) S. Ullah, M. Han, S. Pujar, H. Pearce, A. Coskun, **G. Stringhini**. LLMs Cannot Reliably Identify and Reason About Security Vulnerabilities (Yet?): A Comprehensive Evaluation, Framework, and Benchmarks. In *IEEE Symposium on Security and Privacy*, 2024.

(C91) P. Paudel, C. Ling, J. Blackburn, **G. Stringhini**. PIXELMOD: Improving Soft Moderation of Visual Misleading Information on Twitter. In *USENIX Security Symposium*, 2024.

(C90) P. Paudel, M.H. Saeed, R. Auger, C. Wells, **G. Stringhini**. Enabling Contextual Soft Moderation on Social Media through Contrastive Textual Deviation. In *USENIX Security Symposium*, 2024.

(C89) A. Alsoubai, J. Park, S. Qadir, **G. Stringhini**, A. Razi, P. Wisniewski. Systemization of Knowledge (SoK): Creating a Research Agenda for Human-Centered Real-Time Risk Detection on Social Media Platforms. In *ACM Conference on Human Factors in Computing Systems (CHI)*, 2024.

(C88) M.H. Saeed, K. Papadamou, J. Blackburn, E. De Cristofaro, **G. Stringhini**. TU-BERAIDER: Attributing Coordinated Hate Attacks on YouTube Videos to their Source Communities. In *AAAI International Conference on Web and Social Media (ICWSM)*, 2024.

(C87) M. Singhal, C. Ling, P. Paudel, P. Thota, N. Kumarswamy, **G. Stringhini**, S. Nilizadeh. SoK: Content Moderation in Social Media, from Guidelines to Enforcement, and Research to Practice. In *IEEE European Symposium on Security and Privacy*, 2023.

(C86) P. Paudel, J. Blackburn, E. De Cristofaro, S. Zannettou, **G. Stringhini**. Lambretta: Learning to Rank for Twitter Soft Moderation. In *IEEE Symposium on Security and Privacy*, 2023.

(C85) I. Angelakopoulos, **G. Stringhini**, M. Egele. FirmSolo: Enabling dynamic analysis of binary Linux-based IoT kernel modules. In *USENIX Security Symposium*, 2023.

(C84) A. Efstratiou, J. Blackburn, T. Caulfield, **G. Stringhini**, S. Zannettou, E. De Cristofaro. Non-Polar Opposites: Analyzing the Relationship Between Echo Chambers and Hostile Intergroup Interactions on Reddit. In *AAAI International Conference on Web and Social Media (ICWSM)*, 2023.

(C83) U. Balci, C. Ling, E. De Cristofaro, M. Squire, **G. Stringhini**, J. Blackburn. Beyond Fish and Bicycles: Exploring the Varieties of Online Women's Ideological Spaces. In *ACM Web Science Conference (WebSci)*, 2023.

(C82) W.M. Si, M. Backes, J. Blackburn, E. De Cristofaro, **G. Stringhini**, S. Zannettou, Y. Zhang. Why So Toxic? Measuring and Triggering Toxic Behavior in Open-Domain Chatbots. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2022.

(C81) M. Naseri, Y. Han, E. Mariconti, Y. Shen, **G. Stringhini**, E. De Cristofaro. CER-BERUS: Federated Prediction of Security Events. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2022.

(C80) C. Ling, J. Blackburn, E. De Cristofaro, **G. Stringhini**. Slapping Cats, Bopping Heads, and Oreo Shakes: Understanding Indicators of Virality in TikTok Short Videos. In *ACM Web Science Conference (WebSci)*, 2022.

(C79) Y. Shen, Y. Han, Z. Zhang, M. Chen, T. Yu, M. Backes, Y. Zhang, **G. Stringhini**. Finding MNEMON: Reviving Memories of Node Embeddings. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2022.

(C78) S. Ali, A. Razi, S. Kim, A. Alsoubai, J. Gracie, M. De Chouwhury, P. Wisniewski, **G. Stringhini**. Understanding the Digital Lives of Youth: Analyzing Media Shared within Safe

Versus Unsafe Private Conversations on Instagram. In *ACM CHI Conference on Human Factors in Computing Systems (CHI)*, 2022.

(C77) M. H. Saeed, S. Ali, J. Blackburn, E. De Cristofaro, S. Zannettou, **G. Stringhini**. TrollMagnifier: Detecting State-Sponsored Troll Accounts on Reddit. In *IEEE Symposium on Security and Privacy (Oakland)*, 2022.

(C76) K. Papadamou, S. Zannettou, J. Blackburn, E. De Cristofaro, **G. Stringhini**, M. Sirivianos. "It's just a flu": Assessing the Effect of Watch History on YouTube's Pseudoscientific Video Recommendations. In *AAAI International Conference on Web and Social Media (ICWSM)*, 2022.

(C75) Y. Shen, P.A. Vervier, **G. Stringhini**. A Large-scale Temporal Measurement of Android Malicious Apps: Persistence, Migration, and Lessons Learned. In *USENIX Security Symposium*, 2022.

(C74) M. Aliapoulios, A. Papasavva, C. Ballard, E. De Cristofaro, **G. Stringhini**, S. Zannettou, J. Blackburn. The Gospel According to Q: Understanding the QAnon Conspiracy from the Perspective of Canonical Information. In *AAAI International Conference on Web and Social Media (ICWSM)*, 2022.

(C73) A. Bermudez Villalva, **G. Stringhini**. The shady economy: Understanding the difference in trading activity from underground forums in different layers of the Web. In *APWG eCrime Symposium)*, 2021.

(C72) Y. Wang, S. Zannettou, J. Blackburn, B. Bradlyn, E. De Cristofaro, **G. Stringhini**. A Multi-Platform Analysis of Political News Discussion and Sharing on Web Communities. In *IEEE International Conference on Big Data (BigData)*, 2021.

(C71) C. Ife, Y. Shen, S. Murdoch, **G. Stringhini**. Marked for Disruption: Tracing the Evolution of Malware Delivery Operations Targeted for Takedown. In *International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, 2021.

(C70) O. Bordeanu, T. Davies, Y. Shen, **G. Stringhini**. Jabbic lookups: a backend telemetry-based system for malware triage. In *EAI SecureComm*, 2021.

(C69) S. Ali, H. Saeed, E. Aldreabi, J. Blackburn, E. De Cristofaro, S. Zannettou, **G. Stringhini**. Understanding the Effect of Deplatforming on Social Networks. In *ACM Web Science Conference (WebSci)*, 2021.

(C68) M. Aliapoulos, E. Bevensee, J. Blackburn, B. Bradlyn, E. De Cristofaro, **G. Stringhini**, S. Zannettou. A Large Open Dataset from the Parler Social Network. In *AAAI International Conference on Web and Social Media (ICWSM)*, 2021.

(C67) O. Zungur, A. Bianchi, **G. Stringhini**, M. Egele. AppJitsu: Investigating the Resiliency of Android Applications. In *IEEE European Symposium on Security and Privacy (Euro S&P)*, 2021.

(C66) Y. Shen and **G. Stringhini**. ANDRUSPEX: Leveraging Graph Representation Learning to Predict Harmful App Installations on Mobile Devices. In *IEEE European Symposium on Security and Privacy (Euro S&P)*, 2021.

(C65) A. Papasavva, J. Blackburn, **G. Stringhini**, S. Zannettou, E. De Cristofaro. "Is it a Qoincidence?": A First Step Towards Understanding and Characterizing the QAnon Movement on Voat.co. In *The Web Conference (WWW)*, 2021.

(C64) F. Tahmasbi, L. Schild, C. Ling, J. Blackburn, **G. Stringhini**, Y. Zhang, S. Zannettou. "Go eat a bat, Chang!": On the Emergence of Sinophobic Behavior on Web Communities in the Face of COVID-19. In *The Web Conference (WWW)*, 2021.

(C63) B. Kaleli, B. Kondracki, M. Egele, N. Nikiforakis, **G. Stringhini**. To Err.Is Human: Characterizing the Threat of Unintended URLs in Social Media. In *ISOC Network and Distributed Systems Security Symposium (NDSS)*, 2021.

(C62) J. Onaolapo, N. Leontiadis, D. Magka, **G. Stringhini**. SocialHEISTing: Understanding Stolen Facebook Accounts. In *USENIX Security Symposium*, 2021.

(C61) C. Ling, U. Balci, J. Blackburn, **G. Stringhini**. A First Look at Zoombombing. In *IEEE Symposium on Security & Privacy (Oakland)*, 2021.

(C60) S. Kim, A. Razi, **G. Stringhini**, P. Wisniewski, M. De Chowdhury. You Don't Know How I Feel: Insider-Outsider Perspective Gaps in Cyberbullying Risk Detection. In *AAAI International Conference on Web and Social Media (ICWSM)*, 2021.

