philippnormann

PhD Student · AI for Security

TU Wien · Security and Artificial Intelligence Lab (SAIL) · Advised by Daniel Arp



contact

TU Wien, Informatics
Security and Privacy Unit
Vienna, Austria

philipp.normann@tuwien.ac.at
philippnormann.com
philippnormann
in/pnormann
Google Scholar

interests

AI agents for security
LLM evaluation
ML for security

languages

German (native)
English (fluent)
Romanian (intermediate)

programming

Python, Go, Java,
Clojure, Scala, C

tools

PyTorch, TensorFlow,
Docker, Kubernetes,
AWS, GCP

education

2025 – now **PhD** in Computer Science — *TU Wien*
Project assistant in SAIL since May 2025.
Funded by the WWTF project BREADS.

2018 – 2020 **MSc** in IT Security — *FH Wedel*
Thesis: “Adversarial Attacks and Defenses for Image-Based Recommendation Systems using Deep Neural Networks”.
Thesis grade 1.0 (best grade). Otto Group scholarship.

2013 – 2018 **BSc** in Computer Science — *FH Wedel*
Thesis: “Event-Based Fraud Detection in an E-Commerce Shop using Long Short-Term Memory Networks”.
Thesis grade 1.0 (best grade). Otto Group scholarship.

publications

security and AI

2026 Towards Reliable Local Security Agents: Verifiable Post-Training for Linux Privilege Escalation
Philipp Normann, Andreas Happe, Jürgen Cito, Daniel Arp
Annual Computer Security Applications Conference (ACSAC). To appear.
Artifacts Available, Functional, Reproduced · arXiv · Code · Artifact

2026 From Exploits to Guidelines: What LLMs Can and Cannot Automate in IoT Threat Intelligence
Philipp Normann, Carlotta Tagliaro, Martina Lindorfer, Daniel Arp
Workshop on AI for Cyber Threat Intelligence (WAITI), co-located with ACSAC. To appear.

2026 Chasing Shadows: Pitfalls in LLM Security Research
Jonathan Evertz, Niklas Risse, Nicolai Neuer, Andreas Müller, **Philipp Normann**, Gaetano Sapia, Srishti Gupta, David Pape, Soumya Shaw, Devansh Srivastav, Christian Wressnegger, Erwin Quiring, Thorsten Eisenhofer, Daniel Arp, Lea Schönherr
Network and Distributed System Security Symposium (NDSS).
Artifacts Available, Functional, Reproduced · Paper · Code · Artifact

2026 Towards Explaining Classification Models in Security with Sparse Autoencoders
Nils Ole Breuer, Lorenz Linhardt, **Philipp Normann**, Daniel Arp
IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), XAISec · Paper

recommender systems

2025 Identifying Offline Metrics that Predict Online Impact: A Pragmatic Strategy for Real-World Recommender Systems
Timo Wilm, **Philipp Normann**
ACM Conference on Recommender Systems (RecSys) · Paper

2024 Pareto Front Approximation for Multi-Objective Session-Based Recommender Systems
Timo Wilm, **Philipp Normann**, Felix Stepprath
ACM Conference on Recommender Systems (RecSys) · Paper · Code

2023 Scaling Session-Based Transformer Recommendations using Optimized Negative Sampling and Loss Functions
Timo Wilm, **Philipp Normann**, Sophie Baumeister, Paul-Vincent Kobow
ACM Conference on Recommender Systems (RecSys) · Paper · Code

publications (continued) · datasets

2023 OTTO Recommender Systems Dataset: A real-world e-commerce dataset for session-based recommender systems research
Philipp Normann, Sophie Baumeister, Timo Wilm
Kaggle · Dataset · GitHub

teaching

Winter 2025/26 – Winter 2026/27 **Machine Learning for Computer Security** — *TU Wien*
Teaching assistant. Co-designed and graded the exercises and helped with the exams. Gave a guest lecture on AI-based vulnerability discovery.

Summer 2026 **Attacking and Defending AI-based Systems** — *TU Wien*
Teaching assistant. Designed challenges, partly with colleagues, and graded them.

2025 **Scientific Writing and Research** (bachelor seminar) — *TU Wien*
Graded part of the seminar reports.

supervision

2026 **Diploma thesis** (co-advisor) — *TU Wien*
"User behavior simulation with large language models for security evaluation"

2026 **Bachelor thesis** (co-advisor) — *TU Wien*
"Design and Evaluation of a Local Open-Weight LLM-Based SSH Honeypot for Linux Shell Emulation"

2023 **Master thesis** (co-advisor) — *OTTO and FH Wedel*
"Graph Neural Networks for Complementary Product Recommendations in E-Commerce". Received the Hochschulpreis of the Wedeler Hochschulbund.

service

2025 – now **Subreviewer:** USENIX Security (2026, 2027), ACM CCS (2026), ACSAC (2026), IEEE SaTML (2026, 2027), RAID (2025), DIMVA (2026), ACM AISec (2025, 2026)

talks

10 Dec 2026 Towards Reliable Local Security Agents: Verifiable Post-Training for Linux Privilege Escalation — *ACSAC 2026, Los Angeles (upcoming)*

7 Dec 2026 From Exploits to Guidelines: What LLMs Can and Cannot Automate in IoT Threat Intelligence — *WAITI at ACSAC 2026, Los Angeles (upcoming)*

10 Jul 2026 Towards Reliable Local Security Agents — *DeMeSSAI at IEEE EuroS&P 2026, Lisbon*

Mar 2023 Insights from the OTTO Kaggle Competition — *RecSys Meetup by NVIDIA*

2022 Deep Multimodal Recommendations: Solving the Cold Start Problem — *MAIN 2.0 Conference*

2018 Real-Time Fraud Prognosis using Recurrent Neural Networks ▶ — *code.talks, Hamburg*

industry experience

Oct 2021 – Apr 2025 **Senior Data Scientist** — *OTTO, Hamburg*
- Co-authored OTTO's first papers at ACM RecSys (2023–2025).
- Ran OTTO's first Kaggle competition (2,500+ teams) and released its dataset.
- Built session-based Transformer and multimodal cold-start recommenders.

Apr 2019 – Sep 2021 **Data Scientist** — *OTTO, Hamburg*
Built session-based recommenders with RNNs. Improved the fraud detection system.

Apr 2018 – Mar 2019 **Junior Data Scientist** (part-time) — *OTTO, Hamburg*
Built a real-time fraud detection system with RNNs, based on the BSc thesis.

Apr 2017 – Sep 2017 **IT-Security Engineer** (intern) — *OTTO, Hamburg*
Built Security Belt, a web app for teams to assess and improve their IT security.

outreach

2019 – 2025 **Hamburg Coordinator** — *meetup.ai*
Organized the largest AI meetup in Hamburg (2,000+ members).