(C59) Y. Wang, F. Tahmasbi, J. Blackburn, B. Bradlyn, E. De Cristofaro, D. Magerman, S. Zannettou, **G. Stringhini**. Understanding the Use of Fauxtography on Social Media. In *AAAI International Conference on Web and Social Media (ICWSM)*, 2021.

(C58) Y. Shen, P.A. Vervier, **G. Stringhini**. Understanding Worldwide Private Information Collection on Android. In *ISOC Network and Distributed Systems Security Symposium (NDSS)*, 2021.

(C57) K. Thomas, D. Akhawe, M. Bailey, D. Boneh, E. Bursztein, S. Consolvo, N. Dell, Z. Durumeric, P. Kelly, D. Kumar, D. McCoy, S. Meiklejohn, T, Ristenpart, **G. Stringhini**. SoK: Hate, Harassment, and the Changing Landscape of Online Abuse. In *IEEE Symposium on Security & Privacy (Oakland)*, 2021.

(C56) M. Ribeiro, J. Blackburn, B. Bradlyn, E. De Cristofaro, **G. Stringhini**, S. Long, S. Greenberg, S. Zannettou. The Evolution of the Manosphere Across the Web. In *AAAI International Conference on Web and Social Media (ICWSM)*, 2021.

(C55) S. Zannettou, M. El Sherief, S. Nilizadeh, E. Belding, **G. Stringhini**. Measuring and Characterizing Hate Speech on News Websites. In *ACM Web Science Conference (WebSci)*, 2020.

(C54) A. Papasavva, S. Zannettou, E. De Cristofaro, **G. Stringhini**, J. Blackburn. Raiders of the Lost Kek: 3.5 Years of Augmented 4chan Posts from the Politically Incorrect Board. In *AAAI International Conference on Web and Social Media (ICWSM)*, 2020.

(C53) O. Zungur, **G. Stringhini**, M. Egele. Libspector: Context-Aware Large-Scale Network Traffic Analysis of Android Applications. In *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2020.

(C52) S. Zannettou, B. Bradlyn, E. De Cristofaro, **G. Stringhini**, J. Blackburn. Characterizing the Use of Images by State-Sponsored Troll Accounts on Twitter. In *AAAI International Conference on Web and Social Media (ICWSM)*, 2020.

(C51) B. Alahmadi, E. Mariconti, R. Spolaor, **G. Stringhini**, I. Martinovic. BOTection: Bot Detection by Building Markov Chain Models of Bots Network Behavior. In *ACM ASIA Conference on Computer and Communications Security (ASIACCS)*, 2020.

(C50) K. Papadamou, A. Papasavva, S. Zannettou, J. Blackburn, N. Kourtellis, I. Leontiadis, **G. Stringhini**, M. Sirivianos. Disturbed YouTube for Kids: Characterizing and Detecting Inappropriate Videos Targeting Young Children. In *AAAI International Conference on Web and Social Media (ICWSM)*, 2020.

(C49) Y. Shen, **G. Stringhini**. attack2vec: Leveraging Temporal Word Embeddings to Understand the Evolution of Cyberattacks. In *USENIX Security Symposium*, 2019.

(C48) C. Ife, Y. Shen, S. Murdoch, **G. Stringhini**. Waves of Malice: A Longitudinal Measurement of the Malicious File Delivery Ecosystem on the Web. In *ACM ASIA Conference on Computer and Communications Security (ASIACCS)*, 2019.

(C47) O. Mirzaei, G. Suarez-Tangil, J. de Fuentes, J. Tapiador, **G. Stringhini**. AndrEnsemble: Leveraging API Ensembles to Characterize Android Malware Families. In *ACM ASIA Conference on Computer and Communications Security (ASIACCS)*, 2019.

(C46) B. Kaleli, M. Egele, **G. Stringhini**. On the Perils of Leaking Referrers in Online Collaboration Services. In *Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, 2019.

(C45) O. Zungur, **G. Stringhini**, M. Egele. BORDERPATROL: Securing BYOD using fine-grained contextual information. In *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2019.

(C44) S. Zannettou, T. Caulfield, M. Sirivianos, **G. Stringhini**, J. Blackburn. Who Let The Trolls Out? Towards Understanding State-Sponsored Trolls. In *ACM Conference on Web Science (WebSci)*, 2019.

(C43) B. Perez, M. Musolesi, **G. Stringhini**. Fatal Attraction: Identifying Mobile Devices Through Electromagnetic Emissions. In *ACM Conference on Security and Privacy in Mobile and Wireless Networks (WiSec)*, 2019.

(C42) S. Matic, G. Tyson, **G. Stringhini**. Pythia: a Framework for Automatic Analysis of Web Hosting Environments. In *The Web Conference (WWW)*, 2019.

(C41) D. Ibisiola, I. Castro, **G. Stringhini**, S. Uhlig, G. Tyson. Who Watches the Watchmen: Exploring Complaints on the Web. In *The Web Conference (WWW)*, 2019.

(C40) J. Echeverria, N. Kourtellis, I. Leontiadis, E. De Cristofaro, **G. Stringhini**, S. Zhou. LOBO - Evaluation of Generalization Deficiencies in Twitter Bot Classifiers. In *Annual Computer Security Applications Conference (ACSAC)*, 2018.

(C39) Y. Shen, E. Mariconti, P. Vervier, **G. Stringhini**. Tiresias: Predicting Security Events Through Deep Learning. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2018.

(C38) S. Zannettou, T. Caulfield, J. Blackburn, E. De Cristofaro, M. Sirivianos, **G. Stringhini**, G. Suarez-Tangil. On the Origins of Memes by Means of Fringe Web Communities. In *ACM SIGCOMM Internet Measurement Conference (IMC)*, 2018.

(C37) L. Onwuzurike, M. Alameida, E. Mariconti, J. Blackburn, **G. Stringhini**, E. De Cristofaro. A Family of Droids: Analyzing Behavioral Model based Android Malware Detection via Static and Dynamic Analysis. In *Annual Conference on Privacy, Security and Trust (PST)*, 2018.

(C36) A. Founta, C. Djouvas, D. Chatzakou, I. Leontiadis, J. Blackburn, **G. Stringhini**, A. Vakali, M. Sirivianos, N. Kourtellis. Large Scale Crowdsourcing and Characterization of Twitter Abusive Behavior. In *AAAI Conference on Web and Social Media (ICWSM)*, 2018.

(C35) S. Zannettou, J. Blackburn, E. De Cristofaro, M. Sirivianos, **G. Stringhini**. Understanding Web Archiving Services and Their (Mis)Use on Social Media. In *AAAI Conference on Web and Social Media (ICWSM)*, 2018.

(C34) D. Ibosiola, B. Steer, A. Garcia-Recuero, **G. Stringhini**, S. Uhlig, G. Tyson. Movie Pirates of the Caribbean: Exploring Illegal Streaming Cyberlockers. In *AAAI Conference on Web and Social Media (ICWSM)*, 2018.

(C33) B. Perez, M. Musolesi, **G. Stringhini**. You are your Metadata: Identification and Obfuscation of Social Media Users using Metadata Information. In *AAAI Conference on Web and Social Media (ICWSM)*, 2018.

(C32) **G. Stringhini**, Y. Shen, Y. Han, X. Zhang. Marmite: Spreading Malicious File Reputation Through Download Graphs. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2017.

(C31) M. Weissbacher, E. Mariconti, G. Suarez-Tangil, **G. Stringhini**, W. Robertson, E. Kirda. Ex-Ray: Detection of History-Leaking Browser Extensions. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2017.

(C30) S. Nilizadeh, F. Labrèche*, A. Sadighian, A. Zand, J. Fernandez, **G. Stringhini**, G. Vigna, C. Kruegel. POISED: Spotting Twitter Spam Off the Beaten Paths. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2017.

(C29) S. Zannettou, T. Caulfield, E. De Cristofaro, N. Kourtellis, I. Leontiadis, M. Sirivianos, **G. Stringhini**, and J. Blackburn. The Web Centipede: Understanding How Web Communities Influence Each Other Through the Lens of Mainstream and Alternative News Sources. In *Proceedings of the ACM SIGCOMM Internet Measurement Conference (IMC)*, 2017.

(C28) D. Chatzakou, N. Kourtellis, J. Blackburn, E. De Cristofaro, **G. Stringhini**, and A. Vakali. Mean Birds: Detecting Aggression and Bullying on Twitter. In *Proceedings of the International ACM Conference on Web Science (WebSci)*, 2017.

(C27) D. Chatzakou, N. Kourtellis, J. Blackburn, E. De Cristofaro, **G. Stringhini**, and A. Vakali. Hate is not binary: Studying abusive behavior of #GamerGate on Twitter. In *Proceedings of the ACM Conference on Hypertext and Social Media (HyperText)*, 2017.

(C26) A. Haslebacher, J. Onaolapo, **G. Stringhini**. All Your Cards Are Belong To Us: Understanding Online Carding Forums. In *Proceedings of the APWG eCrime Symposium*, 2017.

(C25) G. Hine, J. Onaolapo, E. De Cristofaro, N. Kourtellis, I. Leontiadis, R. Samaras, **G. Stringhini**, J. Blackburn. Kek, Cucks, and Goad Emperor Trump: A Measurement Study of 4chan's Politically Incorrect Forum and its Effect on the Web. In *Proceedings of the International Conference on Web and Social Media (ICWSM)*, 2017.

(C24) P. Andriotis, S. Li, T. Spyridopoulos, **G. Stringhini**. A comparative study of Android users' privacy preferences under the runtime permission model. In *Proceedings of the*

International Conference on Human Aspects of Information Security, Privacy and Trust, 2017.

(C23) E. Kolodenker, W. Koch, **G. Stringhini**, M. Egele. PayBreak: Defense against cryptographic ransomware. In *Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2017.

(C22) S. Sajadmanesh, S. Jafarzadeh, S.A. Ossia, H.R. Rabiee, H. Haddadi, Y. Mejova, M. Musolesi, E. De Cristofaro, **G. Stringhini**. Kissing Cuisines: Exploring Worldwide Culinary Habits on the Web. In *Proceedings of the International World Wide Web Conference (WWW), Web Science Track*, 2017.

(C21) E. Mariconti, J. Onaolapo, S. Ahmad, N. Nikiforou, M. Egele, N. Nikiforakis, **G. Stringhini**. What's in a Name? Understanding Profile Name Reuse on Twitter. In *Proceedings of the International World Wide Web Conference (WWW)*, 2017.

(C20) E. Mariconti, L. Onwuzurike, P. Andriotis, E. De Cristofaro, G. Ross, **G. Stringhini**. MaMaDroid: Detecting Android Malware by Building Markov Chains of Behavioral Models. In *Proceedings of the ISOC Network and Distributed Systems Symposium (NDSS)*, 2017.

(C19) J. Onaolapo, E. Mariconti, **G. Stringhini**. What Happens After You Are Pwnd: Understanding The Use Of Stolen Webmail Credentials In The Wild. In *Proceedings of the Internet Measurement Conference (IMC)*, 2016.

(C18) S. J. Murdoch, I. Becker, R. Abu Salma, R. Anderson, N. Bohm, A. Hutchings, M. A. Sasse, **G. Stringhini**. Are Payment Card Contracts Unfair? In *Proceedings of Financial Cryptography and Data Security*, 2016.

(C17) S. Hao, K. Borgolte, N. Nikiforakis, **G. Stringhini**, M. Egele, M. Eubanks, B. Krebs, G. Vigna. Drops for Stuff: An Analysis of Reshipping Mule Scams. In *Proceedings of the ACM Symposium on Computer and Communication Security (CCS)*, 2015.

(C16) **G. Stringhini**, P. Mourlanne, G. Jacob, M. Egele, C. Kruegel, G. Vigna. EvilCohort: Detecting Communities of Malicious Accounts on Online Services. In *Proceedings of the USENIX Security Symposium*, 2015.

(C15) **G. Stringhini**, O. Thonnard. That Ain't You: Blocking Spearphishing Through Behavioral Modelling. In *Proceedings of the Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, 2015.

(C14) J. Huang, **G. Stringhini**, P. Yong. Quit Playing Games With My Heart: Understanding Online Dating Scams. In *Proceedings of the Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, 2015.

(C13) A. Zarras, A. Kapravelos, **G. Stringhini**, T. Holz, C. Kruegel, G. Vigna. The Dark Alleys of Madison Avenue: Understanding Malicious Advertisements. In *Proceedings of the Internet Measurement Conference (IMC)*, 2014.

(C12) **G. Stringhini**, O. Hohlfeld, C. Kruegel, and G. Vigna. The Harvester, the Botmaster, and the Spammer: On the Relations Between the Different Actors in the Spam Landscape. In *Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, 2014.

(C11) N. Nikiforakis, F. Maggi, **G. Stringhini**, M. Z. Rafique, W. Joosen, C. Kruegel, F. Piessens, G. Vigna, and S. Zanero. Stranger Danger: Exploring the Ecosystem of Ad-based

URL Shortening Services. In *Proceedings of the International World Wide Web Conference (WWW)*, 2014.

(C10) **G. Stringhini**, C. Kruegel, and G. Vigna. Shady Paths: Leveraging Surfing Crowds to Detect Malicious Web Pages. In *Proceedings of the ACM Symposium on Computer and Communication Security (CCS)*, 2013.

(C9) **G. Stringhini**, G. Wang, M. Egele, C. Kruegel, G. Vigna, H. Zheng, and B. Y. Zhao. Follow the Green: Growth and Dynamics in Twitter Follower Markets. In *Proceedings of the Internet Measurement Conference (IMC)*, 2013.

(C8) F. Maggi, A. Frossi, **G. Stringhini**, B. Stone-Gross, C. Kruegel, G. Vigna, and S. Zanero. Two Years of Short URLs Internet Measurement: Security Threats and Countermeasures. In *Proceedings of the International World Wide Web Conference (WWW)*, 2013.

(C7) M. Egele, **G. Stringhini**, C. Kruegel, and G. Vigna. Compa: Detecting Compromised Accounts on Social Networks. In *Proceedings of the ISOC Network and Distributed Systems Symposium (NDSS)*, 2013.

(C6) **G. Stringhini**, M. Egele, A. Zarras, T. Holz, C. Kruegel, and G. Vigna. B@bel: Leveraging Email Delivery for Spam Mitigation. In *Proceedings of the USENIX Security Symposium*, 2012.

(C5) A. Doupè, M. Egele, B. Caillat, **G. Stringhini**, G. Yakin, A. Zand, L. Cavedon, and G. Vigna. Hit 'em Where it Hurts: A Live Security Exercise on Cyber Situational Awareness. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2011.

(C4) **G. Stringhini**, T. Holz, B. Stone-Gross, C. Kruegel, and G. Vigna. BotMagnifier: Locating Spambots on the Internet. In *Proceedings of the USENIX Security Symposium*, 2011.

(C3) **G. Stringhini**, C. Kruegel, and G. Vigna. Detecting Spammers on Social Networks. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2010.

(C2) **G. Stringhini**, M. Migliardi. Travelling Information For Intrusion Prevention Systems. In *Security & Management*, 2010.

(C1) **G. Stringhini**, M. Migliardi. A distributed model for intrusion detection and prevention. In *Proceedings of the WWW/Internet International Conference*, 2009.

Workshop Proceedings (Peer Reviewed)

(W33) Z. Zhang, J. Li, R. Kumar, L. Korver, A. Byrne, **G. Stringhini**, A. Matta, A. Coskun. PraxiPaaS: An Efficient PaaS Cluster Container Package Discovery Framework Using Machine Learning. In *MLSys Young Professionals Symposium (YPS)*, 2024.

(W32) I. Angelakopoulos, **G. Stringhini**, M. Egele. FirmDiff: Improving the Configuration of Linux Kernels Geared Towards Firmware Re-hosting. In *Workshop on Binary Analysis Research (BAR)*, 2024.

(W31) Y. Zhou, J. Li, **G. Stringhini**, A. Coskun, Z. Liu. Enabling Privacy-preserving Network Telemetry with Autoencoders. In *Networking Women Professional Development Workshop (N2WOMEN)*, 2023.

(W30) J. Park, J. Gracie, A. Alsoubai, **G. Stringhini**, P. Wisniewski. Towards Automated Detection of Risky Images Shared by Youth on Social Media. In *International Workshop on Cyber Social Threats (CySoc)*, 2023.

(W29) F. Labreche, E. Mariconti, **G. Stringhini**. Shedding Light on the Targeted Victim Profiles of Malicious Downloaders. In *International Workshop on Cyber Crime (IWCC)*, 2022.

(W28) C. Jennifer, F. Tahmasbi, J. Blackburn, **G. Stringhini**, S. Zannettou, E. De Cristofaro. Feels Bad Man: Dissecting Automated Hateful Meme Detection Through the Lens of Facebook's Challenge. In *Workshop on Cyber Social Threats (CySoc)*, 2022.

(W27) M. H. Saeed, J. Blackburn, **G. Stringhini**. There are N Impostors Among Us: Understanding the Effect of State-Sponsored Troll Accounts on Reddit Discussions. In *Workshop on Cyber Social Threats (CySoc)*, 2022.

(W26) P. Paudel, J. Blackburn, E. De Cristofaro, S. Zannettou, **G. Stringhini**. A Longitudinal Study of the Gettr Social Network. In *Workshop on Cyber Social Threats (CySoc)*, 2022.

(W25) X. Caddle, A. Soubai, A. Razi, S. Kim, S. Ali, **G. Stringhini**, M. De Chowdhury, P. Wisniewski. Instagram Data Donation: A Case for Partnering with Social Media Platforms to Protect Adolescents Online. In *Social Media as a Design and Research Site in HCI: Mapping Out Opportunities and Envisioning Future Uses Workshop*, 2021.

(W24) A. Razi, S. Kim, A., A. Soubai, X. Caddle, S. Ali, **G. Stringhini**, M. De Chowdhury, P. Wisniewski. Teens at the Margin: Artificially Intelligent Technology for Promoting Adolescent Online Safety. In *Artificially Intelligent Technology for the Margins: A Multi-disciplinary Design Agenda Workshop*, 2021.

(W23) C. Ling, **G. Stringhini**. Examining the Impact of Social Distance on the Reaction to a Tragedy: A Case Study on Sulli's Death. In *Workshop on Cyber Social Threats (CySoc)*, 2020.

(W22) A. Bermudez Villalva, M. Musolesi, **G. Stringhini**. A Measurement Study on the Advertisements Displayed to Web Users Coming from the Regular Web and from Tor. In *Workshop on Attackers and Cyber-Crime Operations (WACCO)*, 2020.

(W21) B. Kaleli, M. Egele, **G. Stringhini**. Studying the Privacy Issues of the Incorrect Use of the Feature Policy. In *Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb)*, 2020.

(W20) C. Bradley, **G. Stringhini**. A Qualitative Evaluation of Two Different Law Enforcement Approaches on Dark Net Markets. In *Workshop on Attackers and Cyber-Crime Operations (WACCO)*, 2019.

(W19) J. Onaolapo, M. Lazarov, **G. Stringhini**. Master of Sheets: A Tale of Compromised Cloud Documents. In *Workshop on Attackers and Cyber-Crime Operations (WACCO)*, 2019.

(W18) S. Zannettou, T. Caulfield, E. De Cristofaro, M. Sirivianos, **G. Stringhini**, J. Blackburn. Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web. In *Workshop on Computational Methods in Online Misbehavior (CYBERSAFETY)*, 2019.

(W17) M. Edwards, G. Suarez-Tangil, C. Peersman, **G. Stringhini**, A. Rashid, M. Whitty. The Geography of Online Dating Fraud. In *Workshop on Technology and Consumer Protection (ConPro)*, 2018.

(W16) E. Bernard-Jones, J. Onaolapo, **G. Stringhini**. BABELTOWER: How Language Affects Criminal Activity in Stolen Webmail Accounts. In *Workshop on Computational Methods in CyberSafety, Online Harassment and Misinformation (CYBERSAFETY)*, 2018.

(W15) S. Zannettou, B. Bradlyn, E. De Cristofaro, M. Sirivianos, **G. Stringhini**, H. Kwak, J. Blackburn. What is Gab? A Bastion of Free Speech or an Alt-Right Echo Chamber?. In *Workshop on Computational Methods in CyberSafety, Online Harassment and Misinformation (CYBERSAFETY)*, 2018.

(W14) E. Mariconti, J. Onaolapo, G. Ross, and **G. Stringhini**. The Cause of All Evils: Assessing Causality Between User Actions and Malware Activity. In *Proceedings of the USENIX Workshop on Cyber Security Experimentation and Test (CSET)*, 2017.

(W13) J. Serrà, I. Leontiadis, D. Spathis, **G. Stringhini**, J. Blackburn, and A. Vakali. Class-based Prediction Errors to Categorize Text with Out-of-vocabulary Words. In *Proceedings of the Workshop on Abusive Language (ALW)*, 2017.

(W12) G. Mba, J. Onaolapo, **G. Stringhini**, L. Cavallaro. Flipping 419 Cybercrime Scams: Targeting the Weak and the Vulnerable. In *Companion Proceedings of the International World Wide Web Conference (WWW), International Workshop on Computational Methods for CyberSafety (CYBERSAFETY)*, 2017.

(W11) D. Chatzakou, N. Kourtellis, J. Blackburn, E. De Cristofaro, **G. Stringhini**, and A. Vakali. Measuring #GamerGate: A Tale of Hate, Sexism, and Bullying. In *Companion Proceedings of the International World Wide Web Conference (WWW), International Workshop on Computational Methods for CyberSafety (CYBERSAFETY)*, 2017.

(W10) M. Whitty, M. Edwards, M. Levi, C. Peersman, A. Rashid, A. Sasse, T. Sorell, **G. Stringhini**. Ethical and Social Challenges with developing Automated Methods to Detect and Warn potential victims of Mass-marketing Fraud (MMF). In *Companion Proceedings of the International World Wide Web Conference (WWW), International Workshop on Computational Methods for CyberSafety (CYBERSAFETY)*, 2017.

(W9) P. Andriotis, M.A. Sasse, **G. Stringhini**. Permissions Snapshots: Assessing Users' Adaptation to the Android Runtime Permission Model. In *Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS)*, 2016.

(W8) E. Mariconti, J. Onaolapo, G. Ross, **G. Stringhini**. What's your major threat? On the differences between the network behavior of targeted and commodity malware. In *Proceedings of the International Workshop on Malware Anaysis (WMA)*, 2016.

(W7) M. Lazarov, J. Onaolapo, **G. Stringhini**. Honey Sheets: What Happens to Leaked Google Spreadsheets? In *Proceedings of the USENIX Workshop on Cyber Security Experimentation and Test (CSET)*, 2016.

(W6) I. Becker, A. Hutchings, R. Abu Salma, S. J. Murdoch, R. Anderson, N. Bohm, M. A. Sasse, **G. Stringhini**. International Comparison of Bank Fraud Reimbursement: Customer Perceptions and Contractual Terms. In *Proceedings of the Workshop on the Economics of Information Security (WEIS)*, 2016.

(W5) E. Mariconti, J. Onaolapo, S. Ahmad, N. Nikiforou, M. Egele, N. Nikiforakis, **G. Stringhini**. Why Allowing Profile Name Reuse Is A Bad Idea. In *Proceedings of the European Workshop on System Security (EUROSEC)*, 2016.

(W4) M.B. Line, A. Zand, **G. Stringhini**, R. Kemmerer. Targeted Attacks against Industrial Control Systems: Is the Power Industry Prepared?. In *Proceedings of the Smart Energy Grid Security Workshop (SEGS)*, 2014.

(W3) J. Iedemska, **G. Stringhini**, R. Kemmerer, C. Kruegel, and G. Vigna. The Tricks of the Trade: What Makes Spam Campaigns Successful?. In *Proceedings of the International Workshop on Cyber Crime (IWCC)*, 2014.

(W2) **G. Stringhini**, M. Egele, C. Kruegel, and G. Vigna. Poultry Markets: On the Underground Economy of Twitter Followers. In *Proceedings of the ACM SIGCOMM Workshop on Online Social Networks (WOSN)*, 2012.

(W1) B. Stone-Gross, T. Holz, **G. Stringhini**, and G. Vigna. The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns. In *Proceedings of the USENIX Workshop on Large-Scale Exploits and Emerging Threats (LEET)*, 2011.

Posters (Peer Reviewed)

(P3) S. Qasim, M. Toslali, S. Parthasarathy, F. Oliviera, Z. Liu, **G. Stringhini**, A. Coskun. Efficient Navigation of Cloud Performance with 'nuffTrace. In *IEEE International Conference on Cloud Engineering (ICSE)*, 2023.

(P2) S. Ullah, A. Coskun, A. Morari, S. Pujar, **G. Stringhini**. Step-by-Step Vulnerability Detection using Large Language Models. In *USENIX Security Symposium*, 2023.

(P1) Y. Zhou, J. Li, **G. Stringhini**, A. Coskun, Z. Liu. Enabling Privacy-preserving Network Telemetry with Autoencoders. In *IEEE International Conference on Cloud Engineering (ICSE)*, 2023.

Patents

2017 **Systems and Methods for Detecting Compromised Messaging Accounts**, *U.S. Patent and Trademark Office — Publication Number US9756007 B1*, Gianluca Stringhini and Olivier Thonnard.

Conference Chair Service

2024 **Program Co-Chair**, *Annual Computer Security Applications Conference (ACSAC)*.

2024 **Track Chair**, *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, Chair for the "Security Usability and Measurement" Track.

2023 **Program Co-Chair**, *Cyber Security Experimentation and Test Workshop (CSET)*.

2022 **Program Co-Chair**, *Truth and Trust Online Conference (TTO)*.

2021-2022 **Artifact Evaluation Co-Chair**, *Annual Computer Security Applications Conference (ACSAC)*.

2021 **Data Challenge Co-Chair**, *AAAI International Conference on Web and Social Media (ICWSM)*.

2021 **Co-Chair**, *Symposium on AI in Healthcare: Mitigating Disparities, Biases & Misinformation*, Boston University Hariri Institute for Computing.

2020	**Program Co-Chair**, *BU Data Science (BUDS) Day.*
2020	**General Chair**, *APWG eCrime Symposium.*
2020	**Publication Chair**, *International Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA).*
2018-2019	**Program Chair**, *APWG eCrime Symposium.*
2019	**Publication Chair**, *ACM Conference on Computer and Communications Security (CCS).*
2016	**Program Co-chair**, *International World Wide Web Conference (WWW), Poster Track.*

Journal Editor Service

2023-	**Co-Department Editor of AI Security and Privacy**, *IEEE Security & Privacy Magazine.*
2020-2024	**Guest Editor**, *ACM Digital Threats: Research and Practice (DTRAP).*
2019	**Co-Editor**, *Crime Science Journal, Special Issue on Cybercrime.*

Program Committee Service

2016-2024	**USENIX Security Symposium**.
2015, 2018, 2023, 2024	**Network and Distributed System Security Symposium (NDSS)**.
2015-2022,2024	**International Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)**.
2015-2023	**Annual Computer Security Applications Conference (ACSAC)**.
2023	**USENIX Security Symposium**, *Research Ethics Committee Member.*
2018-2020, 2022	**IEEE Symposium on Security and Privacy (Oakland)**.
2022	**IEEE Symposium on Security and Privacy (Oakland)**, *Research Ethics Committee Member.*
2022	**IEEE European Symposium on Security and Privacy**.
2021-2022	**International Symposium on Research in Attacks, Intrusions and Defenses (RAID)**.
2016-2021	**The Web Conference (WWW), Security and Privacy Track**.
2020-2021	**ACM Conference on Web Science (WebSci)**.
2020-2021	**AAAI International Conference on Web and Social Media (ICWSM)**.
2015-2020	**ACM Conference on Computer and Communications Security (CCS)**.
2018-2019	**ACM SIGCOMM Internet Measurement Conference (IMC)**.
2017,2019	**ACM Asia Conference on Computer and Communications Security (ASIACCS)**.
2015-2018	**European Workshop on System Security (EuroSec)**.
2017-2018	**Workshop on Innovations in Mobile Privacy and Security (IMPS)**.
2017-2018	**Workshop on Targeted Attacks**.
2017-2019	**CyberSafety Workshop**.
2016, 2018	**USENIX Workshop on Cyber Security Experimentation and Test (CSET)**.
2016-2017	**eCrime Symposium**.
2016	**International Symposium on Engineering Secure Software and Systems (ESSoS)**.
2015	**ACM Cloud Computing Security Workshop (CCSW)**.
2015	**International World Wide Web Conference (WWW), Demo Track**.

2015 **International Conference on Availability, Reliability and Security (ARES)**.

2015 **IEEE International Conference on Distributed Computing Systems (ICDCS), Security and Privacy Track**.

2015 **OWASP AppSecEU**.

2014 **IEEE International Symposium on Cyberspace Safety and Security (CSS)**.

2014 **Annual Workshop on Simplifying Complex Networks for Practitioners (SIMPLEX)**.

Teaching

At Boston University

2019-2024 **EC 327: Introduction to Software Engineering**, *Boston University*, Boston, MA.

2020-2023 **EC 521: Cybersecurity**, *Boston University*, Boston, MA.

2019-2023 **EC 700: Malware, Online Abuse, and Cybercrime**, *Boston University*, Boston, MA.

2020 **UK Cybersecurity Winter School**, *Newcastle University*, Newcastle, UK.
Lecture

At University College London

2015-2018 **UCL Computer Science Hacking Seminar**, *University College London*, London, UK.

2016-2018 **SECUGC62: Cybercrime**, *University College London*, London, UK.

2015-2018 **COMPGA02: Computer Security 2**, *University College London*, London, UK.

2017 **Malware**, *University of Oxford*, Oxford, UK.
Lecturer for a week-long course in the Software Engineering Programme (SEP)

2015-2017 **Malware**, *University of Oxford*, Oxford, UK.
Lecturer for a week-long course in the Centre for Doctoral Training in Cyber Security

2017 **Usable Security and Privacy in Online Social Networks Summer School**, *Cyprus University of Technology*, Cyprus, CY.
Lecture

Mentorship and Supervision

Postdoctoral researchers – at University College London

2018-2019 **Srdjan Matic**, Now postdoctoral researcher at IMDEA Software.

2017-2018 **Guillermo Suàrez De Tangil**, Now Faculty at IMDEA Networks.

2016 **Panagiotis Andritiotis**, Now Faculty at the University of Birmingham.

PhD students – at Boston University

2023- **Olawale Akanji**, Co-advised with Manuel Egele.

2023- **Juehao Lin**, Co-advised with Manuel Egele.

2023- **William Wang**, Co-advised with Manuel Egele.

2021- **Saad Ullah**.

2020- **Pujan Paudel**.

2018- **Giannis Angelakopoulos**, Co-advised with Manuel Egele.

2018- **Beliz Kaleli**, Co-advised with Manuel Egele.

2019-2024 **Shiza Ali**.

2019-2024 **Mohammad Hammas Saeed**.

2019-2024 **Cici Ling**.

2018-2023 **Yuping Wang**, Now Assistant Professor at Renmin University of China.

PhD students – at University College London

2018-2024 **Octavian Bordeanu**, Second Supervisor to Toby Davies.

2016-2022 **Dario Adriano Bermudez Villalva**, Now Research Associate at Royal Holloway, University of London.

2016-2021 **Colin Ife**.
First Employment at Snyk

2017-2021 **Francois Labreche**, *Ecole Polytechnique de Montreal, (Co-advised with Josè Fernandez)*, Now at SecureWorks.

2015-2020 **Beatrice Perez**, Second Supervisor to Mirco Musolesi.
First Employment CIFI Fellow at Dartmouth College

2016-2019 **Cerys Bradley**, First Employment Researcher at Galop.

2015-2019 **Enrico Mariconti**, Now Faculty at University College London.

2014-2019 **Jeremiah Onaolapo**, Now Tenure Track Assistant Professor at the University of Vermont.

2014-2018 **Lucky Onwuzurike**, Second Supervisor to Emiliano De Cristofaro.
First Employment at EY

MS/MEng Students – at Boston University

2023-2024 **Arthur Savage, Jingyi Zhang**.

2023 **Angela Castronuovo**.

2021-2022 **Assel Aliyeva, Fahad Farid**.

MS/MEng Students – at University College London

2016-2017 **Giulia Della Rossa, Anastasia Grigoropolou, Spyridoula Karapanagioti, Andria Kyriacou, Qiaoyu Luo, Christopher Ojinaka, Adrian Rothan Ortiz, Tom Sigler**.

2015-2016 **Mahmoud Al-ghreify, Antonios Athanasopoulos, Emeric Bernard-Jones, Alex Kornitzer, Beverley Nutter, Natdanai Saitong-in, Elodie Thomann, Matthew Wixey**.

2014-2015 **Aristeidis Athanasiou, Sarah Azouvi, Khalid Binsaeed, Caitlin Egen, Andreas Haslebacher, Katarzyna Klosieska, Nicolas Nikiforou, Bethany Simpson**.

BS Students – at Boston University

2023-2024 **Primah Muwanga, Jason Redick**.

2020-2022 **Quan Minh Pham**.

2019-2020 **Terry Zhen**.

BS Students – at University College London

2017-2018 **Amir Dhada**.

2015-2016 **Martin Lazarov**.

2014-2015 **Giulia Deiana, Genki Saito, Cheung Tin Timothy Szeto**.

Visiting Students

2020	**Simone Patuelli**, *Visiting MS Student from Politecnico di Milano.*
2017	**Omid Mirzaei**, *Visiting PhD Student from University Carlos III de Madrid.*
2017	**Francois Labrèche**, *Visiting PhD Student from Ecole Politechnique de Montreal.*
2015-2016	**Beata Slomka**, *Visiting PhD Student from University of Warsaw.*

PhD examinations

2023-2024	**Ashwaq Alsoubai (Vanderbilt), Freddie Barr-Smith (Oxford University), Alexander Bulekov (BU), Feisi Fu (BU), Seunghyun Kim (Georgia Tech), Stefan Gvozdenovic (BU).**
2022-2023	**Novak Boskov (BU), Rasoul Jahanshahi (BU), Jan Leukfeldt (KIT), Sadullah Kanakci (BU).**
2021-2022	**Max Aliapoulious (NYU), Muhammad Anas Imtiaz (BU), Calvin Brierley (University of Kent), Henry Clausen (University of Edinburgh).**
2020-2021	**Andrew Cutler (BU), Leila Delshadtehrani (BU), Ziya Alper Genk (Luxembourg University), Laura Greige (BU).**
2019-2020	**Onur Zungur (BU).**
2018-2019	**Sajjad Arshad (Northeastern), Ahmet Buyukkayhan (Northeastern), Boyou Zhou (BU).**
2017	**Rodrigo Carvalho**, *University of Oxford.*
2016	**Marjan Falahrastegar (Queen Mary University of London).**
2016	**Mariam Nouh (Oxford University).**
2016	**Kimberly Tam (Royal Holloway, University of London).**
2015	**Ingolf Becker (UCL).**

Government Engagement

03/07/2018	**Witness to the Select Committee on International Relations of the House of Lords**, *House of Parliament*, London, UK, Gave evidence on the threats posed by state and non-state actors to the UK.

Invited Talks

Keynotes

9/23/2022	**Computational Methods to Measure and Mitigate Online Disinformation**, *Computing Student Research Day*, University of Vermont, Burlington, VT.
10/07/2021	**A Large-Scale, Multi-Platform, and Multi-Modal Look at Online Disinformation**, *Truth & Trust Online Conference (TTO)*, Online.
05/15/2019	**Computational Methods to Understand and Mitigate Online Hate**, *Workshop on Computational Methods in Online Misbehavior*, San Francisco, CA.
07/21/2015	**On The Threats To Cloud-based Online Service Users**, *International Conference on High Performance Computing and Simulation (HPCS)*, Amsterdam, Netherlands.

Invited talks and seminars

10/11/2023 **Computational Methods to Measure and Mitigate Online Aggression**, *Rebooting Social Media Speaker Series*, Harvard Berkman Klein Center.

9/27/2023 **Computational Methods to Measure and Mitigate Online Disinformation**, *OSoMe Awesome Speaker Series*, Indiana University (Online).

6/30/2023 **Computational Methods to Measure and Mitigate Online Disinformation**, *Doctoral Training Centre in Cybersecurity Symposium*, University College London, UK.

05/15/2023 **Computational Methods to Measure and Mitigate Online Aggression**, *Workshop on Social Processes of Online Hate*, University of California, Santa Barbara.

11/02/2022 **Measuring and Mitigating Online Influence Campaigns**, *Google Security, Privacy, and Anti-Abuse Research Workshop*, Online.

07/12/2022 **Tracking image-based (mis|dis)information**, *Conference on Mis/Dis Information in Global Health*, Massachussets Institute of Technology.

04/27/2022 **A Large-Scale, Multi-Platform, and Multi-Modal Look at Online Disinformation**, *Milton Academy*.

04/08/2022 **Computational Methods to Measure and Mitigate Weaponized Online Information**, *Dartmouth College*, Online.

02/16/2022 **AI for Cloud Ops**, *Red Hat Research Days*, Online.

12/08/2021 **Computational Methods to Measure and Mitigate Weaponized Online Information**, *MIT Lincoln Laboratory*, Online.

11/01/2021 **Computational Methods to Measure and Mitigate Weaponized Online Information**, *University of Cambridge*, Online.

09/22/2021 **Measuring Image-based COVID Misinformation at Scale**, *BU Research on Tap*, Boston, MA.

02/17/2021 **Computational Methods to Measure and Mitigate Weaponized Online Information**, *University of Illinois at Urbana Champaign*, Online.

02/12/2021 **Computational Methods to Measure and Mitigate Weaponized Online Information**, *Florida International University*, Online.

02/03/2021 **Computational Methods to Understand and Mitigate Online Aggression**, *USENIX Enigma Conference*, Online.

09/14/2020 **Computational Methods to Measure and Mitigate Weaponized Online Information**, *Cylab, Carnegie Mellon University*, Online.

03/02/2020 **Computational Methods to Measure and Mitigate Weaponized Online Information**, *Exploring Media Ecosystems Conference*, Cambridge, MA.

02/14/2020 **Measuring and Disrupting Malware Delivery Networks**, *BU Cloud Computing Workshop*, Boston, MA.

02/05/2020 **Data-driven Modeling of Harmful Online Behavior**, *BU Data Science Day*, Boston, MA.

12/11/2019 **Computational Methods to Measure and Mitigate Weaponized Online Information**, *Hariri Meet Our Fellows Series*, Boston, MA.

07/27/2018 **Understanding the influence of fringe communities on the greater Web**, *University of Chicago*, Chicago, IL.

04/16/2018 **A Measurement Study of 4chan's Politically Incorrect Board and its Effects on the Web**, *Europol ECTC Advisory Board*, The Hague, The Netherlands.

01/22/2018   **The Influence of Fringe Communities in the Spread of Fake News**, *WebRoots Democracy Workshop*, London, United Kingdom.

11/30/2017   **Interdisciplinary Cybercrime Research: Where Are We?**, *RISCS Cybercrime Workshop*, London, United Kingdom.

11/16/2017   **Understanding and Mitigating Online Abuse**, *Exeter University*, Exeter, United Kingdom.

09/13/2017   **The Hacker, the Swindler, and the Troll: Understanding and Measuring Abuse on Online Services**, *CISPA, University of Saarland*, Saarbrücken, Germany.

09/11/2017   **Cyberfraud and Scams**, *Dagstuhl Seminar*, Schloss Dagstuhl, Germany.

07/14/2017   **Understanding the Use of Stolen Credentials by Cybercriminals**, *Cambridge Cybercrime Conference*, Cambridge, UK.

06/21/2017   **Understanding Modern Cybercriminal Operations**, *AON Benfield Research Forum*, London, UK.

05/24/2017   **Fighting Modern Cybercriminal Operations**, *University of Kent*, Canterbury, UK.

05/22/2017   **A Measurement Study of 4chan's Politically Incorrect Forum and its Effects on the Web**, *VoxPol Workshop*, London, UK.

11/17/2016   **The Hacker, the Swindler, and the Troll: Understanding and Measuring Abuse on Online Services**, *University of California, Santa Barbara*, Santa Barbara, CA.

10/26/2016   **Understanding and Measuring Abuse on Online Services**, *Facebook*, London, UK.

06/26/2016   **Understanding and Fighting Cybercriminal Operations**, *Telefonica Investigacion y Desarrollo*, Barcelona, Spain.

04/29/2016   **Fighting Modern Cybercriminal Operations**, *University of Oxford*, Oxford, UK.

03/16/2016   **Following the Trail of Cybercriminal Operations**, *Workshop on the Human Factors in Security, University of Surrey*, Guildford, UK.

09/23/2015   **Detecting Compromised Accounts on Online Services**, *Lancaster University*, Lancaster, UK.

05/05/2015   **Dissemination of False and Malicious Information on Online Social Networks**, *Sikkerhet & Sårbarhet Workshop*, Trondheim, Norway.

05/04/2015   **Dissemination of False and Malicious Information on Online Social Networks**, *Norwegian University of Science and Technology (NTNU)*, Trondheim, Norway.

04/21/2015   **On The Exploitation Of Trust On Online Social Networks (And What We Can Do About It)**, *University of Cambridge*, Cambridge, UK.

02/09/2015   **On The Exploitation Of Trust On Online Social Networks (And What We Can Do About It)**, *University of Oxford*, Oxford, UK.

02/05/2015   **On The Exploitation Of Trust On Online Social Networks (And What We Can Do About It)**, *University of Birmingham*, Birmingham, UK.

02/03/2015   **Large Scale Cybercrime Vs. Targeted Attacks: What Are The Differences And How Can We Fight These Threats?**, *CyberCount Workshop*, London, UK.

10/30/2014   **Leveraging The Scale Of Cybercrime To Fight Malware Operations**, *Royal Holloway, University of London*, Egham, UK.

10/06/2014   **Leveraging The Scale Of Cybercrime To Fight Malware Operations**, *CSecLab Workshop on Mobile Security*, Genova, Italy.

05/01/2013   **Fighting Targeted Email Attacks**, *Symantec Corp.*, San Francisco, CA.

04/26/2013 **Stepping Up The Cybersecurity Game**, *Yahoo! Inc.*, Sunnyvale, CA.

12/13/2012 **Modelling Host Network Behavior To Detect Stealthy And Targeted Attacks**, *IBM T.J. Watson Research Center*, Yorktown Heights, NY.

12/22/2011 **The Spammer, the Botmaster, And The Researcher: On The Arms Race In Spamming Botnet Mitigation**, *Università degli Studi di Genova*, Genova, Italy.

07/06/2010 **Detecting Spammers On Social Networks**, *Politecnico di Milano*, Milano, Italy.

03/23/2010 **Detecting Spammers On Twitter**, *Twitter Inc.*, San Francisco, CA.

In the Press

6/20/2024 **Empowering defenders through our Cybersecurity Grant Program**, *OpenAI Blog*, https://openai.com/index/empowering-defenders-through-our-cybersecurity-grant-program/.

12/4/2023 **Online 'likes' for toxic social media posts prompt more - and more hateful - messages**, *The Conversation*, https://theconversation.com/online-likes-for-toxic-social-media-posts-prompt-more-and-more-hateful-messages-218220.

10/23/2023 **How Elon Musk ditched Twitter's safeguards and primed X to spread misinformation**, *Politifact*, https://www.politifact.com/article/2023/oct/23/how-elon-musk-ditched-twitters-safeguards-and-prim/.

10/12/2023 **Chain message warning of WhatsApp cyberattack linked to war images is a hoax**, *ABC News*, https://www.13newsnow.com/article/news/verify/israel-hamas-war/viral-chain-message-warning-of-whatsapp-cyberattack-linked-to-israel-hamas-war-hoax/.

9/26/2023 **No, the warnings about the 'Mexico did it' virus aren't legitimate**, *Verify*, https://www.verifythis.com/article/news/verify/social-media/mexico-did-it-virus-warnings-not-legitimate-fact-check/536-54e64395-0360-41f8-9cab-c407d1c6d330.

9/19/2023 **False claim of malware disguised as message about COVID-19 and Mexico**, *USA Today*, https://www.usatoday.com/story/news/factcheck/2023/09/19/experts-say-no-evidence-of-malware-message-about-mexico-fact-check/70867234007/.

7/26/2023 **Inside the Mind of an Internet-Safety Vanguard**, *The Brink*, https://www.bu.edu/articles/2023/inside-the-mind-of-an-internet-safety-vanguard/.

1/14/2023 **Andrew Tate charged with human trafficking — and continues to gain followers**, *Salon*, https://www.salon.com/2023/01/14/andrew-tate-charged-with-human-trafficking--and-continues-to-gain-followers/.

12/3/2022 **In Elon Musk's chaotic Twitter reign, right-wing extremists and conspiracy theorists are back**, *Salon*, https://www.salon.com/2022/12/03/in-elon-musks-chaotic-twitter-reign-right-wing-extremists-and-conspiracy-theorists-are-back/.

11/17/2022 **The Twitter Bubble Let Democrats Defy Political Gravity**, *Wired*, https://www.wired.com/story/election-twitter-midterms-trans-kids/.

11/17/2022 **Elon Musk is planning a subtle change to Twitter that could make it harder to stop the bots**, *CNN*, https://www.cnn.com/2022/11/17/tech/elon-musk-twitter-device-identifiers/index.html.

11/10/2022 **Un mondo senza Twitter è possibile?**, *Il Post*, https://www.ilpost.it/2022/11/10/senza-twitter/.

11/08/2022 **Internet and Extremism Experts Predict More Hate Speech and Conspiracy Theories on Musk's Twitter**, *Scientific American*, https://www.scientificamerican.com/article/internet-and-extremism-experts-predict-more-hate-speech-and-conspiracy-theories-on-musks-twitter/.

11/04/2022 **How Musk's takeover might change Twitter: what researchers think**, *Nature News*, https://www.nature.com/articles/d41586-022-03552-4.

7/29/2022 **Combating Misinformation In The Age of Technology**, *BU Experts*, https://buexperts.medium.com/combating-misinformation-in-the-age-of-technology-726ca57d6c05.

3/28/2022 **Video Security Is More Than Just Security – It's About Brand Integrity And Your Customer Commitments**, *Forbes*, https://www.forbes.com/sites/forbestechcouncil/2022/03/28/video-security-is-more-than-just-security—its-about-brand-integrity-and-your-customer-commitments/.

2/3/2022 **Does banning extremists online work? It depends**, *Vox*, https://www.vox.com/recode/22913046/deplatforming-extremists-ban-qanon-proud-boys-boogaloo-oathkeepers-three-percenters-trump.

12/17/2021 **TikTok doesn't read your mind, it makes your mind**, *ZDNet*, https://www.zdnet.com/article/tiktok-doesnt-read-your-mind-it-makes-your-mind/.

12/1/2021 **Researchers Have a Method to Spot Reddit's State-Backed Trolls**, *Wired*, https://www.wired.co.uk/article/researchers-reddit-state-trolls.

10/13/2021 **Everything you need to know about the Facebook outage**, *BU Experts*, https://buexperts.medium.com/everything-you-need-to-know-about-the-facebook-outage-af2b899e7b5a.

10/01/2021 **Endless Thread**, *WBUR Boston*, https://www.wbur.org/podcasts/endlessthread/.

9/28/2021 **Malware Apps Linger on Market for Weeks, Stringhini Finds**, *BU College of Engineering*, https://www.bu.edu/eng/2021/09/24/malware-apps-linger-on-market-for-weeks-stringhini-finds/.

8/12/2021 **Google can take two months to remove malware apps from app store**, *NewScientist*, https://www.newscientist.com/article/2286931-google-can-take-two-months-to-remove-malware-apps-from-app-store/.

3/22/2021 **BU Researchers Warned of Online Surge of Anti-Asian Attacks a Year Ago**, *BU Today*, http://www.bu.edu/articles/2021/bu-researchers-warned-of-online-surge-of-anti-asian-attacks-a-year-ago/.

2/20/2021 **Smiling on the outside: Super Happy Fun America always claimed to be kidding. But the group's history suggests otherwise**, *The Boston Globe*, https://apps.bostonglobe.com/metro/politics/2021/02/super-happy-fun-america/.

2/04/2021 **Zoombombing countermeasures are ineffective in the vast majority of cases**, *Ars Technica*, https://arstechnica.com/information-technology/2021/02/zoombombing-countermeasures-are-ineffective-in-the-vast-majority-of-cases/.

2/03/2021 **Why Insider 'Zoom Bombs' Are So Hard to Stop**, *Wired*, https://www.wired.com/story/zoombomb-inside-jobs/.

1/26/2021 **The Bernie Sanders Sitting Meme's Instant Popularity, Explained by Science**, *The Brink*, http://www.bu.edu/articles/2021/bernie-sanders-sitting-memes-instant-popularity-explained-by-science.

1/25/2021 **Science tells us why the Bernie meme went mega-viral**, *Input Magazine*, https://www.inputmag.com/culture/viral-meme-ai-study-bernie-sanders.

1/09/2021 **La victoria de los troles: de còmo Internet se ha convertido en la vida real**, *El Pais (in Spanish)*, https://elpais.com/tecnologia/2021-01-08/la-victoria-de-los-trols-de-como-internet-se-ha-convertido-en-la-vida-real.html.

1/08/2021 **Banning Trump from Social Media Makes Sense. But Beware the Downside**, *The Brink*, https://www.bu.edu/articles/2021/trump-banned-from-twitter-facebook/.

8/23/2020 **Political trolls adapt, create material to deceive and confuse the public**, *Salon*, https://www.salon.com/2020/08/23/political-trolls-adapt-create-material-to-deceive-and-confuse-the-public_partner/.

8/13/2020 **Political trolls adapt, create material to deceive and confuse the public**, *The Conversation*, https://theconversation.com/political-trolls-adapt-create-material-to-deceive-and-confuse-the-public-135177.

6/17/2020 **Images Play Persuasive Role in Disinformation Campaigns**, *Darkreading*, https://www.darkreading.com/threat-intelligence/images-play-persuasive-role-in-disinformation-campaigns/d/d-id/1338110.

5/18/2020 **Sneakier and More Sophisticated Malware Is On the Loose**, *IEEE Spectrum*, https://spectrum.ieee.org/tech-talk/telecom/security/analysis-shows-malware-evolving-encrypted-sophisticated.

4/08/2020 **As the coronavirus spreads, so does online racism targeting Asians, new research shows**, *The Washington Post*, https://www.washingtonpost.com/technology/2020/04/08/coronavirus-spreads-so-does-online-racism-targeting-asians-new-research-shows/.

3/13/2020 **Don't Believe These 4 Wild Coronavirus Conspiracy Theories**, *Vice News*, https://www.vice.com/en_us/article/epgkkz/dont-believe-these-4-wild-coronavirus-conspiracy-theories.

3/11/2020 **Hand-washing memes**, *The World (Public Radio International)*, https://www.pri.org/file/2020-03-10/hand-washing-memes.

1/22/2020 **What Will 2020 Look Like? BU Faculty Offer Predictions**, *BU Today*, http://www.bu.edu/articles/2020/what-will-2020-look-like-bu-faculty-offer-predictions.

11/8/2019 **Research: How tech can help identify hate speech videos and impact content moderation**, *TechRepublic*, https://www.techrepublic.com/article/research-how-tech-can-help-identify-hate-speech-videos-and-impact-content-moderation/.

6/14/2019 **Algorithms Won't Fix What's Wrong With YouTube**, *The New York Times*, https://www.nytimes.com/2019/06/14/opinion/youtube-algorithm.html.

4/1/2019 **"The Left Can't Meme": How Right-Wing Groups Are Training the Next Generation of Social Media Warriors**, *MotherJones*, https://www.motherjones.com/politics/2019/04/right-wing-groups-are-training-young-conservatives-to-win-the-next-meme-war/.

3/18/2019 **YouTube removes videos continuing to celebrate New Zealand mosque attacks**, *Sky News*, https://news.sky.com/story/youtube-removes-videos-continuing-to-celebrate-new-zealand-mosque-attacks-11669478.

2/8/2019 **Twitter still can't keep up with its flood of junk accounts, study finds**, *Wired*, https://www.wired.com/story/twitter-abusive-apps-machine-learning/.

11/23/2018 **Who let the trolls out? Researchers investigate state-sponsored trolls**, *TechXplore*, https://techxplore.com/news/2018-11-trolls-state-sponsored.html.

10/29/2018 **Pittsburgh Synagogue Shooting Puts Spotlight on Fringe Platforms and Their Partners**, *The Wall Street Journal*, https://www.wsj.com/articles/pittsburgh-synagogue-shootingputs-spotlight-on-fringe-platforms-and-their-partners-1540861173.

07/08/2018 **Where Do Memes Come From?**, *BBC Trending*, https://www.bbc.co.uk/programmes/w3csws6t.

03/02/2018 **Così odio, insulti e fake news invadono i nostri schermi**, *Giornale Radio Rai GR1*, https://soundcloud.com/user-873190463/elezioni2018-gianluca-stringhini-cosi-odio-insulti-e-fake-news-invadono-i-nostri-schermi.

11/24/2017 **Long read: Key evidence linking Kremlin to social media trolls is lacking**, *Sky News*, https://news.sky.com/story/long-read-key-evidence-linking-kremlin-to-social-media-trolls-is-lacking-11137255.

11/2/2017 **Study finds fringe communities on Reddit and 4chan have high influence on flow of alternative news to Twitter**, *Phys.org*, https://phys.org/news/2017-11-fringe-reddit-4chan-high-alternative.html.

06/13/2017 **Hate map, la prima mappa sull'odio online**, *L'Unità (in Italian)*, http://www.unita.tv/focus/hate-map-la-prima-mappa-sullodio-online/.

06/13/2017 **La prima mappa del 'lato oscuro' del web. "Così odio, insulti e fake news viaggiano online"**, *La Repubblica (in Italian)*, http://www.repubblica.it/tecnologia/social-network/2017/06/13/news/odio_insulti_e_fake_news_la_prima_mappa_del_lato_oscuro_del_web-167988521/.

06/12/2017 **Dalle fonti ai social, ecco la prima mappa dell'odio online**, *Ansa (in Italian)*, http://www.ansa.it/sito/notizie/tecnologia/internet_social/2017/06/12/mappa-odio-online-dalle-fonti-ai-social_253eca7b-4d3f-457b-a1ab-6e857d964925.html.

06/10/2017 **Research examines fake news, hate speech and 4chan**, *Sky News*, http://news.sky.com/story/research-examines-fake-news-hate-speech-and-4chan-10910915.

06/09/2017 **Shining a light on the dark corners of the web**, *Nature*, http://www.nature.com/news/shining-a-light-on-the-dark-corners-of-the-web-1.22128.

11/17/2016 **4chan raids: How one dark corner of the internet is spreading its shadows**, *The Independent*, http://www.independent.co.uk/life-style/gadgets-and-tech/4chan-raids-how-one-dark-corner-of-the-internet-is-spreading-its-shadows-a7416631.html.

11/12/2016 **Meme, board e viralità: la rete lontana dai social che ha incoronato Trump**, *La Repubblica (in Italian)*, http://www.repubblica.it/speciali/esteri/presidenziali-usa2016/2016/11/12/news/trump_internet_meme_virali_social_4chan-151826943/?ref=HREC1-1.

11/11/2016 **These are the world's most diverse cuisines**, *The Independent*, https://www.indy100.com/article/healthy-diverse-top-healthiest-countries-cuisine-food-in-the-world-list-7412171.

11/03/2016 **How Data Mining Reveals the World's Healthiest Cuisines**, *MIT Technology Review*, https://www.technologyreview.com/s/602790/how-data-mining-reveals-the-worlds-healthiest-cuisines/.

10/18/2016 **This Is What Hackers Actually Do With Your Stolen Personal Information**, *Huffington Post*, http://www.huffingtonpost.co.uk/entry/what-hackers-actually-do-with-your-stolen-personal-information_uk_58049f32e4b0e982146cd18f?jfn6f1p9kjy1ll3di.

10/16/2016 **How hackers handle stolen login data**, *BBC News*, http://www.bbc.co.uk/news/technology-37510501.

10/14/2016 **Scientists Invented a Tool to Expose 4chan's Racist Trolling Campaigns**, *Motherboard*, http://motherboard.vice.com/read/block-4chan-to-stop-the-alt-right-from-spreading-racist-memes-scientists-say.

10/14/2016 **Rane, odio e pro-Trump: così funziona 4chan, la pancia di internet**, *La Stampa (in Italian)*, http://www.lastampa.it/2016/10/14/societa/rane-odio-e-protrump-cos-funziona-chan-la-pancia-di-internet-qSR7NV32eMNHYxYtWGh4tJ/pagina.html.

08/24/2016 **UK Unis Under Fire as 56% Suffer Ransomware Infection**, *Infosecurity Magazine*, http://www.infosecurity-magazine.com/news/uk-unis-under-fire-56-suffer.

06/07/2016 **Will you get reimbursed if you're a bank fraud victim? Brits think not**, *The Register*, http://www.theregister.co.uk/2016/06/06/bank_terms_study.

03/22/2016 **Hackers for Hire**, *Business Daily — BBC World Service*, http://www.bbc.co.uk/programmes/p03mqj20.

04/11/2015 **Analyzing Reshipping Mule Scams**, *Schneier on Security*, https://www.schneier.com/blog/archives/2015/11/analyzing_reshi.html.

09/28/2015 **With Stolen Cards, Fraudsters Shop to Drop**, *Krebs on Security*, http://krebsonsecurity.com/2015/09/with-stolen-cards-fraudsters-shop-to-drop/.

09/19/2015 **Amico, spia o truffatore? Come difendersi dai finti profili social (in Italian)**, *La Stampa*, http://www.lastampa.it/2015/09/19/tecnologia/amico-spia-o-truffatore-come-difendersi-dai-finti-profili-social-HPH1iX5bny7vquC8yGDs0I/pagina.html.

05/16/2015 **Online Dating Scams Could Cost Lonely Men Thousands**, *The Young Turks*, https://www.youtube.com/watch?v=LbKDH7wIKS4.

05/14/2015 **China's Ingenious Online Dating Scams Put Ours To Shame**, *Buzzfeed*, http://www.buzzfeed.com/josephbernstein/chinas-ingenious-online-dating-scams-put-ours-to-shame.

05/07/2015 **Online Dating Scams**, *Schneier on Security*, https://www.schneier.com/blog/archives/2015/05/online_dating_s.html.

11/12/2014 **Malware doesn't discriminate when it comes to Web ads**, *InfoWorld*, http://www.infoworld.com/article/2846993/malware/malware-doesnt-discriminate-when-it-comes-to-web-ads.html.

09/24/2014 **Malrettende anrgrep – er kraftbransjen forberedt? (in Norwegian)**, *Energiteknikk*, Issue 6, September 2014, Pages 74-75.

07/20/2014 **Im Netz dem Bösen Jungs (in German)**, *Frankfurter Allgemeine Sonnenzeitung*, Issue 29, Page 45.

06/21/2014 **Spam in Blick (in German)**, *Deutschlandfunk*, http://www.deutschlandfunk.de/informatik-spam-im-blick.684.de.html?dram:article_id=289984.

06/19/2014 **A Spam Trinity: Email Harvesters, Botmasters, Spammers**, *Threatpost*, http://threatpost.com/a-spam-trinity-email-harvesters-botmasters-spammers.

06/04/2014 **Relations between spam landscape actors can be leveraged for detection**, *Help Net Security*, http://www.net-security.org/secworld.php?id=16959.

05/02/2014 **Boffins pen 'Guide to better spamming'**, *The Register*, http://www.theregister.co.uk/2014/05/02/boffins_pen_guide_to_better_spamming/.

02/04/2014 **Weak Links: URL Shorteners**, *Brown Hat Security*, http://brownhatsecurity.com/article.php?story=2014020517493113.

12/06/2013 **Hero Hackers: Computer Security Group Arms the Technological World**, *Coastlines — UCSB Alumni Association*, http://www.ucsbalum.com/Coastlines/2013/Fall/feature_cyberthreats.html.

05/03/2013 **Two-Factor Authentication No Cure-all for Twitter Security Woes**, *Threapost*, http://threatpost.com/two-factor-authentication-no-cure-all-for-twitter-security-woes.

03/29/2011 **Behind the curtain of a botnet business**, *CSO Online*, http://www.csoonline.com/article/2127919/social-engineering/behind-the-curtain-of-a-botnet-business.html.

08/10/2010 **Researchers Kneecap "Pushdo" Spam Botnet**, *Krebs on Security*, https://krebsonsecurity.com/2010/08/researchers-kneecap-pushdo-spam-botnet.

03/17/2010 **New Free Service Filters Twitter Spam**, *Darkreading*, http://www.darkreading.com/end-user/new-free-service-filters-twitter-spam/223900274.